SIX QUICK TIPS

Automating Disaster Recovery

Planning, Prioritizing & Testing Are Key To Putting Disaster Recovery On Autopilot

Most companies have established some level of DR (disaster recovery) program, but more and more enterprises are learning the value of automating the process. Before you leave your manual system behind, check out these tips to be sure you're ready to make the jump to an automated program.

✔ Get Buy-In

Before you begin designing an automated disaster recovery plan, it's critical that your organization's key stakeholders agree on the project's scope and objectives and that everyone understands the potential impact of budget constraints. "Create a document that management in your company signs off on which details what you're protecting, to what degree it's protected, and in what way that protection may be exceeded given a certain disaster," advises Mike Chase, J.D., CTO at dinCloud (www.dincloud.com). "Later you will find that costs will mitigate the degree of protection desired, and when a particular disaster exceeds the degree of protection that everyone originally found acceptable and signed off on, you will not be left alone holding the bag."

✔ Prioritize

Most enterprises can't back up everything, so you may need to determine which systems or datasets are most critical. "You should start with a priority list before you talk about anything else," says John F. Pearring, manager of sales and marketing at STORServer (www.storserver.com). "Know which systems in your environment you have to restore, and the reason. Some people think they have to restore everything, but it's not true. You don't." He says that, once less important functions and easily replicated data are removed, "the list of applications or systems that are needed in a disaster recovery scenario will be smaller than you think."

"Always start with the basics and work upwards," suggests Heinan Landa, CEO of Optimal Networks (www.optimalnetworks.com). He says IT groups should examine their infrastructures to identify which areas make sense to focus on first. "What is the easiest and most effective thing to automate? Does the automation provide you with advantages over performing it manually? What sort of checks will you have on the automation? Start with the simpler things, like file backup, and get them working, and then move towards the more complicated things." By fine-tuning your processes on less complex systems, you'll be ready to take on tasks that have multiple layers or require more oversight.

✔ Watch The Timing

"When selecting an automated DR solution for applications, be sure to confirm that the automation works in both directions and within acceptable time frames," says Josh Mazgelis, product marketing manager at Neverfail Group (www.neverfailgroup.com). He cautions that restoring services may be quick, but bringing systems back to production often requires more time and manual intervention. "I've seen a lot of customers test their DR solution's ability to get to the DR data center, but then simply turn the production servers back on without using the DR solution's given process. Being able to failover in minutes becomes much less valuable when it takes hours or even days to fully get back into the production data center." He believes that by getting a more complete understanding of each automated solution's design, data center managers will be better equipped to choose the right one for their needs.

✔ Virtualize

As virtualization technologies become more mature and robust, Chase encourages data center managers to rely more heavily on them when automating their disaster recovery programs. "Virtualize everything," he says. "Not just your servers, but your desktops, applications, storage, and voice system."

If a disaster forces your business to relocate or spread its operations across several areas, virtualization may offer fewer location-based restrictions and allow your organization to get back on its feet more quickly. "Leaving part of your business behind really isn't an option and only adds to the chaos," Chase says. "Plus, it's easier to move a virtual infrastructure than a physical one. It costs less, too."

✔ Remember Local Data

Individual workstations hold an enormous amount of information in many organizations, most of which isn't covered in an automated DR plan. "What's usually left out is the data that people have sitting on workstations that isn't on a server," Pearring says, adding that the common solution—to advise people that their local data won't be backed up—is ineffective, because it often leads to disgruntled executives who've learned their important data was lost. "You can't assume you've solved that problem just because you have a rule," he says.

Pearring adds that trying to get everyone to use NAS is also asking for trouble. Only a DR plan that incorporates all areas where information is stored will be able to give you a reliable recovery point in an emergency.

✔ Test, Test, Test

The only way to ensure your DR program works is to test it. "The actual disaster recovery plan begins with the test," Pearring says. "There are things you're going to miss in a disaster recovery plan [if] you do not [test] it." He says that every recovery test, no matter how sophisticated, is likely to return errors, and ramping up employee participation during testing will help you understand how the plan is likely to hold up during an actual emergency.

"Regular testing of DR solutions is a very important task for many reasons," Mazgelis adds. "Even with a fully automated solution, IT needs to know how to enact the process, what to expect from the process, and how to enact the process of moving back to the original servers." He also points to the benefits gained by pinging the environment for changes. "It is inevitable that something in the environment has changed since the last test, and sometimes those changes can affect the ability of the solution to work properly or affect the ability of the protected applications to work in the DR data center."

Landa believes the complexity of modern systems doesn't easily lend itself to a "set it and forget it" approach and says that testing is the only way to confirm the program is working.

Most Practical Tip:

✔ Remain Vigilant

Heinan Landa, CEO of Optimal Networks (www.optimalnetworks.com), recommends that data center managers maintain what he calls a "healthy skepticism" about automated disaster recovery and says they should be constantly asking if their plan really works. "I also believe that you need to properly establish recovery time objectives and recovery point objectives for each application or type of information or service that you are trying to automate the disaster recovery for, and see if it really bears out in live testing," he says.

Most Overlooked Tip:

✔ Monitor Connectivity

It's important to keep network connectivity in mind when implementing an automated disaster recovery program. "With the multitude of firewall rules, network subnet routes, and IP-specific whitelisting, the move to a DR site often identifies something that has been overlooked," says Josh Mazgelis, product marketing manager at Neverfail Group (www.neverfailgroup.com). He says that issues such as mail relay accessibility and VPN access sometimes become unexpected sticking points. "During testing, IT staff become focused on making sure that applications are running, and sometimes it's not until the users get involved that those connectivity problems get highlighted."

BONUS TIPS:

✔ Know your enterprise.

"Document your entire infrastructure first," advises Mike Chase, J.D., CTO at dinCloud (www.dincloud.com). "You can't plan to protect what you don't know you have." Remember to include legacy systems and individual workstation data.

✔ Start with the easy stuff.

"I would say that the easiest things to automate are backup systems," says Heinan Landa, CEO of Optimal Networks (www.optimalnetworks.com). "From there, everything that you automate requires more attention and more time on an ongoing basis."