Kaseya Automating IT

Kaseya BACKUP

SMB Compliance: Best Practices Using Disk-Based Backups

Kaseya BU/DR Solution Simplifies Disaster Recovery of Distributed Systems

Kaseya.com

SMB Compliance: Best Practices Using Disk-Based Backups

Kaseya BU/DR Solution Simplifies Disaster Recovery of Distributed Systems

The business world is growing increasingly flat, spreading even the smallest workforces over distance. Employees are seemingly always on the move, constantly meeting with customers or distributors and making sure the supply chain flows unabated. Salesmen rarely come into the office anymore, instead checking email from their PDA or cell phone and only coming into the office to attend meetings or to pick up a paycheck. Even your company's desk jockeys are getting into the action, telecommuting from home or the local coffee shop, able to access the corporate network from anywhere with an Internet connection.

Perhaps your organization is set up in a campus environment like a healthcare center, university or city government with staff spread throughout multiple buildings over several square blocks. However you structure your business, it is increasingly rare today for any company to house its entire workforce under one roof.

Despite this shift to a distributed model, it is important that every employee has access to the business tools and information they need to do their job. This responsibility falls to the IT organization—an increasingly critical component of any company's mission. However, managing a distributed IT infrastructure presents all sorts of complexity, consistency, compliance and cost issues. At the same time, backing up the mission-critical business data that is being created, stored and archived across an increasingly distributed geographic area is growing in importance as well, and is absolutely vital to the long-term health of the business and the ability to ensure compliance of industry and government regulations.

Without the peace of mind that comes with a robust backup and disaster recovery strategy that encompasses the entire organization, companies run the risk of limiting the productivity of its employees, shutting its doors for long stretches of time following a disaster, inconveniencing customers and being in non-compliance of government and industry regulations. The health of the business is directly tied to IT's ability to develop a reliable disaster recovery strategy for distributed systems.

In this white paper, we will discuss:

The problems associated with distributed backup solutions today

What companies should look for when deploying a reliable disaster recovery solution

Kaseya Backup and Disaster Recovery (BU/DR)

Problems with Distributed Backup

Even the smallest companies have robust local backup solutions in place that back up business data to either disk or tape. The solutions are relatively reliable and are reasonably easy to manage on-site. If a PC crashes, it is possible to recover the lost data once a replacement computer is procured, set up and reloaded with the appropriate software, user settings and drivers (though the process is extremely complex and labor-intensive). If any data loss occurs, it's usually just the changes that had been made since the last backup cycle, typically conducted over the weekend. Local file and database servers are backed up and recovered much the same way—if not with a little more complexity.

However, once a business outgrows a single facility and starts deploying systems in a distributed environment, all the rules go out the window. Despite the claims of major server vendors, the free remote management software that comes with the system is not reliable enough to satisfy even the most lax disaster recovery strategy. As a result, the backup process in remote offices is typically unreliable, requiring constant on-site tinkering and administration to keep the solution online and working properly.

Since most small businesses cannot afford to employ an IT professional at every location, the company either has to hire a costly contractor or tab an unsuspecting member of the business staff who has to be given cursory, on-the-fly training. This conscripted "administrator" is responsible for loading the media, configuring the backup software, administering the process on a consistent schedule and storing the media in a safe, secure location (usually the trunk of their car). Given that data protection is absolutely vital to business continuity and the long-term success of the company, the fact that anyone would trust this process to someone that is not trained to administer backups is troubling—no matter how competent they are in the other aspects of their responsibilities. Throw in the financial consequences of compliance failures, and small to medium business owners are just asking for an ulcer.

Technical Issues with Distributed Backups

Remote backups are difficult to fit in a reasonable backup window. As data growth continues to explode, the time it takes to reliably transfer files from a server or workstation to storage is taking longer and longer. This is an issue for even the healthiest and most robust backup processes. Imagine the problems a less reliable solution would have fitting in the window if it constantly has to stop or start over. If it takes your company 20 hours to backup the entire network, it is impossible to do a full backup each night without causing an interruption to end users. The alternatives are to either pick and choose what data gets backed up each night or to forgo nightly backups altogether.

