Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

A SIMULATOR FOR DESIGNING DEPENDABLE STORAGE SOLUTION FOR SHARED APPLICATION ENVIRONMENT IN STORAGE AREA NETWORK

Padmini M S (Assistant Professor)[1], Babitha M[2], Manjula L N[3], Kavya M[4], Yogeetha Patel K N[5]
[1,2,3,4,5]*Dept. of Computer Science and Engineering,The National Institute Of Engineering,Mysore, India*

Abstract-The cost of data loss and unavailability can be large, so businesses use many data protection techniques for storing the data in the network to make it possible for access in different locations. This also adds up the advantage of dynamic growth of storage capacity with the changing needs. However this data on the network should be backed up to ensure the fault tolerance in the cases of storage device failure (like HDD, tape drives, etc.), system crash (server or application), etc. So how to depend on such storage or data stored in the network?! Choosing an appropriate combination of techniques is difficult because there are numerous approaches for protecting data and allocating resources.

Solution for this is by using many data protection techniques such as remote mirroring, instant copies, LUN masking and concurrent access in shared application environment.

I. INTRODUCTION

The Storage Area Network (SAN) technology introduces a concept called intelligent disk sub-system (IDSS).This IDSS consists of the various methodologies for backing up the data stored on to the servers, amongst which following are three major methods for achieving the fault tolerance[1].

Instant copying technique in this context is the process of copying/backing-up the huge amount of data in very less time. This is done to speed-up the backup process and to maintain the copied data for use in time of crashes.

Remote mirroring in IDSS is the way of copying or backing-up the data in are most replaces such as a data center or a storage server in a distant location. This is used to make use of dynamic storage capacity and to utilize the complete (most possible) storage space in a server.

In synchronous remote mirroring[1], server gets the acknowledgment from storage disk system as soon as disk sub system receives the data without needing the server to wait for copying this data to secondary disk sub system.

In asynchronous remote mirroring[1], server sends data to 1st disk system. Now this data is forwarded to 2nd disk system. After storing this data, 2nd system sends acknowledgment to 1st system. First disk sub system then acknowledges the completion of data to the server.

Hybrid remote mirroring combines both the above mentioned techniques to provide backing-up of data. First half consists of synchronous and the second half, the asynchronous remote mirroring to provide faster response to server and high level of fault tolerance using 3rd staged storage.

Logical Unit Number (LUN) masking in IDSS provides the two ways of configuration of servers with the disk systems to facilitate the security of data stored in the shared disk sub system.

II. DESIGNING DEPENDABLE STORAGE SYSTEMS

Our goal is to find the best storage solution, which is the one that minimizes overall costs; including infrastructure out- lays, as well as penalties for application downtime and data loss.

The solution to this problem specifies
1) A combination of data protection and recovery techniques for each application workload (e.g., remote synchronous mirroring, local snapshots, and local backup), 2) how those data protection techniques should be configured (e.g., how frequently snapshots and backups are taken). To understand how the design tool makes choices among design alternatives, this section describes the design space and all the parameters used to prescribe a particular design. We begin by describing how we model the design space, including the data protection and recovery techniques, application workload characteristics, device infrastructure, and failure scenarios. We then describe how the cost of a particular solution is computed and provide a precise description of the problem we solve, in terms of this design space.

1 Data Protection and Recovery Techniques
In order to protect applications against data loss and unavailability, it is necessary to make one or more secondary copies of the data that can be isolated from failures of the primary data copy. Although standard redundant hardware techniques such as RAID are used to protect data from internal hardware failures, they are not sufficient to protect data from other kinds of failures such as human errors, software failures, or site failure due to disasters. The geographic distribution of secondary copies (e.g., through interarray mirroring [4], [5] or remote vaulting) provides resilience against site and regional disasters. Point-in-time [6] and backup [7], [8], [9] copies address application data object errors like accidental deletion and software failures due to buggy software or virus infection by permitting restoration of a previously consistent copy. Those data protection techniques can be combined to provide a more complete coverage for a broader set of threats. After a failure, application data can be recovered either by restoring one of the secondary copies at the primary site or a secondary site or by failing over to a secondary mirror. For the restoration case, data is copied from the secondary copy to the target site. For failover, the computation is simply transferred to the secondary mirror, without any data copy operations. Failover requires a later failback operation (performed in the background) to copy data and transfer computation back to the target site.

