

BUYER CASE STUDY

West Jefferson Medical Center Rearchitects Its Data Protection Infrastructure with NetApp Syncsort Integrated Backup

Robert Amatruda

IDC OPINION

IDC has discovered many organizations are rearchitecting their data protection and recovery infrastructure and backup processes to attain more effective protection and disaster recovery. Also, many companies are dealing with unabated data growth, increased server virtualization, and aggressive service-level agreements (SLAs). More importantly, customers are seeking ways to lower their capital and operational costs while improving their disaster recovery preparedness. As a result, disk systems are being placed in the data protection path in many customer environments. The use of disk in the data protection process relieves many of the backup bottlenecks associated with using traditional storage methodologies — such as tape. Highlights include:

- ☒ We have found customers are demanding faster backup, restore, and recovery to meet their shrinking backup windows. Many customers are augmenting or foregoing further investments in data protection processes that rely solely on physical tape infrastructure. Today, customers need improved tools that allow them to extend their protection framework to safeguard their growing numbers of virtual servers and the burgeoning storage requirements. IDC research indicates that over the past several years, the customer drivers for increased investment in disk-based data protection solutions result from the need to improve backup window time, provide faster restore and recovery times, enable seamless integration with existing backup applications, improve performance and utilization of backup resources, and lower operational and capital costs.
- ☒ West Jefferson Medical Center, a parish-run hospital in the greater New Orleans area, implemented NetApp Syncsort Integrated Backup (NSB) after a rigorous proof-of-concept process to rearchitect its data protection and recovery infrastructure. The NSB implementation yielded significant operational benefits and cost savings in its data protection infrastructure and backup processes. Additionally, the IT staff no longer has to rely solely on tape for recovery.

IN THIS BUYER CASE STUDY

This IDC Buyer Case Study assesses the deployment and use of NetApp Syncsort Integrated Backup (NSB) at the West Jefferson Medical Center. Additionally, IDC examines the operational benefits the center's IT organization has gained after the NSB deployment. IDC conducted an in-depth interview with Nicholas Burlison, senior

systems engineer, responsible for VMware infrastructure, storage, and backup and recovery. Burlison outlined the hospital's organizational needs and proof-of-concept process that led to the deployment of the NSB solution.

SITUATION OVERVIEW

Organization Overview

West Jefferson Medical Center is a 451-bed not-for-profit hospital located in Marrero, Louisiana, serving the West Bank portion of Jefferson Parish. The medical center currently has approximately 2,000 employees, occupies a 20-acre campus near downtown New Orleans, and serves 7–10 outlying clinics.

Burlison is responsible for VMware infrastructure as well as backup and recovery at the medical center. In addition to Burlison, the IT staff has one backup administrator for day-to-day activities and an engineer to handle any back-end storage or engineering issues. Burlison is responsible for delivering IT services including support and testing and infrastructure planning, design, vendor selection, and day-to-day backups and restores as required by the medical center's SLAs. The IT organization supports 350 servers and relies on VMware to virtualize its systems. Currently, 60% of the hospital's environment is virtualized. Additionally, the IT staff supports Red Hat Linux AIX servers with nearly 2,300 users and 1,700 end points. The medical center also supports TSM, which supports an extensive physical tape back end, as a primary data protection tool for its backup and recovery.

The medical center's current backup environment consists of two NetApp 3240v filers with a 30TB disk capacity for local backups and a single 20TB NetApp FAS2040 filer for replication to a collocation site. Data deduplication is performed after every backup and is done on the 3240v filer. Data deduplication is done on the NetApp array and it frees resources on the Master Server, which is orchestrated by the Syncsort data protection software. The IT staff has a single Master Server and a Reporting Server to administer the Syncsort Data Protection software. Furthermore, the IT staff uses Advanced Recovery for SnapVault as well as Exchange, SQL, and SharePoint modules. In addition, the IT staff uses a portion of the NetApp arrays along with NetApp's Open Systems SnapVault (OSSV) for backup and recovery of approximately 20–30 Linux AIX servers. NetApp's OSSV allows the IT staff to create more frequent backups from changed blocks of data rather than entire changed files. However, the recovery process is managed completely by the Syncsort data protection software client. This methodology improved backup performance and used less disk space. It allowed Burlison and his staff to continue block-level backups even though the current version of their Syncsort Data Protection software supported only Linux and Windows OSs.

