THE CLIPPER GROUP
Navigator™
Navigating Information Technology Horizons℠
Published Since 1993 Report #TCG2008016 March 7, 2008

Continuity Software Launches DR Assurance Service as Complement to RecoverGuard

Analyst: Michael Fisch

Management Summary

What if you went to the doctor for your annual physical, had the requisite battery of tests (blood work, etc.), and went home, never to hear about the results? You would have achieved your first goal, which was to have the physical. However, you would have failed a more important goal, really knowing whether you have an undiagnosed problem. You might assume that if your doctor did not call, all is OK, but would you like to rely on silence (or lack of follow up) to be your indicator of good health? Not these days, with overburdened and overbooked medical staffs – silence may not be golden. Not going the last ten yards to cross the goal line means that your efforts to get down the field were for naught.

The same is true for preparing for disaster recovery (DR) planning in your IT organization. You may have gone to the expense and trouble of implementing a DR program but if you don't follow up with the reports that indicate potential vulnerabilities, then you may be at risk and not be aware of it. Ignoring the problem may be blissful (out of sight is out of mind) but the enterprise may be exposed.

Continuity Software recently announced a new *DR Assurance Service* as a complement to its *RecoverGuard* disaster recovery monitoring software solution. The DR Assurance service dedicates a team of DR experts to review and analyze clients' RecoverGuard reports and alert the appropriate personnel when vulnerabilities arise. Clients get the opportunity to correct misconfigurations before they cause problems in an actual recovery situation. This service further simplifies the task of maintaining DR readiness. Read on for details.

RecoverGuard for DR Readiness

Is your enterprise prepared for a timely and complete recovery in the event of a disaster? RecoverGuard is a software tool that allows enterprises to answer this question with a confident *yes* instead of an uncertain *maybe*. RecoverGuard represents the last 10 yards of a DR solution. While it does not provide replication and failover, which is the domain of many DR solutions available today, it enables these solutions to work reliably by tracking and reporting configuration faults and errors that are so common in DR environments. It identifies these hidden problems and gives administrators a chance to correct them well before they become a hindrance in actual recovery situations.

DR solutions provide recovery from system failures or local and regional disasters, such as a fire, flood, or power outage. They protect critical data and the IT applications and businesses processes that depend on it. A system typically involves replicating data from a production data center (source) to a secondary 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.

IN THIS ISSUE

This is an excellent approach for protecting enterprise data, though it has a hidden, soft underbelly: Day-to-day changes to the production environment that are not applied simultaneously and/or correctly to the secondary site can create faults causing recoveries to stall or fail. Such configuration changes may be as normal and mundane as adding storage capacity or volumes. If the secondary environment becomes out of sync, such as when volumes and replicas not mapped correctly, there will be unanticipated delays in recovery or even data loss. This downtime can lead to serious productivity and economic losses.

Maintaining a continual state of DR readiness requires automated software that gives regular visibility into potential problems so administrators can resolve them. DR testing by itself is not sufficient because it cannot be done frequently enough. Realistically, enterprises can only test every three or six months, while DR faults may arise daily.

RecoverGuard is agent-less and draws on a knowledge base of over 1,600 gap or vulnerability signatures for scanning a DR environment. Engineers at Continuity Software regularly revise this descriptive signature list based on testing and customer input. It also includes signatures that flag underutilized and un-optimized resources, so customers can better utilize their existing storage and network assets.

DR Assurance Service

If RecoverGuard represents the last ten yards of disaster recovery, the DR Assurance Services takes the ball over the line. It provides a team of DR experts to review and analyze the daily reports generated by clients' RecoverGuard installations. Most significantly, it screens this information for urgent issues and alerts the appropriate client personnel by phone and e-mail when one arises. Clients then have the opportunity to respond and fix vulnerabilities in a timely manner.

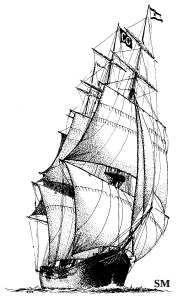
The DR Assurance Service also generates monthly and quarterly summary reports and offers conference calls and meetings for review. Clients can therefore understand the impact of noncompliant configurations and ways to resolve them. They can see trends and improvements and make sure an adequate state of DR readiness is maintained.

This service targets busy IT departments that need assistance in monitoring their DR status, perhaps because they lack the personnel or expertise to dedicate to this area. It gives them access to Continuity Software's experts and best practices. This service is also helpful for less-technical IT managers as well as information security and business continuity professionals responsible for data protection, business continuity and disaster recovery (DR) initiatives that want to understand and stay current on DR readiness. The list price of the DR Assurance Service is $3,200 annually per protected server.

In addition to this ongoing professional service, Continuity Software offers an introductory 48-hour "no-risk" assessment service that demonstrates to prospective customers where their actual vulnerabilities lie. Upon seeing the gaps in their DR infrastructure, Continuity claims the clear majority of participants decide to install RecoverGuard.

Conclusion

DR vulnerabilities are like weeds in a garden. Despite IT departments' best efforts at change management, they pop up spontaneously and need to be removed. RecoverGuard takes the first step and identifies them. The new DR Assurance Service then makes you aware of them in a timely manner. Together, they deliver a valuable solution for DR readiness and business continuity.



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 eleven 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.