Some companies choose to conduct backups during business operations when employees need seamless access to the files. However, most backup solutions require a reboot, knocking end users offline and causing availability issues. Backups also drain computing power away from critical business applications, slowing the performance of employees using the applications. If conducted during a crucial time—such as the start of a sale—the performance hit can be noticeable, affecting customer service.

Complete coverage is also an issue for distributed companies. Salesmen that spend most of their time on the road need to bring their laptops in the office to be fully protected. Employees that work from home, or bring their laptops home over the weekend, risk not being covered as well. Any data protection strategy that puts backup responsibility on the end user is doomed to failure. People either are careless or simply don't care.

Inefficient Backups = Inefficient Recoveries

This inefficient, complex and costly process seriously affects your company's ability to recover systems in case of data loss. By taking data protection out of the hands of trained IT professionals and putting into the hands of inexperienced business staff, companies can not reliably know that backups are being done consistently or properly. Backups are failing every day in branch offices across the country unbeknownst to headquarters, and unfortunately, senior leadership usually doesn't find out until it's too late.

Assuming that the backups have been done correctly, data can now be recovered. Unfortunately, the recovery process is much more complex and labor-intensive than the backup process. The data needs to be found in the archives, loaded and recovered locally and then restored to the original device. If the server or workstation needs to be replaced, it needs to be loaded with an operating system, business applications, user settings and drivers before the data is loaded. Chances are that the conscripted administrator in the branch office has not been fully trained in this process. In order to reliably recover lost data, a local consultant needs to come in or an administrator needs to travel from headquarters. Both options are expensive and can add days to the recovery process.

Despite this inefficient, costly process and the dire consequences of not doing backups right, many companies refuse to deploy a reliable, consistent disaster recovery solution that encompasses the entire organization from corporate headquarters to branch offices.

Characteristics of a Reliable Data Protection Solution

Companies need to deploy a reliable backup and disaster recovery solution that gives them complete coverage throughout the organization, ensuring that every system on the network—from corporate headquarters to the most remote branch office—can be easily recovered in case of data loss. The solution needs to take administering responsibility out of the hands of the end user, allowing trained IT staffers to manage backups centrally while automating and simplifying much of the process. It has to work in the background without interrupting the daily duties of your employees, and it has to fit each backup cycle within the allotted backup window.

Most importantly, your disaster recovery solution needs to enable fast, efficient restores so your employees can get back up and running quickly in case of system or data loss. And the solution needs to ensure compliance of any government or industry regulations that affect your business.

Central Management

Central management ensures that all servers and workstations are protected under your company's disaster recovery strategy—including systems in branch offices, mobile devices and laptops that are used by traveling employees. Given the distributed nature of IT infrastructure today and the demands end users put on technology, it is essential that the IT organization is able to accurately detect and protect every system—no matter where it sits on the corporate network or how often it operates outside the firewall.

Intuitive and Simple Interface

The central management console also needs to be simple and easy to administer without requiring additional training or storage expertise. Automation can go a long way in easing management complexity, eliminating the most common cause of failed backups: human error.

Complete Coverage

Ensuring complete coverage enables seamless business continuity in case the entire organization is crippled in the event of a widespread data center disaster. What good is having your billing department up and running if your sales force can not fill orders? Ensuring complete coverage through central, simple management ensures that the entire supply chain can recover quickly.

No Interruption to End Users

Most backup and disaster recovery solutions require a reboot after each backup, knocking end users off-line for a few minutes each day. Even planned downtime can be disruptive, especially if it occurs right in the middle of a customer call or transaction. Each failed business process affects employee productivity as well as customer satisfaction. If your front-line employees do not have continual access to the tools and information they need, you're truly not a 24x7 business.

In addition to having limited impact on network resources that affect performance, the backup and disaster recovery solution should be able to schedule backups when it is most convenient for both end users and administrators. Existing solutions often give companies the ability to schedule backups overnight or during the weekend, but require an administrator present to start and monitor the process. Make sure you choose a solution that neither inhibits the end user nor requires administrators to work overnight or on the weekend.