2 Failure Model The primary copy of an application's data set faces a variety of failures after deployment, including hardware failures, software failures, human errors, and site and regional disasters. A failure scenario is described by its failure scope or the set of failed storage and interconnect devices. Examples include primary data object failure, primary disk array failure, and primary site disaster. A primary data object failure indicates the loss or corruption of the data due to human or software error without a corresponding hardware failure. Each failure scenario also has a likelihood of occurrence, which describes the expected annual likelihood of experiencing that failure. We assume that primary disk array failures and primary site disasters are detected immediately and that the desired point of recovery is the most recent point in time. For primary data object failures, we assume that there is a delay between the failure and the discovery of the failure (e.g., due to user error). The desired point of recovery is the time (in the past) of the failure. For any failure, we assume that the recent data loss is the failure detection delay (i.e., the updates made after the failure) plus any additional updates lost due to recovery from a point-in-time copy that is out of date, relative to the desired recovery point. For instance, the failure may have occurred just before a backup, resulting in the loss of all updates since the previous backup. Failed applications incur penalty costs due to the unavailability and loss of data. We model these penalties as described in [17]. In particular, a data outage penalty rate describes the cost (e.g., in US dollars per hour) of data unavailability. After a failure, data is recovered from a secondary copy, which may be out of date relative to the time of the failure, thus implying the loss of recent updates. The recent data loss penalty rate describes the cost (e.g., in US dollars per hour) of recent data loss.

III. Existing System

The existing system does not provide efficiency over the shared application environment. In the IEEE paper on remote mirroring done write data mirroring is a classic technique for tolerating failures by keeping two or more copies of important information, access can continue if one of them is lost or becomes unreachable. The design for remote mirroring are complicated by competing goals keeping the copies as closely synchronized as possible, delaying foreground writes as little as.

IV. Proposed system

The proposed system provides reliable and efficient access through the shared application environment in storage area network. Sans are designed to enable centralization of storage resources, while at the same time overcoming the distance and connectivity limitations posed by directly attached storage. This data on the network should be backed up to ensure the fault tolerance in the cases of storage device failure, system crash. So to depend on such storage or data stored in the network the storage area network with intelligent disk sub-system and added security to avoid the errors in shared application environment. The storage area network (san) technology introduces a concept called Intelligent Disk Sub-System (IDSS). This IDSS consists of the various methodologies for backing up the data stored onto the servers that they achieve fault tolerance. Instant copying technique is the process of copying/backing- up the huge amount of data in very less time. This is done to speed-up the backup process and to maintain the copied data for use in time of crashes. Remote mirroring is the way of copying or backing-up the data in remote possible, maintaining accessibility in the face of as many failure types as possible, and using as little expensive inter-site network bandwidth as possible.

In the IEEE transactions on dependable and secure computing the costs of data loss and unavailability can be large, so businesses use many data protection techniques such as remote mirroring, snapshots, and backups to guard against failures. Choosing an appropriate combination of techniques is difficult because there are numerous approaches for protecting data and allocating resources.

In the IEEE transactions on parallel and distributed systems, vol. 22, no. 2[16][15], design and partitioning method this paper proposes a few file domain partitioning methods designed to reduce lock conflicts under the extent-based file locking protocol. Experiments from four i/o benchmarks on the ibm gpfs and luster parallel file systems show that the partitioning method producing minimum lock conflicts wins the highest performance. The benefit of removing conflicted locks can be significant that more than thirty times of write bandwidth differences are observed between the best and worst methods places such as a data center or a storage server in a distant location. This is used to make use of dynamic storage capacity and to utilize the complete storage space in a server. Logical Unit Number (LUN) masking provides the two ways of configuration of servers with the disk systems to facilitate the security of data stored in the shared disk subsystem.

V. MODULES

Instant copy:

Instant copies can copy several terabytes of data within a disk subsystem in a few seconds. The original data is practically copied in a few second,then server 2 can work with the data copy, meanwhile server 1 continues to operate with the original data[10][12].

