2012 International Conference on Information and Computer Networks (ICICN 2012)
IPCSIT vol. 27 (2012) © (2012) IACSIT Press, Singapore

A Multi-site Disaster Recovery Solution based on IP Storage Networking

Rekha Singha

TCS Innovation Lab, Mumbai, India

Abstract. This paper proposes an optimal service continuity solution based on IP SAN technology which will allow multi-site organizations to be active 24X7 even in case of major disasters. The solution is designed at global level which incorporates service continuity for all sub levels of services in an organization. This is useful for multi-site organizations providing e-services such as data centers and e-government. The proposed design uses a virtual centralized disaster recovery center (DRC) which is robust and can sustain failures, bypassing the weaknesses of centralized architecture. This paper also discusses the design of the proposed solution which is cost efficient while promising zero RPO and negligible RTO.

Keywords: IPSAN, Disaster Recovery, RPO, RTO, Service Continuity

1. Introduction

The globalization has led to multi-site presence for corporate. Especially, the data centers having world-wide presence need to have their sub data centers at lower levels. A request for service from data center may get initiated at any of its sub centers. Each of the sub data centers may have large amount of their client's data to protect from disasters. The Government of India is another good example of multi-site organization, which has initiated several e-governance services both at the central and state levels. Several initiatives such as e-panchayat, Sarita for land records, e-passport seva etc are already operational. All these services generate enormous amount of valuable data about citizens. Loss of any of these records may create loss of an identity for a citizen. Moreover, disruption of any of these services is not acceptable for normal functioning of the government system.

To summarize, there is great need for multi-site organizations such as Data Centers to protect their data against loss and also provide continuity to its services even in case of any disaster. The naïve approach for solving this problem is to use backup mechanism for recovering the last saved data and restarting the services in case of disaster. However, they lead to high data loss (RPO) since the last backup may be few hours old, and large time taken to start the service (RTO) since time is taken in retrieving the data from back-up system and starting the services. Wiboonrat [8] discusses the various DR solutions with their offered quality of service. Storage based data replication turns out to be most effective technology for optimal service continuity [7], which are zero RPO and negligible RTO.

Most of the DR solutions [1, 4, and 6] proposed in the literature addresses the issue of increasing the availability of single site organizations only, in case of disaster. For multi-site organizations, one option may be a linear solution with DR solution for each of the site; this may lead to non utilization of resources as DR sites are in full capacity of their primary site. Chidambaram [4] has looked at increasing the availability of data by doing replication in a grid environment where a failed site may be replaced by any other site (node) in the grid. Wang[5] has discussed a robust disaster recovery system model (RDRS) to ensure service continuity while maintaining high security; this is the need of the hour especially for e-governance. Wu [1] ensures the high availability for the data through the DIMM (Disaster Indexing Measurement Mechanism), which uses a scheduling model for the data backup and synchronization locally and remotely, based on the hierarchical infrastructure. However, it does not address the issues of multi-site services.

We are proposing architecture for establishing a disaster recovery or optimal service continuity solution for multi site organization such as government's e-services which are spread across whole nation. This may also be applicable to organizations spread on multiple locations. We propose a logically centralized and physically distributed Disaster Recovery as a Service model for service continuity of all multi-site services. One of the key requirements for a disaster recovery site is its geographical distance from its primary site. A naïve approach could be to set up a separate DR site for each of the sub center of the multi-site organization. This may double up the system installations, increases the man power, and under utilize the system. (Please Note that a DR site of a sub data center is mostly in passive mode while it has same hardware capacity as the primary site.)

The proposed structure makes it possible to have virtually many DR sites, for each sub center, in different physical locations; thereby decreasing the probability of failure of a service in case of any disaster as well as efficiently utilizing the DR resources. The paper is organized as follows. Section II discusses the design of the Optimal DR solution. Section III talks about the design of the Centralized DR Center (CDRC) proposed as part of the optimal DR solution. Section IV provides details on how do we achieve optimal business continuity using the proposed architecture. Finally, we conclude in Section V.