Protection from Widespread Data Loss

It is important that your company is able to protect itself from both large and small instances of data loss. Make sure your solution provides volume-level as well as folder-level and file-level backups and recoveries. How efficient is it to recover an entire Exchange mailbox if an end user only deleted one important customer email?

It's also important to protect your company from widespread disaster. Most experts recommend that companies store a copy of their backup data at least 90 miles away in an off-site disaster recovery facility that will be safe if a regional event such as a hurricane, flood or earthquake renders the main data center inoperable. Contingencies should be put into place to quickly set up a new data center and recover the backup sets.

Ensure Compliance

Many government regulators and industry watchdog groups require some companies to show they can recover any file or piece of data up to seven years old, putting a huge strain on their backup and disaster recovery solution. Having the ability to search, identify and recover data from any point in time is vital to remaining compliant.

In addition to giving your company this granular recovery ability, it's important that your backup and disaster recovery solution allows you to do it efficiently, without requiring unnecessary manpower or network resources. A powerful reporting engine is also important, giving administrators the ability to efficiently conduct compliance audits regularly. A highly searchable backup data set ensures that proving compliance isn't as complex and time-consuming as ensuring compliance.

Your CIO will thank you.

Efficient Backup Window

Most backup solutions—especially ones that backup to tape—are extremely inefficient, struggling to complete the backup cycle in the allotted window. As a result, companies often have to choose which data they want to backup, leaving large volumes of less mission-critical data unprotected. The other option is to do just one backup during the weekend instead of nightly backups, leaving new files and data created or edited during the week vulnerable to loss. The weekend backups also make it harder for employees to work over the weekend if the entire network is being backed up from Friday evening to Monday morning.

Make sure your backup solution offers incremental backups—the process of only backing up new and edited data. This drastically reduces the amount of physical data that needs to be replicated, allowing efficient, nightly backups.

Quick, Reliable Restores

What good are backups if a company isn't able to efficiently recover the lost data when needed? Most disaster recovery vendors focus on making backup more reliable and less invasive to the business but completely ignore the complexity surrounding recoveries. It doesn't matter how fast you can back up data if it takes weeks to recover it. Fast backups are impressive (and important), but it's fast recoveries that save the business.

It's also important that disaster recovery doesn't stop at restoring data. If a laptop is fried, loading a new system with data is only part of the process to getting it functional again. The laptop needs to be loaded with an operating system, business applications, user settings and drivers. A solution that enables quick restorations of the entire system is much more valuable to a company that cares about getting its employees up and running quickly.

Vendor Neutral

Most small companies procure workstations as they need them, using deals and new pricing to make brand decisions. The result is a mix of HP, Dell, IBM Lenovo and Sony machines. Following a disaster, companies may not have access to the same percentage of brands, having to make do with what is available. A solution that enables restores to dissimilar hardware allows companies to recover on the fly more quickly without having to worry about interoperability issues.

Scalable

Growth is always on the minds of the IT department, making sure the expanding workforce is equipped properly and the infrastructure is able to support the additional performance and availability demands. Systems management can quickly grow out of control. Backup is much the same way. The IT department has to make sure that the network is fully protected and all new systems are folded into the disaster recovery strategy. Additional backup media needs to be deployed and the backup window needs to be re-engineered to accommodate the increase in volume.

Instead of doing this on your own, deploy a reliable backup and disaster recovery solution that automates much of this process and can scale efficiently as the business continues to grow.

Kaseya Backup and Disaster Recovery

Kaseya Backup and Disaster Recovery (BU/DR) provides real-time automated disk backup, disk imaging, file level backup and bare metal restore for Windows servers and workstations. Unlike conventional file-based only products, Kaseya BU/DR creates an image of the entire system state—including operating system, business applications, user settings, drivers and data—giving administrators the framework to completely rebuild a downed system in less than an hour.

The solution is part of Kaseya's IT Automation Framework, giving administrators the ability to deploy, configure, manage, monitor, secure, back up and restore distributed systems from a single management console.

