

TEN MUST-HAVE TECHNOLOGIES FOR CONTINUOUS IT AVAILABILITY

Does downtime mean lost productivity and revenues? If so, you need to implement the right tools to make sure your systems stay up when there is a disruption in normal service, whether caused by disaster or human error. Here's a list to help you get started.

1. Virtualized servers and storage for data backup

Server virtualization is a key technology for IT because it helps reduce the number of physical servers needed. This leads to easier management, lower-cost maintenance, reduced power consumption and better utilization. As an added benefit, virtual machines (VMs) can be copied to any other VM, whether or not it has the same operating system or applications on it. This provides a fail-over system if there is a disk or server crash.

2. Data snapshots

When you start setting up many VMs, keep in mind that they have to be backed up. Snapshot software is a simple, fast, non-disruptive solution. A snapshot is a point-in-time image of a drive with pointers to file locations. Snapshots can run multiple times a day and can be copied to an offsite location. Symantec's VMware Consolidated Backup lets you take a snapshot of an entire server running as many as 80 VMs.

3. Continuous data protection

Continuous data protection (CDP) technology is the best solution to prevent downtime and data loss. CDP backs up every change to disk as it's made. While it sounds ideal, the cost is still prohibitive for most businesses to use with every application. However, if you have individual applications with zero tolerance for downtime, CDP is the solution.

4. Deduplication

Deduplication is the easiest technology decision this year. It will pay for itself and reduce ongoing storage needs. Why? Backups create copies of files, including the same files day after day. Deduplication eliminates data that is already stored elsewhere on a backup. It can run on disk and tape backups, and will be available for archiving soon.

5. Encrypted backup

HIPPA data. Credit card numbers. Identity theft. There's no good reason to ignore encryption. A growing number of backup products are bundling it, such as Symantec Veritas NetBackup Server. NetBackup encrypts data on tape and disk backups using the latest encryption technologies. Encryption should run at a backup server so it doesn't affect production server performance.

6. WAN link controllers

WAN link controllers deal with threats you cannot prevent: those that bring down Internet connections. Link controllers automatically detect a WAN or Internet Service Provider (ISP) failure and redirect traffic to a redundant link without a pause in service. Be sure to arrange redundant Internet service through different Central Offices (COs), just in case disaster strikes the CO.

7. VPN spike capacity

If a disaster strikes and prevents your users from getting to the office, the corporate Virtual Private Network (VPN) will let users connect to the WAN and work remotely. But for cost reasons, most VPNs are not configured with enough capacity to support every user at once. No worries. Products like the SonicWALL Aventail Spike License Pack allows customers to immediately increase their remote user count temporarily in the event of a disaster. You won't have to rush to acquire new infrastructure or ration system access.

8. Mobile backup

You agreed to support PDAs and smartphones. What do you have to do besides back up phone numbers, email and Microsoft Office Mobile files? There are also contacts, text messages, photos, videos, voicemail, ringtones, Web bookmarks and speed dials. Hosted services allow IT to retain control. iDrive Pro replicates iPhones, and Dashwire Mobile backs up Windows Mobile, Symbian, Android and BlackBerry units. For a few dollars a month per device, you can rest easy knowing that backups and restorations will occur without your involvement.

9. Virtualized desktops

Virtualization saves money, reduces management effort and improves user access. Desktop virtualization separates the user interface from the hardware so the user can access their desktop from any device with an Internet connection. Since the desktop and data is stored on a server, backups and software upgrades are controlled centrally, a dream for IT. The downside? You need an always-on network and deduplication to manage the additional data on the server.

10. Remote system administration

LAN and WAN administration can keep you up long after your users are asleep. Remote administration is the answer. There are tools for managing servers, routers, VMs, desktops, laptops and smartphones, anytime and anywhere. NTRadmin from NTRglobal, Inc. lets IT administrators control devices remotely. NTRadmin can power data center equipment on and off, automate processes, deliver alarms, manage WAN components and monitor Internet connections. It's available by license or by using Software as a Service (SaaS).

If you're not using these technologies to protect your business, it's time to start adopting them now before it's too late.