Challenges and Solution

Burlison and other members of the IT organization began to reevaluate their data protection and recovery needs during a comprehensive proof-of-concept analysis of their current data protection and recovery architecture. The project was driven out of the need to provide much more aggressive SLAs, particularly for recovery time

objectives (RTOs) and recovery point objectives (RPOs) for their applications. Another key objective for the IT staff was to move away from an incumbent data vendor and reliance on traditional tape-based processes while improving recovery performance. The IT staff was dealing with lengthy backup windows and did not have the confidence or fidelity of recovery from its current tape-based solution. However, tape still needs to be supported in their IT environment for the foreseeable future. The project included a bake-off of four other major midtier backup and recovery vendors. Burlison's staff analyzed each vendor's features, benefits, costs, and administrative time needed to manage the solution.

Ultimately, Burlison's staff decided to deploy NSB as the medical center's primary data protection solution after the evaluation process concluded. NSB is an integrated solution that combines Syncsort data protection software with NetApp snapshot, clone, and replication technology using high-performance NetApp disk storage. NSB is a fast, efficient, and easy-to-use data protection solution for physical and virtual servers running in heterogeneous storage environments. The implementation started in March 2011, with 98% of the deployed systems now protected using the NSB solution. The additional systems are still using the incumbent solution for RAW file systems and a proprietary backup process. The IT staff offloads the proprietary data to the NSB system in the form of a VTL format. Currently, Exchange data and File Server data have the most stringent RPOs and RTOs. As a result, the IT staff uses snapshots on Exchange data stores twice a day and retains them for approximately a month. However, the staff snaps the File Server data twice a day, but it is only retained for seven days because of the significant amount of changes. Also, some database applications with very intensive RTOs are snapped weekly and retained for only three days.

Results

The West Jefferson Medical Center IT staff greatly improved its RTOs and RPOs after the NSB deployment. Burlison states that the IT staff has had no complaints meeting the aggressive RTOs and RPOs. Rearchitecting or changing data protection at a major medical institution is no easy feat. Typically, changing data protection vendors can be a long, painful, and drawn-out process. However, Burlison claimed the choice was a "no-brainer" due to the ease of the NSB implementation and its ease of use. Furthermore, he states, "The ease of use for implementing NSB was untouchable by the other vendors."

To support his claim, Burlison and his staff configured the master server on the first day of deployment and initiated a backup before lunch. Then an extensive set of tests were conducted on NSB's recovery features. Burlison claims NSB's recovery capability was far superior to the IT staff's incumbent vendor's solution that would experience failures or missed backup jobs on a daily basis. In fact, the backup administrator would need to devote hours every day to manually correct the problems. The RTO has improved remarkably using NSB's Instant Availability, Instant Virtualization (IA/IV) capabilities. The IT staff, using IA/IV, can now provide rapid recovery with no data loss. Also, NSB's reporting and alerting capabilities provided a windowpane into the backup process.

Burlison's staff performs 1–5 weekly recoveries using the IA capability. The staff has used the IV capability only in testing. Overall, Burlison is very pleased with the NSB deployment, stating, "On a scale of 1 to 5, with 5 being the highest, I would say our satisfaction is in the 4.5 range." Additionally, he is happy with the level of service and support he has experienced with NSB.

ESSENTIAL GUIDANCE

The opportunity looks bright for disk-based data protection, in particular those systems with deduplication. IDC believes solution vendors should consider the following guidance:

- ☒ Communicate to customers the value proposition and potential benefits of using more disk-based storage solutions for data-protection.
- ☒ Provide nondisruptive integration of disk-based storage solutions so customers need not change any procedures and policies.
- ☒ Support seamless data movement capability from disk-based systems to physical tape to support archive and disaster recovery.
- ☒ Support industry-standard interfaces, APIs, and application software to ease deployment.
- ☒ Add features that optimize storage efficiency, such as data deduplication. Although this may reduce the potential number of terabytes per installation, vendors that offer storage efficiency will be compelling.

LEARN MORE

Related Research

- ☒ *Worldwide Purpose-Built Backup Appliance 2011–2015 Forecast and 2010 Vendor Shares* (IDC #228091, May 2011)
- ☒ *Data Deduplication Gaining Adoption and Enabling Disk-Based Data Protection and Recovery* (IDC #227924, April 2011)
- ☒ *IDC's Worldwide Disk-Based Data Protection and Recovery Taxonomy, 2011* (IDC #227713, April 2011)

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2011 IDC. Reproduction is forbidden unless authorized. All rights reserved.