Realtime publishers

Taking a Fresh Look at Business Continuity and Disaster Recovery

The Essentials Series

sponsored by

DELL

Don Jones

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Taking a Fresh Look at Business Continuity and Disaster Recovery

For the longest time, organizations' approach to disaster recovery was simple: back up as much as possible, as often as possible, and hope that you never need the backups. In the past few years, businesses have become a bit more proactive and demanding. Instead of asking, "How will we recover from this disaster?" they're asking "How can we keep our business running *through* the disaster?" Commonly referred to as *business continuity,* this desire forces us to take a fresh look at how we keep our systems up and running. Although the "fail and recover" approach will always be part of our layered business protections, it can't always be the *first* layer because in order to *use* a backup, something first has to *fail*—which isn't always an acceptable option. We need to discard the one-size-fits-all approach of "just back it up," and start thinking about business continuity approaches that are tailored to specific services within the organization.

Email Continuity

Email is perhaps one of the most mission-critical applications within any organization. Our ability to communicate not only runs our business but also fosters growth. The near-instant communication offered by email can also be a key tool during a disaster or crisis because email enables us to coordinate activities, share priorities, and react more dynamically to a changing situation.

Many organizations are looking to outsource their email services to not only save money but also better ensure the availability of email through any kind of circumstance. Ensuring the availability of email as well as email-connected devices (such as Blackberry devices) and distributed users is crucial.

This is *not* a statement that "cloud computing" is the way to go for email. For some companies, cloud-based email services are definitely beneficial. But many companies have strict data management and security needs around email—often related to regulatory or industry requirements—that can't always be met by popular "email as a service" providers.

Outsourced email can also simply mean having your email infrastructure live elsewhere and be managed by someone else in a more highly-available, fault-tolerant fashion than you can provide on your own. You might still call this "cloud-based" email because it's a service coming from the cloud, but that doesn't mean it's a generic, unmanaged, unsecure arrangement. Many vendors today can provide the same level of security, e-Discovery services, data retention management, and other features that you currently provide in your own data center—they simply do so out of highly-redundant data centers that won't be impacted if yours is struck by a disaster. Thus, your email keeps working.

Server Clusters

Many applications can be made more fault tolerant through the use of server clusters. Available for most modern server operating systems (OSs) including Microsoft Windows and Red Hat Linux, server clusters are typically configured as Figure 1 shows (which specifically illustrates a Microsoft Windows Server cluster).

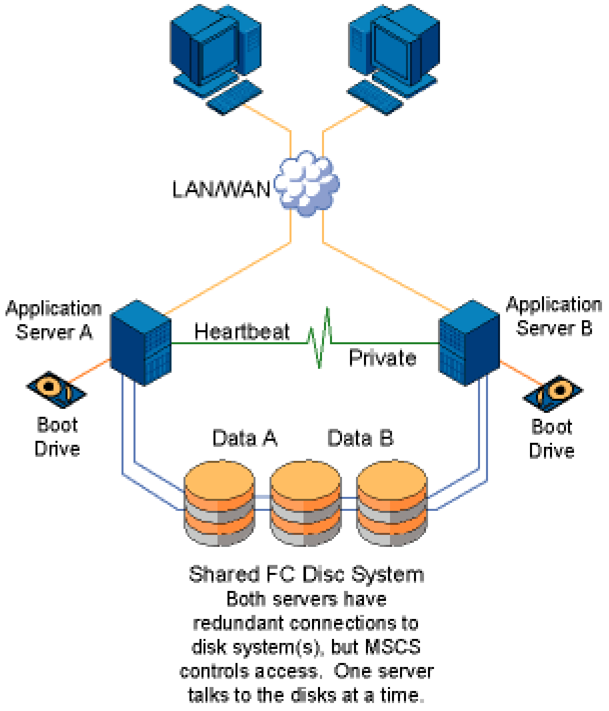
LAN/WAN
Application Server A
Heartbeat
Private
Application Server B
Boot Drive
Data A
Data B
Boot Drive
Shared FC Disc System
Both servers have redundant connections to disk system(s), but MSCS controls access. One server talks to the disks at a time.

Figure 1: A typical high-availability cluster.

Here, a cluster-aware application is configured so that it can run on either of the two application servers. Normally, the application runs on only one of them at a time, leaving the other server free to perform other tasks, undergo planned maintenance, and so forth. That "spare" server monitors the active one by means of a *heartbeat,* which occurs over a private network connection. Should the first server fail, the second one starts the application and takes over the workload. A shared storage system ensures that both servers can access the same application data, enabling them to run the application equally well.

