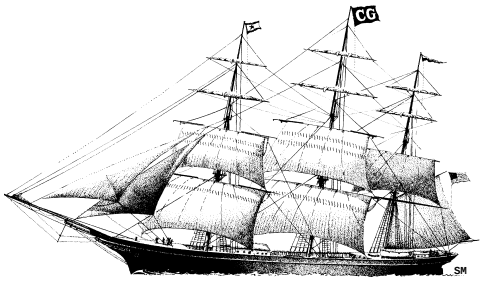
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2006029 May 4, 2006

Symantec's Answer to Remote Office Backup

Analyst: Dianne McAdam

Management Summary

IT administrators in large data centers have had the responsibility for backing up data (and restoring it when necessary) for years. Unfortunately, data is no longer centralized in the main data center. A large amount of important enterprise data is located in remote offices. In many cases, the responsibility of backing up and protecting that data also resides in the remote office. Many remote offices do not have people dedicated to supporting the backup process and that can cause problems when data is accidentally deleted or corrupted and must be restored.

One nationwide retail company is now very familiar with the problems that can occur when backups are not tested, or monitored. This organization had hundreds of stores located across the United States. Each retail store was responsible for their local human resources, payroll, and customer marketing applications and for managing the nightly backups. In most store locations, the store manager assumed the backup responsibilities. Store managers, who excelled at managing the store, had little, if any, IT expertise. Throughout the year, several of the stores had data that was accidentally deleted or corrupted and needed to be restored. Many of the restore jobs failed since the backup jobs were never properly tested or monitored. In those cases, personnel, payroll and customer data had to be manually entered back into the system, a long and tedious task.

IT management at the central data center visited many of the stores, and discovered that backups were not consistently implemented across all locations, were not regularly monitored, corporate policies were not always enforced or not properly enforced, and data was not properly secured.

This story is not unusual. **Remote offices do not have the resources or expertise to manage - adequately - backup processes.**

Symantec's NetBackup PureDisk Remote Office solution addresses these needs in several ways. Read on to learn how.

Different Ways to Protect Remote Offices

There are several different ways to protect data at remote location, each with its advantages and disadvantages. The first approach creates nightly backup tapes. These tapes are stored onsite (which provides no protection from a localized disaster) or are shipped to a remote location. If tapes shipped offsite are not encrypted and are lost in transit, enterprises leave themselves vulnerable to the possibility of data theft, fines, and negative publicity. This approach is favored by many

IN THIS ISSUE

- Different Ways to Protect Remote Offices 1
- Choosing the Right Remote Office Solution 2
- Symantec's Answer 2
- What's Available Today 3
- Summary 3

companies, since it is relatively inexpensive, but does not provide data security.

Another common way to protect data at remote locations is to transmit the backups every night to the main data center. Usually, the data shipped over the network is encrypted, providing adequate security. However, this approach can heavily utilize existing networks, adding to the cost. Both approaches do little to ensure that all data is properly backed up or that corporate policies are enforced.

Choosing the Right Remote Office Solution

Large corporations have hundreds (or thousands) of remote offices that need data protection and must choose solutions to protect remote data wisely. Choosing the wrong solution can be costly and ineffective. The following questions should be asked about each solution under evaluation.

1. *Does the solution start up the backup process automatically? Does it require manual intervention by end users?*
   - Remote users should not be required to perform manual operations, such as swapping tapes in tape drives.
2. *Does the solution discover and protect all new data stored on remote servers?*
   - By default, all data should be backed up on a regular schedule.
3. *Can corporate policies be set by central IT administrators that specify how often data is backed up?*
   - It is important that policies be enforced to ensure that the corporation complies with regulations.
4. *Can end users restore their own data?*
   - Allowing end users to restore their own data can eliminate many calls to centralized help desk personnel.
5. *Can the solution scale to support a large number of remote offices? Can the solution scale to support the growing amount of data in each office?*
   - The solution acquired today should be able to support growth in both the amount of data and number of locations.
6. *Does the solution provide data security?*
   - Data in flight needs to be encrypted to prevent unauthorized access.
7. *Can the solution be managed by qualified IT administrators in a central location?*
   - Managing remote backups in one centralized location reduces costs.
8. *How much storage is required to store the backups at the remote site*
   - Functions such as compression or storing only one instance of the data, can dramatically reduce the amount of storage required at remote locations.
9. *How much network bandwidth is required to transmit the backups to the central data center? Is the entire backup sent every night, or are only the changes sent?*
   - Sending only changed data saves network bandwidth.

Answering these questions should help in choosing the right solution.

