Tape Backup for Disaster Recovery? *Really?*

Keith B. Evans >> Shadowbase Product Management >> Gravic, Inc.

A document recently passed across my desk and it got me thinking. It discussed a data backup and restore process, to be used during disaster recovery, such as restoring IT services on a backup system after some kind of production system outage. The DR process involved creating production data backups on the storage medium of tape or virtual tape, restoring the data to disk on a backup system, and then rolling forward the audit trail (updates performed since the backup was taken), to bring the data up-to-date.

This process might be perfectly reasonable for some less important applications, but the thought that came to mind was whether anyone still uses this approach to business continuity for a mission-critical application? Surely not? But when I mentioned it to Paul Holenstein, EVP of Gravic, Inc. and responsible for the Shadowbase data replication and integration product suite, he disagreed, stating that over the course of his 30-plus years of experience in the business continuity field, he has come across many organizations using this approach, even today!

But why is backup/restore such a problematic technique to use for disaster recovery? Here are a few of the more significant reasons that Holenstein cited:

- Locating a backup/standby system or datacenter may be difficult, assuming you don't already have one and need to go and declare an "event" at your recovery provider's datacenter.
  - Don't be last in line to declare your "event" either, as many DR service providers take customers on a first-come, first-served basis and you don't want to queue behind someone else's use of the datacenter/DR equipment.
- Downtime might be lengthy (higher Recovery Time Objective, or RTO) due to the time taken to find the right backup data, restore that data, roll-forward through any interim changes, load and then restart the application. This sequence often takes many hours or even days.
- Significant amounts of data are likely to be lost (higher Recovery Point Objective, or RPO). Data loss is governed by the frequency of sending the backups and interim changes off site, hence a frequent safe-store period is required or else significant data loss will occur.
- The recovery process has a high probability of failure, often referred to as a "failover fault." Many things can go wrong or not occur within specified Service Level Agreement (SLA) times, therefore making this form of business continuity replication far more risky than the forms discussed below.

Add the cost and inconvenience of periodically testing the failover process – assuming you even ***do*** failover testing, since budget cuts have decimated DR testing budgets – and this approach simply cannot be trusted for many applications.

All of these issues can lead to lengthy outages, often measured in ***days*** of downtime. In today's always-on world, a mission-critical application being down for days is simply unacceptable. Companies have gone out of business for less. Given the high value of some data, losing any of it is to be avoided.

However, there are solutions available ***today*** for disaster recovery and higher levels of business continuity protection which are comparatively easy to implement, relatively inexpensive when compared to the ***total cost*** of downtime, and which do not suffer from these egregious shortcomings. Figure 1 shows these various technologies and their relationship to the duration of the outage (RTO), and the amount of data loss (RPO) that each approach may cause to occur.

What is clear is that data replication is a far superior solution for ensuring business continuity of mission-critical applications than tape backup/restore methods, as it reduces outage times and amounts of data lost from days to seconds or sub-seconds, or even to zero in the case of active/active synchronous replication. Holenstein commented that there are several products on the market today which support one or more of the data replication architectures shown in Figure 1.

In conclusion, while it is interesting to read about an old-

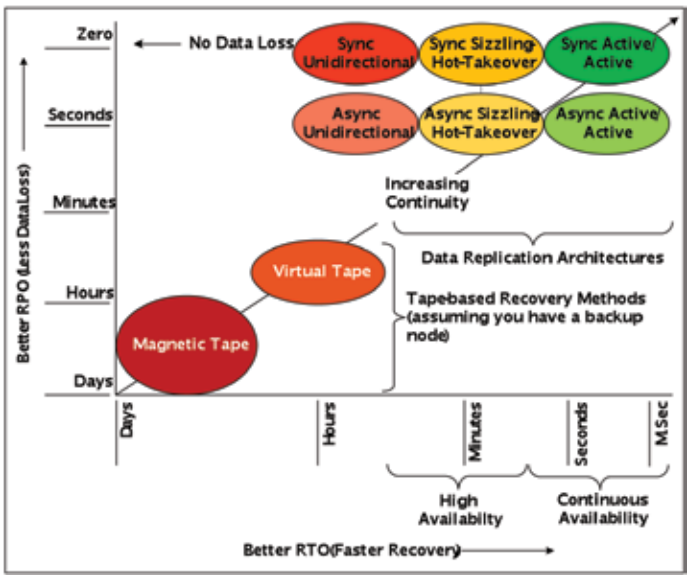

Figure 1 - The Business Continuity Continuum

school methodology for performing a backup/restore procedure in case of the need for disaster recovery, the real takeaway is that such techniques are insufficient for mission-critical applications, and come with significant and unnecessary risks. Organizations that still use such methods should immediately put these risks behind them, consider a data replication solution, and begin the move to continuous availability as soon as possible (Figure 2).

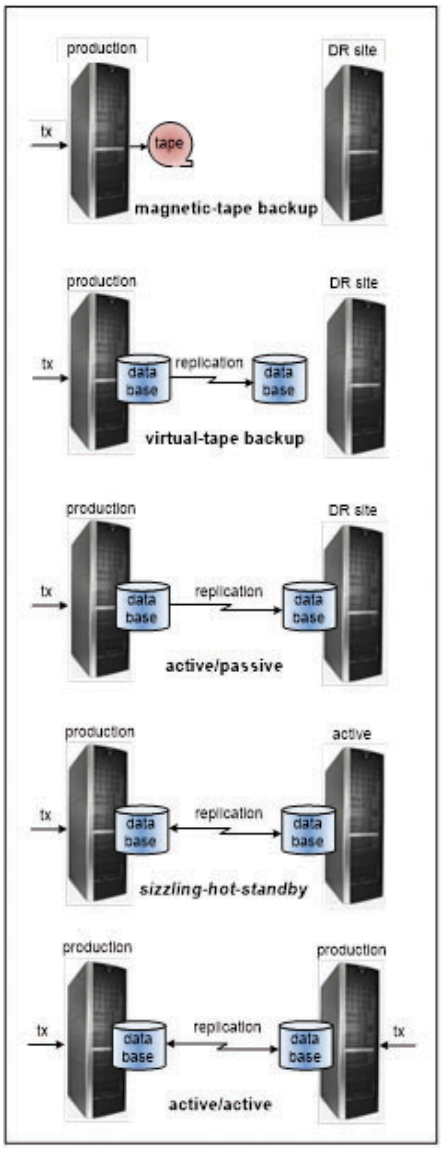

Figure 2 - Moving to Continuous Availability

Note: For more information about disaster recovery and improving your application availability profile, reducing risk, and how the more advanced architectures can satisfy your most-pressing business continuity requirements, please download the white paper, Choosing a Business Continuity Solution to Match Your Business Availability Requirements at www.gravic.com/shadowbase/whitepapers or email shadowbase@gravic.com.

Keith B. Evans works on Shadowbase business development and product management for the Shadowbase product suite, including business continuity, data integration, application integration, zero downtime migration, data utilities, and synchronous replication, a significant and unique differentiating technology. To contact the author, please email: SBProductManagement@gravic.com

Note, this article focuses on the use of tape/virtual tape backup/restore techniques specifically for the purposes of providing business continuity for mission-critical applications, such as applications that must always remain available, and be recoverable in very short timeframes (seconds/minutes). There are many other uses of tape/virtual tape backup/restore for which this technique is appropriate and perfectly suited to the task.