Clusters can be complicated to build on your own, which is why some organizations tend to shy away from them. They require specially-selected hardware components that are designed to work with each other in this kind of configuration. Most major hardware vendors, however, offer certified, preconfigured cluster configurations that are basically plug-and-play, enabling you to take advantage of this business continuity model with less effort and hassle.

Application Continuity

Even without clustering, it's possible to make *any* critical application more highly available. There are a few key techniques for doing so:

- Move critical applications onto their own dedicated servers, and equip those servers with redundant hardware components (such as power supplies, network adapters, and so forth). This setup helps reduce the number of things that could cause the application to go offline, including unexpected interactions with *other* applications.
- Locate application data to external Storage Area Networks (SANs), which are themselves built to be highly-redundant. SANs can be built in a wide variety of configurations, enabling a wide range of availability in different scenarios.
- Centralize application data to a highly fault-tolerant data center. Consider replicating data to a different physical location, if possible. If not, ensure that the data center has redundancies in place for utility power, cooling, and other necessities so that it can continue communicating with application servers through an outage.

The broad availability of SANs and high-speed network interconnects means that application data doesn't *have* to live in close physical proximity to the servers that utilize that data. Moving data to a different location can help make it easier to come back online faster in the event of a failure.

Rapid Restore

The biggest traditional problem with backups is the time it takes to restore from them. Find the right tape, wait until it transfers the data, and hope it works.

Today, backup and recovery solutions are increasingly focusing on minimizing downtime. For example, disk-to-disk backup systems can back up *and* restore data exponentially faster than tape solutions, enabling you to restore *terabytes* of data in just a few minutes, if necessary. Tape backups can still act as a last line of defense by providing a durable, easily-portable means of storing backed-up data at an off-site location. Removable disk backups provide a middle ground: They're easily portable like tape but enjoy the speed of a disk.

Many companies are finding success with a new breed of "Backup 2.0" solution, designed to capture storage changes at a disk block level and replicate changes to a centralized backup server for safekeeping. Able to restore anything from a single file to an entire server in just a few minutes, these solutions are often themselves backed up to tape or replicated across the wire to provide redundancy and off-site storage capabilities.

Virtualization and Off-Site Recovery

Off-site recovery has long been a final line of defense for many organizations. In the event of a complete facility disaster, the technology team heads off to the recovery location, tape backups in hand, to start reviving the most critical portions of their infrastructure on rented equipment.

Virtualization has made this approach more affordable and effective. It's even feasible to build your own off-site recovery center simply by having a few powerful virtualization hosts. In a basic form, you restore entire servers to virtual machines—which can happen very quickly—to get key services up and running again. In more advanced cases, you might be able to migrate virtual machines from failing hosts to active ones in anticipation of a disaster.

In the most-advanced scenarios, two virtual machines can be kept in perfect synchronization over a high-speed network—even separated by as much as a kilometer or more. If the "active" virtual machine goes offline due to a failure, the "backup" virtual machine simply starts processing the workload. With zero downtime, this is true business continuity: keeping the business going *through* the disaster without the downtime required to *recover* from the disaster.

Emergency Management

Be ready with a plan in the event of an emergency. More and more vendors are available to help your organization deal with a crisis effectively and efficiently. For example, if you haven't outsourced corporate communications such as email, you don't want to have to rely on employees' personal email accounts on Gmail or Yahoo for communications. Instead, have a backup plan. Emergency notification vendors can provide two-way message delivery during a crisis, enabling key employees to remain in contact, coordinate activities, and respond to the situation. These vendors can often set up call-in centers where employees can leave messages for each other, helping to ensure contact.

Incident Management vendors can also help. These vendors manage external centers that are designed to coordinate team activities in the event of a crisis. Your teams will be able to communicate and collaborate, often using Web-based applications and portals. You can create and manage task lists, log status information, and share critical documents—including a library of response documents that are secured for your company's exclusive use.

This is the "soft" side of business continuity: making sure that, if something *does* go wrong, you're not dependent upon your team members all having up-to-date response documents, call lists, and other materials at their disposal. You're not relying on out-of-band channels of communication, and you're not at the mercy of "free" services to connect you with your team.

Business Continuity for the Modern Age

Business continuity will *always* include disaster recovery planning, as sometimes the best you can do for continuity is recover as quickly as possible. Technologies like rapid restore and off-site recovery can help minimize downtime when it's unavoidable, and outsourced crisis management services can help coordinate and manage that activity to ensure it is performed efficiently and safely.

To help *prevent* downtime entirely, you can turn to technologies like clusters and virtualization, along with the outsourcing of key services. These options keep your organization up and running *through* the disaster. All you need is a fresh perspective and a willingness to custom-tailor an availability and recovery solution for each critical aspect of your organization's technology infrastructure.