7 Menachem Begin Rd Ramat Gan 52681 Israel Tel. +972 3 68 71 727 Fax. +972 3 68 71 720 www.idc.co.il

CASE STUDY

BBVA Implements Continuity Software's RecoverGuard to Gain Improved Control Over Its DR/HA Environment

Sponsored by: Continuity Software

Dan Yachin

April 2012

IDC OPINION

Disaster recovery (DR) and high availability (HA) are top priorities for organizations of all sizes. Driven by the need to ensure business continuity and comply with data protection policies and regulatory requirements, DR/HA is a major area of IT spending. However, in light of the dynamic nature of datacenter configuration changes and the complexity of DR implementations, it is becoming increasingly difficult to ensure critical data and business processes are successfully recoverable at all times.

As one of the largest financial institutions in the world, BBVA deals with IT infrastructure that is constantly growing and diversifying. BBVA has therefore been faced with the challenge of effectively controlling its DR/HA environment while ensuring consistent readiness. To address this issue, among others, the company chose Continuity Software's RecoverGuard to automate DR/HA management processes and gain immediate visibility into configuration gaps between primary production and disaster recovery sites. As a result, BBVA has been able to improve operational efficiency and remove one of the major and most common causes of DR and availability failures: a lack of timely identification of impending risks.

IN THIS CASE STUDY

This IDC Case Study discusses BBVA's use of Continuity Software's RecoverGuard to address DR/HA risks. It analyzes BBVA's business continuity challenges and how RecoverGuard helped tackle them while enabling a proactive approach to identify and fix problems before they escalate and disrupt critical revenue-generating services.

SITUATION OVERVIEW

Organization Overview

Headquartered in Spain, BBVA is a global provider of financial and non-financial products and services for individual and corporate customers. Founded in 1857, the group employs more than 110,000 people in 7,457 branches in 32 countries around the world and has more than 50 million customers and 900,000 shareholders. It is the 15th largest commercial bank operating in the U.S. and has a strong presence in Europe, as well as in emerging markets such as Latin America, China, and Turkey. In 2011, BBVA recorded EUR 4.01 billion in net attributable profit and EUR 20.5 billion in gross income.

BBVA is recognized as one of the most technologically advanced financial institutions in the world. In 2011, it spent EUR 2.15 billion on ICT, out of which over 40% was dedicated to new technologies as part of BBVA's strategy to transform its business model and improve the customer experience by making its services accessible from anywhere at any time. Specifically, the company focuses on the development of non-branch or alternative channels such as the Internet and smartphones as a main competitive advantage.

BBVA is also making significant investments into cloud, mobile, and social technologies to improve internal collaboration and communication. It recently signed a major agreement with Google to start using Google Apps (Google Docs, Google Sites, Gmail, and Google Calendar). The deal, the biggest Google Apps contract so far, aims to help BBVA's employees collaborate more easily, regardless of location.

Challenges and Solution

The transformation of BBVA's IT infrastructure to support the group's business objectives has had a substantial impact on its business continuity plan. BBVA uses a DR/HA architecture based on the replication of critical data and the availability of servers shared with other services. Due to growing diversity and the number of systems encompassed by the DR/HA strategy, the group needed to optimize the process of managing service continuity while ensuring compliance with disaster recovery objectives driven by internal policies and regulatory requirements. In particular, BBVA was looking for efficient ways to proactively detect and mitigate risks related to unprotected components, missing replication, and recovery service level-agreement (SLA) breaches such as recovery point objective (RPO) and recovery time objective (RTO) violations. This challenge was further compounded by BBVA's increasing reliance on its IT infrastructure to support business-critical customer-facing services and the rapid pace of change in this dynamic environment.

To address its growing DR/HA needs, BBVA looked for solutions to simplify and automate the management, analysis, planning, implementation, and maintenance of

recovery plans, as well as the periodic tests of the systems that are within the backup and recovery strategies (BRS) functions.