Integrates with IT Automation Framework

The BU/DR module integrates seamlessly within the Kaseya IT Automation Framework, giving administrators a consistent feel and look to managing distributed systems. The consolidated interface allows companies to monitor, manage, audit, secure and backup all systems on the network from a single management console, eliminating much of the complexity and redundancy associated with ensuring the health of distributed systems. The simple framework also reduces the need for additional training for IT staff, giving employees with limited expertise all the tools they need to ensure business continuity and compliance.

By integrating backup and disaster recovery with IT automation and systems management, the IT organization is able to streamline basic administrative tasks through automation. The complete solution is more reliable, more robust and is able to provide greater coverage. A powerful scripting engine allows administrators to automate and combine tasks. For example, if Windows announces a vulnerability to Windows NT machines, Kaseya can search the network for these systems and do a full backup before a patch is downloaded and deployed. The last-minute backup ensures that the systems can be restored to their original state if there is a flaw with the patch—which can be a common occurrence. In another example, the Kaseya solution can audit a PC to make sure it has enough hard drive space and memory to support specific business applications before an administer restores to the machine. Otherwise, a system lacking the basic requirements could continue to crash or run slowly.

The integrated solution reduces administrator workload and helps avoid human error while ensuring reliable backups. More efficient administrators are more productive, provide better IT service and are more apt to meet the business's performance and availability service level agreements. The integrated solution also helps ensure compliance, giving administrators the visibility to

enforce security policies consistency throughout the organization and generate reports on demand for quick, reliable compliance auditing.

Remote Access

Kaseya gives administrators complete visibility and access into distributed servers and workstations from a central management console, allowing them to remotely administer backups and recoveries without having to physically visit the system. Coupled with powerful automation technology, this remote administration dramatically cuts back on manual maintenance and travel times between facilities.

Backup administrators no longer need to physically walk from system to system to deploy, set up and test backup software. In addition, recoveries can be completed remotely in less than an hour, eliminating the wait time usually associated with full restores. An accurate scheduling engine can start the backup process in the late evening when the impact on end users is minimal without requiring an administrator on site.

Auto-Discovery

Making sure all systems are protected is a vital component of any company's disaster recovery strategy. Kaseya's inventory management and auditing module provides administrators with the peace of mind that every system on the corporate network has been identified and is being reliably backed up. The module also ensures that systems are loaded with the required components (operating system, storage capacity, memory, security policies, etc.) to handle the backup load. This visibility into all systems on the network also helps with compliance efforts, giving companies a reliable and accurate tool for conducting regular audits and proving compliance status internally as well as to regulators.

Off-Site Vaulting

Kaseya provides geographic disaster recovery protection through off-site vaulting features, protecting companies in case of major disasters such as a fire, flood, hurricane or earthquake. Copies of the backup images are automatically replicated over distance to an off-site facility and are easily recoverable in case the original backups are lost. The process is completely automated, eliminating the need for an administrator or member of the business staff to remember to take media home or drop them off at a storage facility.

Bare Metal Restore

During the backup cycle, Kaseya BU/DR creates an image of the entire system state—including operating system, business applications, user settings, drivers and data—allowing administrators to completely restore a machine to its exact status just before the last backup. A sales rep that watched his laptop burst into dozens of pieces after dropping it down a flight of stairs can have a completely rebuilt computer within an hour that performs and feels exactly like the previous piece of hardware.

Point-in-time Recovery

Kaseya's flexible recovery features allow administrators to restore large volumes of data or more granular recoveries on the folder or file level. The solution's incremental backups enable point-in-time recoveries, allowing systems to be rebuilt to a set point in the past (as long a successful backup was conducted at that time). This is useful when an employee inadvertently saves over a previous version of a file or if a software upgrade goes horribly wrong. Point-in-time recovery is also helpful for compliance issues, allowing a company to recover a file from the past seamlessly without having to rummage through a warehouse of file cabinets or reels of backup tapes.

