BEST PRACTICES FOR CLOUD BASED DISASTER RECOVERY
OR IT MANAGERS, disaster recovery has always been high priority, however the new IT landscape and increased deployment of cloud has complicated the management for cloud-based disaster recovery. In this e-guide, learn what the experts suggest are the best management practices for cloud-based disaster recovery, such as properly configured provisioning, cloud bursting and failover. Learn what these can do for your DR plan as well as why cost should not be a deterrent when implementing DR in the cloud.
MANAGING CLOUD-BASED DISASTER RECOVERY

After you’ve defined recovery point objectives and recovery time objectives and tested your disaster recovery methods, maintaining cloud-based DR requires a considerable amount of management -- even if a disaster never strikes.

The key to successful disaster recovery management involves bringing systems online and restoring them according to service-level agreements (SLAs), meeting RPO and RTO goals and mitigating results of your business impact analysis (BIA).

But before disaster actually hits, it’s important to know where -- physically and virtually -- underlying systems such as servers are located, which end users and IT staff can and need to access them to restore service, and what other components, such as network switching, routing, firewalls, etc., are central to the disaster recovery plan. For example, you should have a directory system in place such as Active Directory or OpenLDAP to manage user authentication, database systems to store data and end-user access points to obtain data.

The easiest way to manage these aspects of DR is to have a three-pronged provisioning protocol in place. First, you need to bring the underlying directory
system online. Next, bring up database systems and then bring back application servers. Finally, you are ready to restore data.

In a manual disaster recovery process, the process of restoring data can take hours per system. With virtual machine-based backup to the cloud, it’s as simple as taking a VM that’s located in the cloud, making it available and then powering it on. Point-in-time, snapshot-based VMs that power up and take over for downed servers have taken the place of tape backups.

It is the DR manager’s responsibility to ensure that, in addition to testing the validity of the VM-based recovery systems, provisioning is properly configured. Automated provisioning, or having VMs start automatically, allows you to meet SLA-based RPO/RTO metrics. You then can use the central log interface built into most cloud and virtualization platforms to document the testing process and results to verify you’ve met SLAs.

While this sounds very complex -- and it can be in large environments -- cloud computing offers small and medium businesses a level of efficiency that traditional backups cannot match. The typical SMB environment often is a flat network with minimal complexity (virtual LANs, etc.). Using a third-party cloud provider that specializes in recovery greatly reduces the time and effort involved in setting up and testing a product.
DR in the cloud is flexible, so IT teams can monitor, test and adjust it without affecting production systems. This makes disaster recovery in SMBs much less labor intensive, a welcome benefit in businesses that can scarcely afford a fully staffed IT department, not to mention a dedicated DR group.

**COST SHOULDN’T PREVENT GOOD DISASTER RECOVERY**

The high cost involved in implementing a solid disaster recovery plan often forces companies to stick with traditional backup and restore methods. While having high RPO and RTO numbers, which indicate a need for quick recovery, is a perfectly valid justification for keeping the old systems in place, cost shouldn’t be an issue.

As the cost-per-GB of cloud storage continues to decrease, the cost of media for tape backups remains roughly constant. Backup devices, such as disk-to-disk-to-tape systems, robotic libraries and others backup products, are expensive to replace. When the time comes to replace them, SMBs often need to examine the cost of storing data in the cloud for backups. That may also be the time to consider implementing full DR in the cloud. This shift in the cost structure, the need to perform a BIA and the relative ease of moving to cloud-based DR make the change an attractive, even compelling, option.
WHAT CLOUD BURSTING AND DISASTER RECOVERY MEAN FOR HYBRID CLOUD

If you ranked certain cloud features by the total revenue they could generate or the total user spending they could affect, cloud bursting and failover would be at the top of both lists. Many enterprises consider these two features equally important and find that the processes can support each other. In fact, the best strategy for hybrid cloud deployment is to combine cloud bursting and failover.