Continuity Software's RecoverGuard – which is designed to ensure business continuity and to mitigate data protection, recovery, and availability risks – was among the solutions BBVA reviewed. The product detects data protection vulnerabilities and configuration gaps and alerts users to potential risks before they impact critical business services.

RecoverGuard uses an agentless technology to scan production and replication infrastructures to collect configuration data from key IT assets and calculate dependencies and relationships between applications, databases, file systems, servers, storage volumes, and replicas. It then searches through the results for known gaps and vulnerabilities. When potential data protection, availability, or disaster recovery risks are detected, a ticket containing the details regarding the severity of the problem and how to resolve it is automatically issued.

In addition, RecoverGuard can be used for optimization, such as detecting under-/over-utilized assets, which enables organizations to fine-tune resources. Reporting and analytic capabilities are also provided to enable deeper examination of the IT infrastructure configuration status, as well as into previously discovered data protection and disaster recovery gaps. Customers can use the product to produce audit reports that include configuration changes and trend analysis, as well as business service recoverability and SLA compliance statuses.

According to Antonio Castillo, who is responsible for BRS for BBVA across Europe, an initial scan using RecoverGuard yielded significant results. "The pilot with RecoverGuard was very satisfactory, since we were able to identify possible risks in our current DR/HA strategy, making it easier for us to anticipate further risks and establish proactive measures prior to contingency tests and simulations," Castillo said. Following a successful pilot, BBVA decided to deploy RecoverGuard across all critical servers, which are now scanned on a regular basis. In addition, alerts are reviewed daily by BBVA to proactively handle gaps, and the product's reporting and visualization features are used to facilitate daily tasks such as planning, documentation, and optimization.

Results

By implementing RecoverGuard, BBVA has been able to automate and streamline processes and gain improved control over its DR/HA environment. In addition to addressing BBVA's operational need to automate the management of DR/HA tasks and ensure uptime of critical systems, the deployment of RecoverGuard has resulted in other key benefits. Most notably, it enabled the group to optimize processes and reduce associated costs by shortening testing cycles and time spent on service calls, for example, and freeing up IT staff to focus on more value-added activities. Furthermore, RecoverGuard has enabled BBVA to optimize resource utilization in periodic contingency tests.

According to BBVA, the main advantages of using RecoverGuard can be summarized as follows:

- **Proactive Detection of Infrastructure Vulnerabilities:** Improved visibility of systems, components, and their interdependencies, which helps anticipate the possible risks that can occur in DR/HA configurations

- **Optimization of Recovery Plans and Testing:** Improved design and implementation of the recovery plans, as well as allowing for the simulation of tests with greater frequency (weekly, daily), without the need to deploy all of the resources to carry these out

- **Risk Assessment:** Improved predictability of business impacts on services and systems that can be affected by downtime or data loss vulnerabilities

ESSENTIAL GUIDANCE

Advice for End Users

Large companies are spending millions of dollars on their DR/HA infrastructures to ensure business continuity in the event of various scenarios. Nevertheless, many of these organizations have limited visibility into data protection gaps and configuration vulnerabilities between the primary production site and the disaster recovery site, especially in dynamic IT environments in which configuration changes occur frequently. As a result, organizations do not know for sure that their critical systems will continue to operate properly in the case of a disaster.

The BBVA example clearly illustrates the need to identify data protection gaps. In recent years, the company has been expanding its IT infrastructure to support its business expansion plans. In light of the increased complexity introduced by this move, BBVA has been dealing with the challenge of identifying problems before they escalate into system failures or downtime and negatively impact business continuity. By using Continuity Software's RecoverGuard, BBVA has been able to take a proactive and automatic approach to identifying and fixing problems and thus improving the availability and recoverability of critical business systems.

LEARN MORE

Related Research

- *Worldwide Business Continuity 2011–2015 Forecast: A Multidimensional IT Market Influenced by Increased Corporate Reliance on IT Systems, Applications, and Data* (IDC #230483, September 2011)

- *The State of Business Continuity in End-User Environments in 2011 (IDC #227783, April 2011)*

Copyright Notice