2. Design of optimal DR Solution

We propose to set up a centralized DR center (CDRC) spread across various states having capacity to support such a cause. CDRC may consist of a set of DR sites in each of the states. Each of the state may have one DR center which may cater to many sub centers active in other states. A sub center in a state or at central level may connect to CDRC through a cloud, VPN [2] or internet. An intermediate layer between an e-service and CDRC may actually form an association of the sub data center with DR sub centers in its own state or in other state depending on the quality of service demanded for that service. The quality of service such as RPO and RTO may decide the right replication strategy and optimized DR solution as proposed in [3].

As shown in Fig 1, the CDRC at national level may be distributed across various states. It is not mandatory for each state to participate in providing DR services, e.g. in Fig 1, state 4 does not have enough resources to contribute to nationalized DR centre. These state level DR centres are connected through high speed virtual private network to ensure privacy and performance.

A data center service may access centralized/nationalized DR services through cloud connectivity, VPN or Internet. The disaster planning and monitoring of the DR system for a service may be executed through certain existing DR management strategy such as in [5].

3. Design of Centralized DR center

The CDRC provides disaster recovery or service continuity solutions to various data center/government services using 'DR as a Service (DRaS)' model. Each of the sub DR centers at each of the state is similar in the infrastructure and functioning. These entire "sub DR" are connected through high speed network and together they behave like a DR cluster; if one fails other sub DR takes over.

A sub DR center consists of cluster of high performance servers, cluster of database servers, cluster of storage appliances and DR appliance. A layer of virtualization sits on top of the cluster of application servers which provides support for executing any application (SaaS) on any operating system (PaaS) installed on any infrastructure (IaaS). An abstract model for each DR sub center is as shown in Fig 2, where each of the servers shown could be a cluster of many more servers and storage based DR appliance (such as CDAC Revival 2000[7]) can be connected to cluster of servers with IPSAN appliance as storage server to provide DR services. The details of the implementation have been discussed in [9].

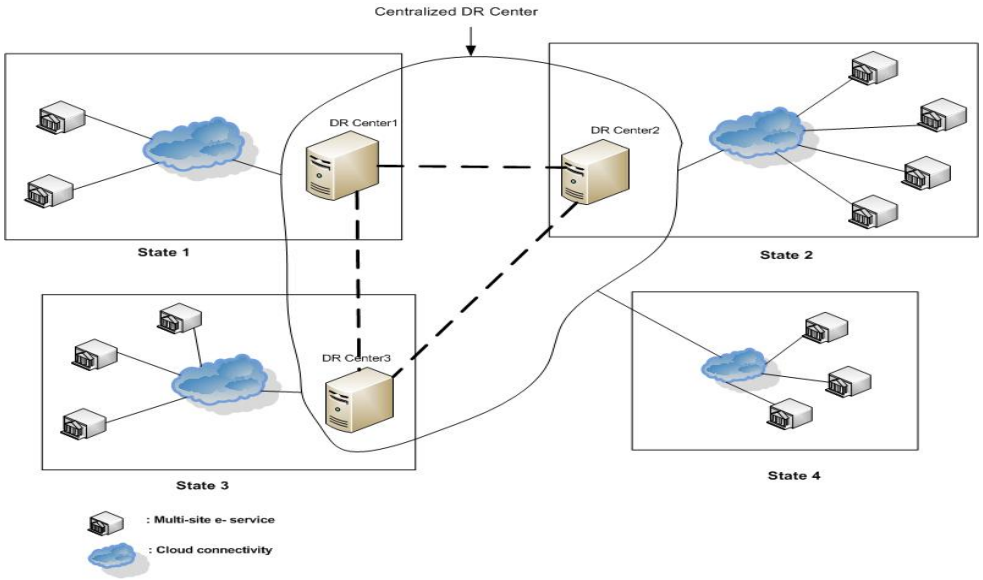

Fig. 1: Design of Optimal multi-site DR Solution for multiple sites organization

4. Working of Optimal DR Solution

To deploy DR solution, a DR appliance is put up at each of the primary site (DC) similar to TV set up boxes at homes. During normal operations, the operational data is replicated to the CDRC through the DR appliance which may get internally replicated at one or more sites within cluster of CDRC.

