

Inside Perspective

Helping you unleash the full power of MEDITECH

Electronic newsletter published every 8 weeks

Do you have a storage strategy? (Part 3: MEDITECH's Integrated Disaster Recovery)

Jim Fitzgerald, Chief Technology Officer

In the first installment of this series on storage strategy, we examined the business and technical drivers for investing in Storage Area Network (SAN) technology. The emergence of the electronic health record (EHR) as the central repository for critical patient information has changed the way IT managers look at data storage. Patient data now transcends any and all storage requirements or applications, and SAN technology has become a critical tool in centralizing, managing, and protecting the electronic health record. From a technical perspective, as newer, more sophisticated clinical applications come on line, SANs become particularly important in the MEDITECH environment as a means of maintaining database performance and availability.

In part two, we explored MEDITECH's Integrated Serverless Backup (ISB). As more and more clinical decision-making becomes dependent on the electronic health record, the notion of any significant downtime becomes less and less palatable. Integrated Serverless Backup (ISB) coordinates BridgeHead and Legato backup software with MEDITECH's backup utilities, as well as SAN features such as Business Continuity Volumes (BCVs) and Snapshots which allow the creation of a point-in-time copy. In an emergency that affects data availability, Integrated Serverless Backup can mean the difference between a 40-minute or a four-hour restoration time for typical MEDITECH databases and an even more dramatic difference on EMR restores.

In view of the growing focus in Healthcare Information Systems (HCIS) on data recovery, this final chapter of the current series will take a look at one technology option for protecting your HCIS data from both operational and actual disasters—Integrated Disaster Recovery (IDR). Introduced by MEDITECH at the MIX CIO Forum in June, 2004, IDR leverages the ability of MEDITECH's Integrated Serverless Backup to coordinate the creation of a SAN-based point-in-time copy. Instead of using these point-in-time copies for backup purposes, IDR manages these one-time replicants to either local or remote SAN storage designated for recovery purposes. IDR is currently supported by BridgeHead HyperTape™ backup software and is also expected to be available as an add-on module to Legato Networker® later this year.

Although IDR leverages Integrated Serverless Backup as a core technology, it is important not to confuse IDR volumes with backup volumes. Backups of MEDITECH and other applications are typically saved either as image files or savesets. Image files, which are used as the default backup mechanism in ISB, enable swift and efficient restoration of an entire storage volume. Savesets are more commonly used by backup software, and contain the actual backup files, along with the directory information required to select them individually for restoration. While savesets take longer to restore than image files, they offer a far greater granularity in selecting specific files to restore. Interesting though this might be, the key point here is that IDR uses *neither* of these technologies. IDR creates a true replica of your MEDITECH database volumes at a specific point in time. In an emergency affecting data availability, these volumes can be associated with new or existing servers and booted immediately to bring MEDITECH back on line.

There are at least two sets of circumstances in which your organization might need to quickly restore a “clean” replica. The first is broadly labeled “Operational Recovery” (which out of deference to our clinician brethren we will not refer to as “OR”). Operational Recovery events are generally limited-scale tactical hiccups which interrupt one or more applications and their associated processes. For example:

- A single server or portion of a storage subsystem experiences a hardware failure.
- A database corruption is accidentally induced on a single application and goes unnoticed for several hours.
- A physical accident temporarily brings down a portion of your IT infrastructure.

In the past, Operational Recovery for MEDITECH has been done mainly from tape backups—which in many cases can be up to 18 hours old at the time they are needed, and may take 2-6 hours per tape to restore. Your systems are up and running again, but there is now a need to manually reconstruct “a day in the life” of your organization. Thoughtful use of ISB and IDR (which builds on ISB) can put you in a position to restore data as little as one hour old in a matter of minutes.

The other set of circumstances is “Disaster Recovery,” called “DR” by the world in general, and not to be confused with “Data Repository” in the MEDITECH environment. We have discussed DR at length here before, but in general, these are some combination of the mundane and the movie-class disasters. (By the way, all of the examples below have actually happened at a hospital using MEDITECH.)

- A pipe leaks over the data center and wipes out your primary SAN array.
- A maintenance worker notices smoke and hits your EPO (Emergency Power Off) switch in the data center, mistaking it for a fire alarm. It takes hours to restore services, and much of your cached SAN and applications data is corrupted.
- Your area gets hit with severe rains and the basement data center floods.
- A quarantine keeps personnel from entering or leaving the data center.
- The generator system fails during an extended power outage.

IDR can help with disaster recovery by making it easy to store point-in-time volume replicas in alternate SANs—on or off your campus—without the expense or potential technical complexity of managing a SAN-to-SAN remote mirror. (SAN mirrors, by the way, are still the *crème-de-la-crème* of remote recovery, but they are not for everybody.) Sure, you will need extra servers and storage to achieve the fastest recovery possible, but depending on your risk tolerance and the uptime requirements of your user base, it may be a worthwhile investment.

I hope this series has been useful in considering your options for storage, backup, and recovery. (If you missed the first two articles, click on Issues 14 and 15 in the Archives section found on the Home Page of this issue.) As IT becomes more integrated into the care process, downtime is becoming less and less tolerable. Storage is playing an increasingly critical role as the focus moves to utilizing the HCIS to drive patient safety and clinical results.

Jim Fitzgerald is the Chief Technology Officer at JJWild. He promises to lighten it up next time and is interested in your favorite topics. As always, your comments, questions, and input are encouraged at editor@jjwild.com.