

STORAGE SWITZERLAND BRIEFING REPORT

COMPLETE DR FOR THE MID-MARKET



Eric Slack, Senior Analyst

Most companies do regular backups. Sometimes they can even get restores accomplished in a timely fashion from those backups. But many don't have an adequate recovery plan. Even after their data has been restored it can still take days for a company, especially in the mid-market space, to get servers up and critical applications on line again.

Whether it's replicating data to a remote location, sending removable media off-site or simply having a standby server in the primary location, even small companies need to make sure their businesses can recover quickly when an outage occurs. [QuorumLabs onQ appliance](#) can provide the insurance that comes with a solid disaster recovery plan.

There's an old vaudeville routine that includes the line: "It's not the fall that kills you it's that sudden stop at the end". An analogy to this can be found in IT, "It's not the lack of a good backup that kills a company, it's the lack of a good recovery" - at least a timely recovery.

It's true, most companies that don't do a good job backing up their data will also have recovery problems. But the

point here is that even if companies DO have an adequate backup infrastructure, many will still fail when their mission critical infrastructure goes down. The reason is they don't have an adequate recovery system. Even being able to restore a backup isn't enough (which in most studies has a 15% chance of failure itself), most companies have to stand up servers, reload applications and restart critical services. Often, the process and time required to accomplish these steps are not well planned for, or overlooked altogether.

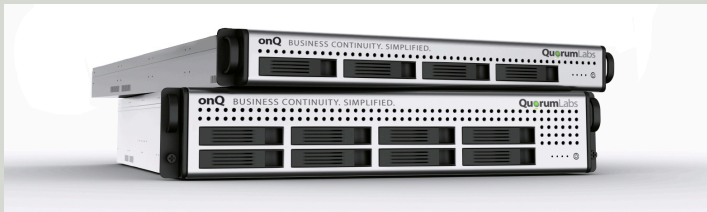
Backup vs Restore vs Recovery

It's not just about backup, it's not just about restore, it's about recovery of the data and the applications. Whether it's continuous data protection (CDP), high availability (HA), redundancy, hot spares, etc., big companies know how critical their recovery time objective (RTO) is and they spend the money required to keep it within an acceptable window. The maximum allowable downtime for critical IT services that a company can endure is the criterion for setting this RTO.

Unfortunately, mid-market companies don't often have this level of understanding, and many don't have the resources these traditional methods required anyway. QuorumLabs' onQ appliance is an alternative way for these organizations to get real downtime recovery, without the complex infrastructure or the price tag.

onQ Appliance

QuorumLabs' onQ is a 1U or 2U server and storage appliance that maintains ready-to-run VM clones of critical servers and applications. Configurations start with a quad-core, 1U appliance with 16GB of memory and enough storage to support seven primary servers. For larger companies, 2U configurations are available with up to 12 CPU cores, 128 GB of memory and 20TB of usable storage capacity. Dual power supplies and four GbE ports enable the onQ appliance to provide DR protection for up to 40 primary servers, depending on combined loading and desired performance. Multiple onQ appliances may be used to scale even higher and each onQ appliance supports on-the-fly disk replacement, enabling it to sustain a single disk failure without disruption.



Plug and play operation

To get going, an onQ appliance is connected to the primary LAN and a lightweight software agent is installed on each server which needs to be protected. OnQ starts creating cloned copies of the server OS, applications and data files for each server. It also creates Recovery Nodes for each server; these are the VM-like server instances that can be started with a single click. Using snapshot technology, the cloned copies of these files are kept up-to-date automatically, with incremental changes of each file sent from the source servers as often as every 15 minutes.

When an event occurs that requires recovery, a single click will start the virtual Recovery Nodes for any affected servers and reconnect users automatically. Typical recovery time is 5 minutes or less. This kind of response would certainly qualify as "high availability" for most of the companies in this mid-range space, and many larger organizations as well. In addition, point in time copies of data and system states are also kept, allowing a file to be restored to a previous version or an entire system to be rolled back to a prior state.

Remote site protection

A second onQ appliance is typically set up at an off-site location to provide DR protection in case the primary data center is taken down. In a similar way that the primary site appliance stays updated with the protected servers, the DR site appliance is also automatically updated. These incremental changes are replicated at the primary appliance, encrypted and sent over the WAN to the secondary appliance. With updates between the primary and secondary sites occurring every time local updates do, the QuorumLabs solution can provide an Recovery Point Objective of as little as 15 minutes.

DR Testing and Monitoring

Another aspect of downtime recovery that typically escapes all but the largest users is testing and monitoring. Like a spare tire that's flat, a DR system that hasn't been maintained can provide a false sense of security. For this reason the onQ appliance Recovery Nodes can be tested at any time in a virtual test network with a single click. In fact, this task can be configured to occur automatically each day. This ensures that changes to primary application servers are maintained in the DR system. Also, onQ appliances are continuously monitored by QuorumLabs and alerts are sent out automatically if anything is out of the normal range.

Problems short of a Disaster

In most cases a natural disaster is not the likely scenario that causes critical applications to go down. More often server or storage hardware failures, data corruption or human error are the things that happen. The server room doesn't have to be under 2 feet of water for it to be a real disaster for a smaller company. In these situations the onQ system can get users or customers back on line with business critical services. And if a tornado or earthquake does strike, having a second appliance in a secure location can handle that as well.

Storage Swiss Take

Data protection, backup, disaster recovery and even business continuity are terms that are often used interchangeably. However, for the company that loses one or more critical applications it's obvious they're not. Simply having a backup stored off-site doesn't guarantee these applications will be up and on line fast enough to keep their business from suffering a substantial loss. It's truly a false sense of security.

Like insurance, a DR plan needs to be comprehensive, full time and reviewed regularly to make sure it's still effective. Unfortunately, many companies, especially in the small and

About Storage Switzerland

Storage Switzerland is an analyst firm focused on the virtualization and storage marketplaces. For more information please visit our web site: <http://www.storage-switzerland.com>

Copyright © 2011 Storage Switzerland, Inc. - All rights reserved