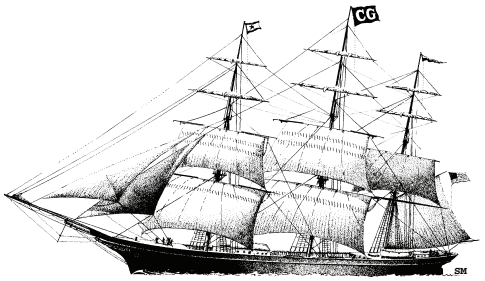
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2007084 August 24, 2007

Continuity Software's RecoverGuard Closes the Gap on Disaster Recovery

Analyst: Michael Fisch

Management Summary

A disaster recovery (DR) system for an enterprise is like a parachute in that people depend on it to work at the moment it is needed. Imagine jumping out of an airplane at 13,000 feet and freefalling toward the earth. The jumper accelerates until reaching terminal velocity – about 120 miles per hour – and the ground below draws nearer by the second. He pulls the rip cord to open the parachute that will carry him gently to the ground. If it is slow to deploy, perhaps by a few seconds, that is alright because there is a margin of error. But if the chute is a few *minutes* late to deploy, well, no one wants to think of that eventuality. A parachute must work fully when it is needed, similar to a disaster recovery system. Too little or too late is not acceptable.

Continuity Software's *RecoverGuard* is a software tool that ensures remote replication DR systems work reliably. You may be surprised to know that even expensive, sophisticated DR systems suffer from reliability issues caused by day-to-day changes in the IT environment. In the course of normal maintenance and expansion, administrators make configuration changes to servers, storage, databases, and networks. If a change at the production site is not immediately and precisely applied to the target site, a DR gap or vulnerability results that may cause the affected applications not to restart in the event of a failover. Like the parachute that is several minutes late to deploy, applications that are late to restart can have a large negative financial impact on an enterprise.

Read on for details about how RecoverGuard closes the gap on disaster recovery.

Disaster Recovery Gaps

A DR system enables business operations to resume quickly in the event of a system failure or disaster, such as a fire, flood, or power outage. A system typically involves replicating data in real time[1] from a production data center (source) to a remote site (target) with standby servers, storage, and networks. If the production data center fails, the remote site can take over operations until the problem is fixed, at which point it transfers back to the production site. This setup provides data and system redundancy as well as geographical remoteness to protect against local and regional disasters.

The challenge is to maintain the DR system in a continuous state of readiness. Why is this so difficult? Because routine changes in the IT environment can create DR gaps or vulnerabilities that hinder the failover process. The production and remote data centers must be configured similarly for a smooth failover. If not, it falls out of tune like a guitar and a harmonious transition cannot occur.

IN THIS ISSUE

[1] Synchronous or asynchronous replication

Examples of DR gaps include:

- The passive node on a cluster is not mapped to the correct disk volume, so an automatic failover stalls.
- The replication of a multi-volume file system or database is not synchronized; hence, the data on the replicas is not consistent.
- Multi-volume databases or file systems use different replication technologies and/or storage systems. The result is slower application performance and remote disk volumes that are not in sync (i.e., not consistent).
- Some disk volumes containing database data files are replicated to the remote site while others are not. In this case, the database is not fully protected and a restart on the remote site may fail.
- Some of the replicated volumes associated with a file system or a database are mapped to the wrong host, which can lead to data corruption as well as a failed restart.
- A standby host server is incorrectly configured for accessing storage devices, network file systems, domain server, etc. Upon failover, the standby host will not have access to the data or, in the worst case, will corrupt the replicated data.
- A host server is mapped to storage volumes that have not been accessed in a long time and, in fact, are no longer needed. Perhaps they were once used for testing and development. These devices can be reclaimed and reused.
- The data in a multi-volume file system or database is not stored in the same RAID type or volumes are not configured with the same number of storage paths. Like the weakest link in a chain, application performance will slow according to the slowest volume in the group.

(The last two are not DR gaps per se, but examples of inefficiency that RecoverGuard can detect.)

DR gaps are correctible, but you first must know they are there. This is not easy to do in a complex and evolving enterprise IT environment. Although replication methodologies and technologies are mature, tools for change management in such environments are lacking and, in many situations, several technologies are used concurrently, making it difficult to manage changes smoothly and spot DR gaps. Periodic testing and auditing are too costly and infrequent to ensure constant state of DR readiness.

RecoverGuard

RecoveryGuard by Continuity Software a software tool that automatically exposes DR gaps, so enterprises can correct them and greatly improve their ability to recover from a disaster. RecoverGuard periodically and automatically scans storage, servers and clusters, databases, and replication solutions. It maps dependencies and generates a graphical topology of the environment. Then, it checks the results against a knowledge base of over a thousand vulnerability signatures, which is continually updated by Continuity's research lab and distributed to customers. RecoverGuard's output is a list of specific vulnerabilities ranked by severity. It provides a holistic dashboard view so administrators can manage the process of closing DR gaps.

Additionally, RecoverGuard provides a view into storage and SAN utilization, so enterprises can improve utilization and better leverage their IT investments.

In the first release, RecoverGuard supports:

- All mainstream server platforms except mainframes
- All mainstream databases
- EMC and NetApp storage systems

The following release will also include IBM, HDS, and HP storage systems. The price of RecoverGuard is based on the number of server CPUs – $2,000 per CPU, at list price.

Benefits to the Business

Placing a value on a solid, reliable DR system is difficult because, when it is needed, it is virtually priceless. It can literally save the business in the event of a fire, flood, storm, outage, massive system failure, and the like. Like wearing a seatbelt in a car or buying a life insurance policy, one hopes it is not ultimately necessary, but common sense says it is better to be safe than sorry.

Conclusion

If your enterprise is spending hundreds of thousands or millions of dollars on DR technology, you want to know it will work fully when it is needed. However, DR gaps and vulnerabilities can hinder its ability to perform a failover. The worst part is that you often do not know they are there until it is too late. We highly recommend considering a solution like Continuity Software's RecoverGuard that enables you to discover and correct DR gaps. It can ensure the effectiveness of your DR investments and safeguard your business.

About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Michael Fisch **is Director of Storage and Networking for The Clipper Group.** He brings over ten years of experience in the computer industry working in sales, market analysis and positioning, and engineering. Mr. Fisch worked at EMC Corporation as a marketing program manager focused on service providers and as a competitive market analyst. Before that, he worked in international channel development, manufacturing, and technical support at Extended Systems, Inc. Mr. Fisch earned an MBA from Babson College and a Bachelor's degree in electrical engineering from the University of Idaho.

- ***Reach Michael Fisch via e-mail at mike.fisch@clipper.com or at 781-235-0085 Ext. 211. (Please dial "211" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group** *Captain's Log*, **The Clipper Group Voyager,** **Clipper Notes**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.