Remote mirroring:

Synchronous remote mirroring an acknowledge is send to the user after storing data in both local system and remote system. Asynchronous remote mirroring an acknowledge is send to the user as soon as data is stored in system. Hybrid remote mirroring is the combination of both synchronous and asynchronous[13][14].

LUN masking:
LUN masking limits accessing towards hard disk that subsystem exports to connected server by assigning logical number to each server which are connected to a disk subsystem, so that only the respected server will have access to the assigned hard disk.port based LUN masking is the poor man's LUN masking.it is found in low-end disksubsysytem.in port based LUN masking the filter only works using the granularity of the port.this means that all servers connected to the disk subsystem via the same port sees the same d isk.server bsed LUN masking offers more flexibility.in this approach every server sees only the harddisk assigned to it,regardless of which port it is connected via or which other servers connected via the same port[10][13].

Concurrent access:
It is the process in which user request for the data ,two or more users can request for the reading the file from the server concurrently, access is permitted to all the user, if any of the user request for a write server checks for the read/write of the file requested, if there is hold in a request it wait until the realize of lock, finally it locks the file and access the file.

VI. CONCLUSION

Today disksubsystem can be constructed so that they can withstand the failure of any component without data being lost or becoming inaccessible
This project helps in the understanding the creation of interactive technologies used to implemented it the building of the project has given me a precise knowledge about how it connects to the disksubsystem

REFERENCES

[1] Storage Networks: The complete Reference, Robert Spalding,Tata McGraw Hill,2003.
[2] Information Storage and management,EMC education services,wlley India 2009 , G Somasundaram,Alok,Srivatsava.
[3] Storage Networking fundamentals Marc Farley, Cisco press, 2005
[4] M. Ji, A. Veitch, and J. Wilkes, "Seneca: Remote MirroringDone Write," Proc. Usenix Ann. Technical Conf. (USENIX '03),pp. 253-268, 2003.
[5] R.R. Schulman, Disaster Recovery Issues and Solutions, white paper, Hitachi Data Systems, http://www.hds.com/pdf/ wp_117_02_disaster_recovery.pdf, Sept. 2004.GAONKAR ET AL.: DESIGNING DEPENDABLE STORAGE SOLUTIONS FOR SHARED APPLICATION ENVIRONMENTS 379
[6] A. Azagury, M.E. Factor, and J. Satran, "Point-in-Time Copy: Yesterday, Today and Tomorrow," Proc. IEEE/NASA Conf. Mass Storage Systems (MSS '02), pp. 259-270, Apr. 2002.
[7] A. Chervenak, V. Vellanki, and Z. Kurmas, "Protecting File Systems: A Survey of Backup Techniques," Proc. IEEE/NASA Conf. Mass Storage Systems (MSS '98), pp. 17-31, Mar. 1998.
[8] HP OpenView Storage Data Protector Administrator's Guide. Hewlett-Packard Development, mfg. Part Number B6960-90106, Release A.05.50, Oct. 2004.
[9] W.D. Zhu, J. Cerruti, A.A. Genta, H. Koenig, H. Schiavi, and T.Talone, IBM Content Manager Backup/Recovery and High Availability:Strategies, Options and Procedures. IBM Redbook, Mar. 2004.
[10] Storage Area Network essentials :A compleate guide to understanding and implementing SAN ,Richard Barker and Paul Massiglia,John Wiley India,2002.
[11] Www.tectarget.com
[12] Information storage and management, emc education services, wileyindia 2009,gsomasundaram,alok,srivatasava Storage networking fundamentals marc farely,cisco press,2005.
[13] Seneca: remote mirroring done writeIeee transactions on dependable and secure computing,vol. 7, no. 4, october - december 2010
[14]Minuet: rethinking concurrency control in storage area networks
[15] Ieee transactions on parallel and distributed systems,vol. 22, no. 2, february 2011 design and partitioning methods
[16] Ieee transactions on parallel and distributed systems,vol. 22, no. 7, july 2011the small world of file sharing
[17] K. Keeton, C. Santos, D. Beyer, J. Chase, and J. Wilkes, "Designing for Disasters," Proc. Third Usenix Conf. File and Storage Technologies (FAST '04), pp. 59-72, Mar. 2004.