Low Footprint

Kaseya operates behind the scenes without end users aware that their system is being monitored against set performance and availability service levels. Backups are conducted seamlessly without the need to reboot; ensuring end users experience no planned or unplanned downtime. Backups can be automated or conducted on demand and can be scheduled for off-peak hours or a time that is least intrusive to end users without an administrator present. The solution can also be left unattended to recover lost files within minutes.

The Kaseya client is deployed and updated automatically and remotely, eliminating the need to travel to branch offices or across a campus environment. Unlike other data protection solutions, no additional hardware or software is required.

Using Kaseya BU/DR for Compliance

Integrated Health Management Services (IHMS), a leading government-based billing and eligibility services company geared toward healthcare organizations in the Southwest US, needed to improve IT support and backup to its more than 100 end users spread out in six geographically-diverse offices. IHMS helps hospitals reduce bad debt and increase cash through government-based eligibility, billing, and follow-up programs, making it essential that the company's staff have access to the business software and patient data they need to do their job. It is equally important that the company protect that patient data and remain in compliance with HIPAA.

After deploying Kaseya and integrating systems management with its backup system, IHMS was able to efficiently backup patient information and its IT systems in its data center in Phoenix as well as in branch offices in Denver; Tucson, Ariz.; Santa Barbara, Calif.; and Pasadena, Calif. By being able to access any system on the network from a central management console and remotely conduct backups, administrators can manage and protect distributed systems without having to travel across state lines.

"Kaseya allowed us to shift our focus from reactive to proactive management, streamlining IT operations and improving service to end users," said Larry Roberts, Principal and IT Manager, IHMS. "By ensuring the protection of data and the security of our systems we can rest assured that our patients' personal information will not fall into the wrong hands."

Kaseya's tracking and event log features provide IHMS with a reliable account of assets that store sensitive patient information, who has access to the information and what maintenance has been done on the systems. Roberts can even set alarms for suspicious activity, alerting him if data has been compromised before the leak can do much damage.

Administrators can also proactively comply with the regulation by making sure all systems are secured through up-to date patching, software updates and systems health. By eliminating vulnerabilities before they become an issue and ensuring that data can be recovered easily, IHMS can ensure they are protecting patient data to the letter of the law. Once a year, IHMS hires third-party auditors to validate the company's compliance status, a process that is much easier through documentation by Kaseya.

Conclusion

Data protection is growing increasingly complex due to the increased reliance today's business environment is putting on distributed systems. Backing up data remotely is difficult, requires a lot of time and resources and puts an unfair burden on the business staff—who are often pressed into IT service. As a result, most companies deploy an ineffective disaster recovery strategy that doesn't protect the entire organization from data loss or meet strict government and industry regulations. The consequences include unproductive employees, poor business continuity, a loss of revenue and non-compliance.

Companies need to look for remote backup and disaster recovery solutions that allow trained IT professionals to remotely administer backups from a central management console. The solution needs to integrate with the systems management framework, allowing administers to monitor, maintain, audit, secure, backup and recover systems from a single, integrated interface. The solution should ensure that every server and workstation in the IT environment is protected—regardless of the physical location of the system—and copies of the backup images are archived in a secure off-site facility.

The solution also needs to enable reliable, fast recoveries of systems from the ground up—allowing companies to get back up and running quickly following a disaster. However, just as importantly, companies need the granular ability to recover single files or folders in case of smaller instances of data loss caused by viruses or human error. Finally, the backup system should not interfere with end users, instead working seamlessly in the background with a scalable and small footprint.

Kaseya's BU/DR module takes all these requirements into account, giving companies an intuitive disaster recovery tool that encompasses the entire organization and ensures business continuity. It does this seamlessly, efficiently and in compliance without being a burden on the business or the bottom line.

About Kaseya

Kaseya is a global provider of IT Automation software for IT solution providers and corporate IT organizations that benefit from deploying Kaseya's systems management capabilities. Kaseya allows businesses to proactively manage distributed IT infrastructure easily and efficiently with one integrated Web-based platform. Kaseya's technology has been deployed on over 1 million machines in more than 25 countries around the world.

For more information visit www.kaseya.com or contact Kaseya at HYPERLINK "mailto:sales@kaseya.com" sales@kaseya.com.