Cloud bursting, or workload overflow processing, occurs when an application’s presented workload exceeds its capacity. It allows an enterprise to spin up additional instances of the application in the cloud to relieve what might otherwise be a detriment to workers’ quality of experience. It’s a perfect example of how public cloud resources can augment internal IT resources, and it makes economic sense if it avoids costly capacity oversupply in the data center.

Cloud bursting requires two key technical elements: an application design that permits multiple instances to run at a time, and a mechanism to load balancing work among all the instances -- whether they’re running in the data center or the public cloud.
Failover, or disaster recovery, in the cloud also makes sense to buyers. Many enterprises already have considered or partially implemented standby data centers to keep their applications running in case a major failure disables some or all of the normal data center resources.

In a failover strategy, the emphasis is often on major incidents, such as hurricanes or power failures that take out an entire geographic area. In many cases, there’s an expected outage period while an enterprise shifts from its primary resources to the standby. In most cases, the applications will be running in one place or the other and traditional mechanisms such as the domain name system (DNS) can redirect work to the standby data center on a failure -- then back to the production data center when the failure has passed.

Clearly, cloud bursting represents a more agile approach for a disaster strategy. If growth in an application’s workload can trigger cloud bursting, a reduction in available resources to the application -- server or even data center failure -- could also trigger it. This DR strategy could deal with not only a complete data center failure but also limited equipment, software or even network failures. Overall, successful cloud bursting is a useful strategy for building hybrid cloud applications.
Creating a Robust Cloud Bursting Implementation

Issues associated with resource failures, not growth in application workloads, help determine whether cloud bursting can work to build hybrid apps. Users need access to any additional copies of an application, and the copies require access to databases and other resources. Are both of these conditions possible using cloud bursting in disaster recovery mode?

User access to these multiple app copies requires a form of load balancing. In most cases, enterprises would include a Level 3 switch, application delivery controller or similar device in their data center between the WAN gateway and data center servers. This device would then switch work among copies of an application as needed. If cloud bursting is supported, as it sometimes is, by connecting the public cloud “behind” these on-premises load-balancing devices, then loss of the data center will not only result in the failure of the servers but also of load-balancing devices. In this case, there will be no way to access public cloud resources.

Instead, the best approach to create a robust implementation of cloud bursting is to start with a network-based load-balancing strategy.

Load Balancing as a Service is a new feature in the Grizzly release of OpenStack and is increasingly being implemented by cloud vendors. Savvy users
could also build such an application and host it in the cloud. With this approach, all load balancing occurs in the cloud, with data center application resources linked to cloud resource allocation. That means a data center failure won’t result in a loss of application connectivity.

The issue of data or application access is more complicated. In workload-driven cloud bursting, it’s safe to assume that app data is still available in the data center and cloud-based copies of the application can access it. If a resource failure triggers cloud bursting -- particularly a failure that takes down an entire data center -- then database resources in the data center are unavailable, and cloud copies of the application cannot access the data.

Moving a company’s entire database to the cloud is not likely practical because of cost, security and compliance reasons. The only alternative is to improve the reliability of the database elements of applications; protect data storage and query processors with additional backup power and cooling or maybe even provide for hot-standby copies of key application data in alternate locations. While this will certainly add to the cost, it will still almost certainly be less expensive than maintaining a complete backup data center.

Both cloud bursting and DR will likely demand some application optimization. Online transaction processing may need to be adapted to update multiple
database copies to maintain a standby copy that’s up-to-date. Enterprises may also need to analyze application workflows to understand which app components can be replicated to improve performance and reliability, as well as how to maintain data integrity if multiple components are accessing the same database at the same time. While these types of application issues aren’t new to seasoned architects, it’s still possible that cloud bursting and disaster recovery processes will demand some new accommodations. It’s even more likely that an application that accomplishes both at the same time -- cloud bursting and failover -- will require special design. Testing and review are critical to achieving business goals.
FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web’s largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more — drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.