Symantec's Answer to Remote Office Protection

Symantec acquired DataCenter Technologies in 2005 to improve their data protection suite of products. DataCenter Technology had developed a product named *DC-Protect eXtended Architecture* (or *DC-Protect XA)* to backup data in remote offices. Now, Symantec has plans to take this product, now called *NetBackup PureDisk Remote Office*, further than DataCenter Technologies ever could.

PureDisk Architecture

NetBackup PureDisk Remote Office is, as the name implies, a disk-only software product for remote offices. Customers can purchase NetBackup PureDisk Remote Office from Symantec and run it on existing servers and disks. We expect that some of Symantec's partners will also offer appliance with the software already installed or will provide a hosted service offering.

What makes NetBackup PureDisk Remote Office different from other products is its modular, scalable architecture that can

protect large numbers of remote offices. There are two major components to PureDisk scalability – the *MetaBase Server* that manages and stores the metadata and the *Content Router* that manages and stores the data across disk systems. Each *Metabase Engine* can store the metadata of 50 million files. Additional Metabase Engines and Content Routers can be added, when needed, to support data growth.

PureDisk saves storage capacity at both the remote site and central site, and also saves network bandwidth. First, it examines all data at the remote location and eliminates redundancies. Then, the data is sent to the Content Routers, which stores only the segments that have changed. This data reduction technique, called *single instance storage*, not only reduces storage requirements, but saves network bandwidth as well, since only changed data is sent "over the wire". The corresponding metadata (that is, data that describes the data) is sent to the metabase.

Some remote office solutions, such as Wide Area File Systems (WAFS), eliminate storage pools at remote locations. However, having remote storage managed by NetBackup Pure Disk Remote Office provides several benefits. It can be easily plugged in to existing remote office environments, while WAFS solutions require rebuilding the remote architecture. End users can restore data quickly at LAN speeds. Data is replicated to a central site providing disaster recovery protection. Global single instance storage compares data at the remote office with data already stored at the data center and only transmits the unique segments, which dramatically reduces bandwidth. Moreover, data is secure since it is encrypted when stored on disk and also when transmitted over the network.

All PureDisk installations can be managed from one central location, which ensures that corporate policies are enforced at remote locations. End users can restore their own files through an easy-to-understand web interface.

What's Available Today

The first version of PureDisk is a standalone remote office backup solution that supports Microsoft *Windows* and *Linux* clients' file-based data. Data is backed up at remote locations and sent over a network to a PureDisk *storage pool* at the main data center. Any backup application, as a separate process, can later back up this data to other disk or tape for offsite storage.

Future Support

Support for *Solaris*, *HP-UX*, and *AIX*, with *Exchange* and *SQL* application support will be added in a later interim release.

The second major version of NetBackup PureDisk Remote Office integrates PureDisk technology with *NetBackup*. Here, the entire process of backing up data from remote offices to main data center to offsite vault is completely automated. A PureDisk Gateway product provides the communication between PureDisk storage and NetBackup. NetBackup can retrieve data from PureDisk to create offsite tapes. Or, NetBackup can stage its own backups to PureDisk storage, to take advantage of the capacity-saving single instance storage technology.

Summary

The amount of data that needs to be protected in remote offices continues to grow; at the same time, government regulations impose strict rules about how this data must be handled. Companies with remote offices must be diligent to ensure that data stored in remote offices is securely protected. The most efficient way to monitor and manage this data is with a centralized solution, such as NetBackup PureDisk Remote Office, now available from Symantec.

Customers installing the first release of NetBackup PureDisk Remote Office will immediately benefit from disk and network savings. Existing NetBackup customers will gain even more benefits from the second major release. Here, NetBackup users can leverage the PureDisk single instance storage technology for space-optimized backups to disk, extending the amount of data that can be retained on disk. Take a close look at NetBackup PureDisk Remote Office Edition.

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

Dianne McAdam **is Director of Enterprise Information Assurance for the Clipper Group**. She brings over three decades of experience as a data center director, educator, technical programmer, systems engineer, and manager for industry-leading vendors. Dianne has held the position of senior analyst at Data Mobility Group and at Illuminata. Before that, she was a technical presentation specialist at EMC's Executive Briefing Center. At Hitachi Data Systems, she served as performance and capacity planning systems engineer and as a systems engineering manager. She also worked at StorageTek as a virtual tape and disk specialist; at Sun Microsystems, as an enterprise storage specialist; and at several large corporations as technical services directors. Dianne earned a Bachelor's and Master's degree in mathematics from Hofstra University in New York.

- ***Reach Dianne McAdam via e-mail at dianne.mcadam@clipper.com or at 781-235-0085 Ext. 212. (Please dial "212" 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**, 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.