Case Study

How Spain's General Comptroller Office Ensures 24x7 Business Continuity

This case study examines the disaster recovery (DR) and high availability (HA) challenges surrounding the need to protect and ensure the continuous availability and performance of critical data center operations at Spain's General Comptroller of the State Administration Office. The case study analyzes the benefits gained by implementing RecoverGuard™ to continuously assess HA/DR readiness, avoid system downtime and data loss, and optimize HA/DR investment.

Background: Commitment to 24x7 service availability

The General Comptroller of the State Administration in Spain (Intervención General de la Administración del Estado, or IGAE) is tasked with providing transparent, reliable, complete and independent accounting information concerning the public administration.

In light of the national importance of its services, and in line with its commitment to complete transparency to the public through pioneering technologies including online access, the General Comptroller Office has been setting very high standards for 24x7 service availability.

The IT Environment

The General Comptroller has put tremendous effort and skill into the design of IT solutions that provide maximum service availability and data protection. The results are state-of-the art facilities with a data center architecture that consists of production and DR sites connected by fiber optics with continuous data replication.

The production environment is based on a central Hitachi storage, Unix and Windows servers (with increasing use of virtualization), and various database tools. Data protection relies on continuous replication and Point-in-Time storage-based technologies. Availability is achieved through extensive use of local and geo-clustering including Veritas Cluster Server, MSCS, and SRM.

"With RecoverGuard in place, the uncertainty factor has been eliminated and we now feel more confident that the IT infrastructure configuration is aligned with our HA/DR recovery goals."

Manuel Alonso
Head of IT Systems and Infrastructure of the Sub Directorate of Operations

General Controller of the State Administration
(Intervención General de la Administración del Estado)

Challenges

Given the criticality of its data center operations, the General Comptroller Office has defined strict Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). RTO refers to the acceptable amount of time to restore operations, while RPO refers to the amount of data that can be lost without significantly affecting the organization. These RTO and RPO therefore define the organization's backup, replication, and other DR requirements.

With daily changes to the IT environment (critical patches, updates, new storage allocation, server refresh, etc.), the readiness of the recovery environment must be continually re-verified. The General Comptroller's IT department has traditionally addressed this need by performing regular DR tests and frequent audits of the recovery configuration.

Without automation, however, these tasks were extremely resource-consuming, and could potentially disrupt systems' availability. With the industry average frequency for a complete DR test being just once a year, the people in charge at the General Comptroller Office were determined to find an innovative way to ensure a higher level of confidence in their 24x7 availability.

To this end, the IGAE decided to look for solutions that would assure readiness and compatibility between the production and DR sites in a consistent and automatic manner. From the several solutions that were evaluated, Continuity Software's RecoverGuard™ was chosen as most suitable and easiest to implement.

The Solution: RecoverGuard

Continuity Software's RecoverGuard was selected to provide the General Comptroller Office with the following key capabilities to ensure ongoing data protection, disaster recoverability, and business continuity:

IT discovery and scanning. RecoverGuard automatically and continually scans the IT environment and unobtrusively collects critical configuration data from key IT assets, including storage, servers, virtual environments, and databases.

Risk detection. RecoverGuard identifies and reports on more than 4,900 known vulnerabilities that can pose downtime or data-loss risk to the IT infrastructure. It then alerts the appropriate IT resources via email or directly through the organization's ticket management system.

Visualization and reports. When users are alerted to a risk, RecoverGuard allows them to drill down and investigate the relevant IT infrastructure configuration status, as well as any previously discovered data protection and disaster recovery gaps (SLA compliance and exceptions, change and audit reports, and configuration changes trend analysis).

Optimization. Leveraging the data center topology map to detect under/over utilized assets, RecoverGuard enables the organization to fine-tune resources and maximize the value of its infrastructure investment.

Cross-environment support. RecoverGuard supports all major platforms, operating and storage systems (e.g. EMC, HDS, IBM, HP, NetApp) and replication solutions (both storage and database level), and integrates with the leading Configuration Management Databases (CMDB). It can also identify and address host configuration gaps and other risks in VMware and other virtualization environments.

In addition to the RecoverGuard™ software, Continuity Software provides DR Assurance, a Web-based service that remotely monitors the customer's environment for disaster recovery and high availability vulnerabilities.

Results and Benefits

"Immediately following the short deployment, RecoverGuard started to demonstrate a clear improvement in our processes and readiness," says Manuel Alonso, Head of IT Systems and Infrastructure of the Sub Directorate of Operations of the General Comptroller Office. "It also provided valuable suggestions for improving our HA/DR infrastructure and maximizing our investment."

The benefits extend significantly beyond the initial scan, however, as RecoverGuard™ continuously detects configuration gaps, prioritizes them and reports in an actionable way. This allows the IT team to immediately mitigate risks and dramatically reduce the time and effort involved in identifying root-cause and maintaining a high state of readiness.

The results are noticeable:

- Reduction in daily workload for HA/DR validation
- Proactive risk management that leads to improved service availability
- Smooth and successful DR testing
- Visibility to RPO and RTO metrics and a single-pane-of glass to show IT readiness at any given time

"With RecoverGuard™ in place, the uncertainty factor has been eliminated and we now feel more confident that the IT infrastructure configuration is aligned with our HA/DR recovery goals," adds Manuel Alonso.

In addition to RecoverGuard, the General Comptroller Office has been using the DR Assurance service, which provides quarterly reports summarizing all events, configuration gaps and errors, as well as recommendations for improving the efficiency of DR and data protection operations and processes.

Conclusion

Despite heavy investments in building and maintaining disaster recovery and high availability environments, many organizations are struggling to ensure their service availability objectives are met in a consistent manner.

Given the criticality of its data center operations, the General Comptroller Office has defined strict DR objectives, which to a large extent could not be met without the proper tools to frequently and thoroughly test DR readiness.

By using Continuity Software's RecoverGuard to automate DR testing and monitoring, the General Comptroller Office has been able to significantly improve its ability to maintain its business continuity objectives while improving the effectiveness of DR operations.