In case of a DC failure, CDRC will switch the user requests to one of the sub DR sites. Please note that the DC data as well as its application and OS meta data would have already been available at the sub DR site(s) through block level replication across DR appliances (Data Center and Sub DR center), therefore RPO is zero. Since the application server and database server are running in passive mode at sub-DR site, it takes negligible amount of time to switch over the application and services of the user, therefore RTO is negligible. The time taken is equivalent to activate the instance of the application through virtualization layer.

5. Conclusions

In this paper we have proposed architecture to achieve an optimal DR solution with zero RPO and negligible RTO for services and organization which are multi-location centric such as data center and e-governance services. This paper has discussed at broad level the design of the solution and one of its major components which is based on DRaaS model. The proposed solution utilizes the resources efficiently (i.e. cost effective) while promising zero RPO and negligible RTO. The simulation and implementation of the system is in progress.

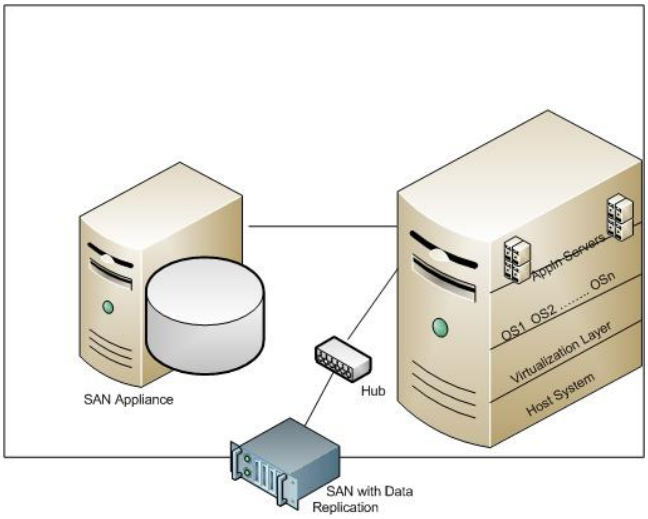

Fig. 2: Design of sub DR Center

6. References

[1] Z.H.Wu and Y. Ni, "A Disaster-Recovery IT Framework Based on Disaster Indexing Measurement Mechanism in E-Government," Proc. of International Conference on Management of e-Commerce and e-Government, 2009.

[2] H. Hiroaki, Y. Kamizuru, A. Honda, T. Hasimoto, K. Shimizu and H. Yhao, "Dynamic IP-VPN architecture for cloud computing", Proc. Information and Telecommunication Technologies (APSITT), June 2010.

[3] M. Wiboonrat1 and K. Kosavisutte, "Optimization strategy for Disaster Recovery", IEEE, 2008

[4] J. Chidambaram, C. Prabhu, P.A. Narasimha Rao, R. Wanker, C.S. Aneesh and A. Agarwal, " A methodology for high availability of data for business continuity planning / disaster recovery in a grid using replication in a distributed database", Proc of TENCON 2008 - 2008 IEEE Region 10 Conference, Hyderabaad, 2008.

[5] K.Wang1, Z. Cai2, Z. Li2 and L. Zhou1, "A Disaster Recovery System Model in an E-government System", Proceedings of the Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'05), IEEE, 2005

[6] Y. P. KongBo, L. Jinping and L. Mengxia ,"Remote Disaster Recovery System Architecture Based on Database Replication Technology", Proc. of International Conference on Computer and Communication Technologies in Agriculture Engineering , IEEE, 2010

[7] R. Singhal, S. Bokare , Y. Pal, R. Singh and P. Pawar, "Design of Enterprise Storage Architecture for Optimal Business Continuity", Journal of Electronics Science and Technology (JEST), Sept 2010.

[8] M. Wiboonrat,"An Empirical IT Contingency Planning Model for Disaster Recovery Strategy Selection" Proc. Of Engineering Management Conference, IEEE, Europe 2008.

[9] R.Singhal and S.Patankar, "Efficient model for multipoint to multipoint Disaster Recovery as a service system", Proc of ICNCC, March 2011.