

# STORAGE SWITZERLAND REPORT

## MANAGING BACKUPS IN THE REAL WORLD



George Crump, Senior Analyst

Developers of backup software work under the expectation that an enterprise will use only their application to protect the environment. Reality couldn't be more different. Most enterprises have more than one backup application and also use more than just backup to protect their data. Snapshots and replication are commonly used, as an example. Managing backups in the real world requires a tool that can not only manage multiple backup applications but can also manage multiple backup targets as well as other data protection processes.

### **The Multi-Vendor Backup Reality**

Realistically, most data centers run more than one backup application. At a minimum they're often split between Operating Systems (OS). For example, the Windows administrators may be more comfortable with Symantec's Backup Exec and UNIX administrators may like EMC's Networker. It's not uncommon for this fragmentation to go further along application lines. For example, the Exchange administrators may implement CommVault Galaxy for improved mailbox protection and the VMware administrators may want to take advantage of Syncsort's Block Level Incremental capabilities. Along with traditional backup applications, customers are also leveraging

features available in most storage systems, like snapshots or replication. Even OS mirroring is a form of data protection that needs to be given some attention.

With each new application or platform comes the possibility of a new backup software product or other form of data protection. While this is far from ideal from the perspective of the backup administrator, it is reality. Application owners demand capabilities for recovery that typically can't be found in a single product. In the end, protecting the data asset is more important than the cost to manage that protection. As a result, additional backup applications or protection methods are often justified. As part of this justification however, the backup administrator needs the ability to manage all these disparate applications with a single process.

If multiple backup applications are a reality in the environment, the task of manually logging into each backup server and checking the status of its backup tasks can be daunting. What's needed is a singular view of the data protection process, one that can interface with the various applications and provide information on other data protection processes, like mirrors, snapshots or replication.

## Centralized View

Applications like Backup Profiler from [Tek-Tools](#) can monitor and report on the success and failure of backup tasks. They can also capture diagnostic details about the backup job and other storage services across multiple applications, from a single web based GUI. The capability of having all the backup results available in a single view can provide valuable information about how the overall backup process is performing. Being able to see backup failures across applications can pin-point problems to a single client or even network segment. This consolidated view is the cornerstone to increasing backup success rates and improving backup administrator productivity. Instead of having to manually log into each backup application and storage device, the GUI can provide a heads-up display on the data protection process as it happens. This is much less time-consuming or prone to error than the alternative.

A consolidated view also allows backup monitoring to be offloaded to overnight operations personnel. They can monitor all the backup processes without needing to be experts in each application. If there is a backup failure the operations person can notify the expert for that particular backup application or storage system, as well as provide them with initial diagnostic information on the failed job.

## Monitoring vs. Reporting

This kind of monitoring is difficult to do with a basic backup reporting

application. Tools that provide backup reporting exclusively, can't provide real-time information on the status of backup jobs, while they're in process and at the moment they complete or fail. This is less than ideal when an operations person is available to monitor the backup process. With shrinking backup windows and growing data sets, job failure reports must be readable by these personnel who are on-site when backups are run. Waiting until after the fact, when a reporting process can analyze the backup logs to determine which backup jobs failed can take hours. This means it may be hours before failed jobs are manually rescheduled. Those lost hours may push the job outside of the available backup window, costing the organization either productivity while the backup task is rerun. Or it can place data at risk for an additional 24 hours if the decision is made to skip re-running the job.

Even without an operations person monitoring the job, real-time event tracking allows for notification via email. Then, when a job fails, the manual job restart can happen quickly. This email can be sent to the individual backup application administrator or to a backup administration team. In either situation, a real-time notification of failure can allow the job to be restarted sooner, and potentially completed within the backup window. Not only does this ensure better data protection it also may maintain a Service Level Agreement (SLA) that the IT department is judged on.

Real-time backup monitoring however, does mean that an agent needs to be installed on the backup server. While

agents in the past used to be a source of concern many of the issues have been resolved, as OSs and developers of the monitoring software have matured their products. Companies like Tek-Tools, which use these agents can provide near-instant updates to the condition of the backup process. These live updates can be reflected on a GUI that a night operations person monitors or the details can be emailed to the appropriate backup administrator.

## Predicting Failure

The best type of backup failure is the one that never happens because the potential problem was eliminated before it occurred. This does require an historical analysis tool. Ideally, it's best if the tool leverages the information that a monitoring application, like Backup Profiler, is already capturing. With this tool in place all the backup jobs can be trended. For example, a sudden change in the amount of time it takes for certain clients to backup, even those that are going to different backup applications, could indicate some kind of network degradation or conflict with a concurrent process that's consuming the available resources. Or, errors caused by lack of media or available disk space on a VTL can be eliminated by using the trending information to predict when backup devices will need additional capacity.

## **Giving Backup Center Stage**

One of the challenges backup administrators have is justifying new additions or upgrades to the backup infrastructure. This is partly because the backup process is only thought of when something goes wrong. Most of the time it's assumed that backups just happen, almost magically. Backup managers need to get the information out about how the backup process is working and if SLAs are being met. They also need to provide information about new backup challenges, like a sudden increase in data load or in the amount of restore requests.

With a backup management tool like Backup Profiler, reports can be created and emailed to the appropriate individuals. They can be high-level executive-style for quick review or they can have more detailed information for departmental review. The action of the IT manager, CTO, or even CEO getting an email every morning graphically showing that everything is protected could have immense value to the department. Finally, there is the ability to match the protection process with compliance or SLA requirements and be able to communicate regularly as to how those standards are being met. Again, all this happens with a single report, regardless of how many applications are being used in the protection process.

It's unlikely that most environments will ever truly be able to settle on just one backup application for the enterprise.

Managing backups in the real world requires skilled professionals armed with the appropriate tools to be able to do their jobs quickly and easily. A tool that can provide a real-time consolidated display of the data protection process goes a long way towards making fully managed backups a reality.

### **About Storage Switzerland**

**Storage Switzerland, is an analyst firm focused on the virtualization and storage marketplaces. For more information please visit our web site: <http://www.storage-switzerland.com>.**