THE CLIPPER GROUP
Navigator™
Navigating Information Technology Horizons℠
Published Since 1993 Report #TCG2009012 Friday, March 13, 2009

Continuity Software's RecoverGuard, Disaster Recovery and High-Availability Assurance, and Your Job Security

Analyst: Michael Fisch

Management Summary

Continuity Software is announcing version 4.0 of *RecoverGuard*, a solution for disaster recovery (DR) and high availability (HA) monitoring and assurance.

RecoverGuard automatically detects gaps and vulnerabilities in DR and HA readiness that result, usually unnoticed, from routine changes or misconfigurations in the IT environment. It solves a serious problem that many enterprises have, even those with multi-million dollar systems. Namely, that the data protection and failover (e.g., server clusters, etc.) environment becomes out of sync with production, risking longer recoveries and data loss or inconsistency in the event of a disaster.

Major enhancements in RecoverGuard v4.0 include:

- High availability cluster verification
- Automatic detection of configuration drifts that affect DR/HA servers
- Identification of the infrastructure changes that created the problems, and suggested solutions for avoiding them in the future
- Deployment analysis – the ability to find and report IT assets that require protection, but do not currently have any level of protection at all

The Stakes are High

Today is Friday the 13th. Some believe this is an unlucky day and take precautions to avoid misfortune, even going so far as to stay home. While we are not inclined to this superstition, it is a good idea in general to take precautions to avoid disaster, especially when the stakes are high.

The stakes are incredibly high when it comes to enterprise high availability, data protection, and business continuity. This is the ability of an enterprise to take a hit and keep going – without inordinate loss or outright failure. A DR/HA system should enable IT applications and their associated business processes to resume quickly and accurately when a system failure or disaster occurs due to a fire, flood, virus, power outage, or even just a simple human error. These things do happen, out of the blue, and not necessarily on visibly unlucky days.

The traditional approach of DR/HA testing alone is insufficient, because it is a disruptive and costly exercise that cannot be done frequently or thoroughly enough to catch all of the problems that arise. Therefore, an intelligent, automated solution like RecoverGuard is now the preferred approach. It is both effective and efficient from a time and financial standpoint.

IN THIS ISSUE

Job Security in Challenging Times

The stakes are also high for the IT managers and CIOs in charge of DR/HA systems. It goes without saying that if a recovery failed and an enterprise suffered significant losses, it would reflect poorly on those responsible. Some call that a CLA or career-limiting action.

- Do you know for certain that a recovery would succeed, from both a recovery time and recovery point objective (RTO and RPO), if a disaster were to occur today, next week, or next month?

From a more positive perspective, involving yourself or even leading a DR/HA assurance initiative could improve your job security in these difficult economic times. Many feel concerned about their jobs, and no one wants to be cut in the next downsizing.

There are two schools of thought about how to manage job security in times like these:

1. *Keep a low profile, take no risks, and do not rock the boat.*
2. *Raise your profile and make yourself indispensable.*

The first is the path of least resistance, which alone makes it suspect. It advocates being a wallflower that managers do not notice. But who thinks twice about laying off a wallflower? It means that managers making headcount decisions may not see you adding value to the company or helping it to be competitive. This approach leaves no strong impression or sense of gravity with which they must contend.

On the other hand, taking action to make yourself visible in a positive way does leave an impression. Furthermore, the most valuable projects and initiatives, and the jobs associated with them, are relatively sheltered even in difficult times. Involving yourself in one is smart.

Consider this scenario: You bring attention to the fact that routine changes in the enterprise's complex IT environment could unknowingly cause the failover system to be out of sync with production, and that the DR and/or HA systems on any given day may not work as intended. Suggest an automated DR/HA assurance solution that will generate a list of specific gaps and vulnerabilities, as well as recommended solutions. Make this list known to management and be part of the solution to find and remedy gaps and vulnerabilities on an ongoing basis. Bottom line, you are ensuring your company's data protection and business continuity strategy.

- **Congratulations, you just went from wallflower to hero, perhaps even making yourself indispensable.**

RecoverGuard 4.0

The new version of RecoverGuard offers more complete recovery assurance by monitoring a wider variety of IT equipment and components. It extends coverage to server clustering, server hardware (i.e., CPU, memory, NIC, HBA), operating systems, patches and service packs, packages, storage routing, and (eventually) kernel parameters, domain and DNS settings, and services. RecoverGuard 4.0 also automatically identifies IT assets and performs root cause analysis of gaps and vulnerabilities.

Conclusion

Many enterprises are adopting RecoverGuard because it solves a serious and tangible problem for data protection, high availability, and business continuity. This new version offers a more complete solution for DR/HA assurance. It is worth considering – for the sake of business continuity *and* job security.

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 12 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

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.