Orchestrating your Disaster Recovery with Quorum onQ

Contents

Orchestrating your Disaster Recovery with Quorum onQ

Chances are that you are dissatisfied with your current backup solution, as half of those surveyed by NetApp have stated. You probably have a pile of tapes or disks that represent you faithfully copying your files using a traditional backup software utility. But when disaster strikes and an entire server goes south, getting a working server online quickly and without a lot of running around isn't going to happen. And chances are that the recovery process is so tortured and involved that you are lucky if you can do a full recovery test procedure once a year.

This isn't news to many of you. According to another survey, less than a third of the respondents have actually ever tested their disaster recovery (DR) plan. Ever. And only 16% test their DR plans even monthly. That is somewhat disheartening.

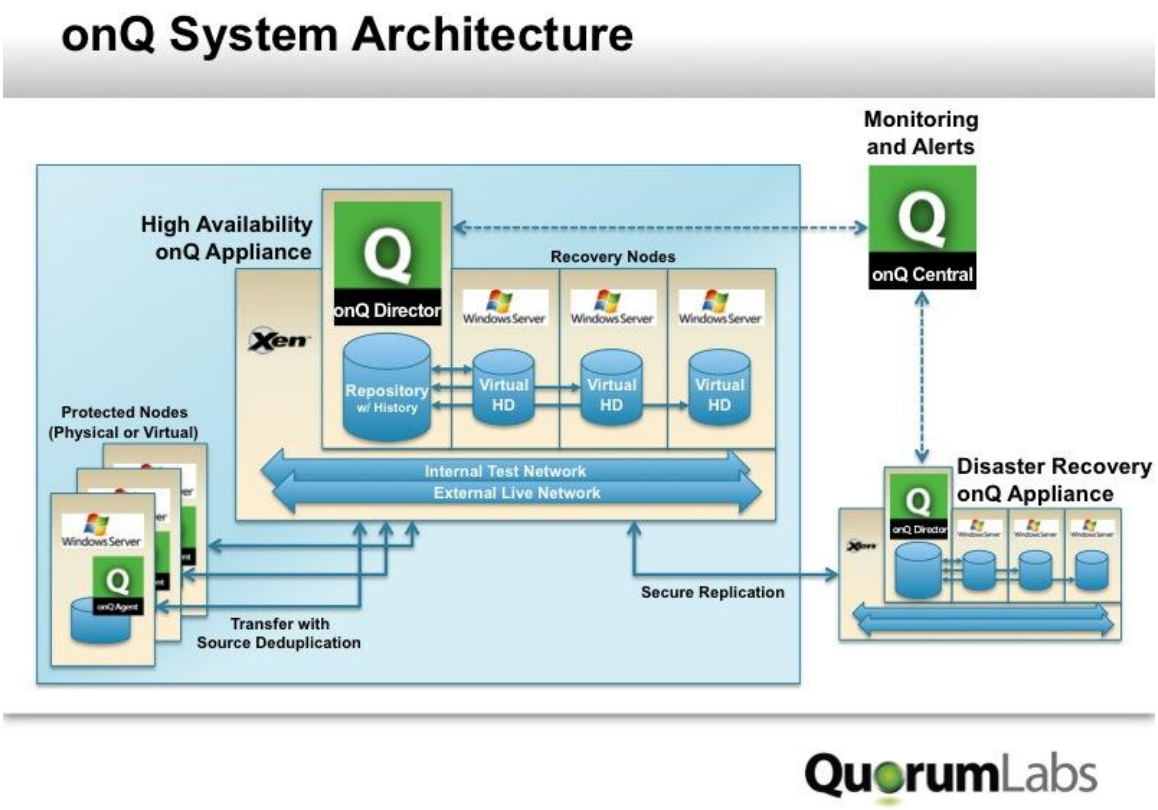
On top of this is that we are getting less tolerant for longer recovery times when outages occur. And while many businesses have service level agreements with their backup providers, they are usually unrealistic given the pace of the technologies used in the recovery process. Even a few hours disruption can cripple many businesses, even those that aren't usually thought of as online-only operations.

What if I told you that there is a better way to orchestrate your backups and recovery process that wasn't a hassle, didn't cost as much as a duplicate DR site, and could be accomplished with relatively unskilled staff that could bring your dead servers back online in a matter of minutes? That is what Quorum' onQ Recovery appliances attempt to do. Now downtime can be a thing of the past.

How onQ works

onQ actually has four components: the central monitoring console software that runs on an actual 'high availability 'appliance that acts as a repository for all the server images. The typical solution is sold in pairs and the second 'disaster recovery' appliance is located at a remote location. The two automatically synchronize their files so that once a server is protected on one; its information is transferred to the other.

The third piece is the individual agents that are installed on each physical and/or virtual Windows server. At present, only Windows 2003-2008 servers, both 32-bit and 64-bit, are covered. Finally, there is onQ Central, which will monitor your daily recovery tests, as well as report on any hardware failures. Here is a diagram showing you the various pieces:



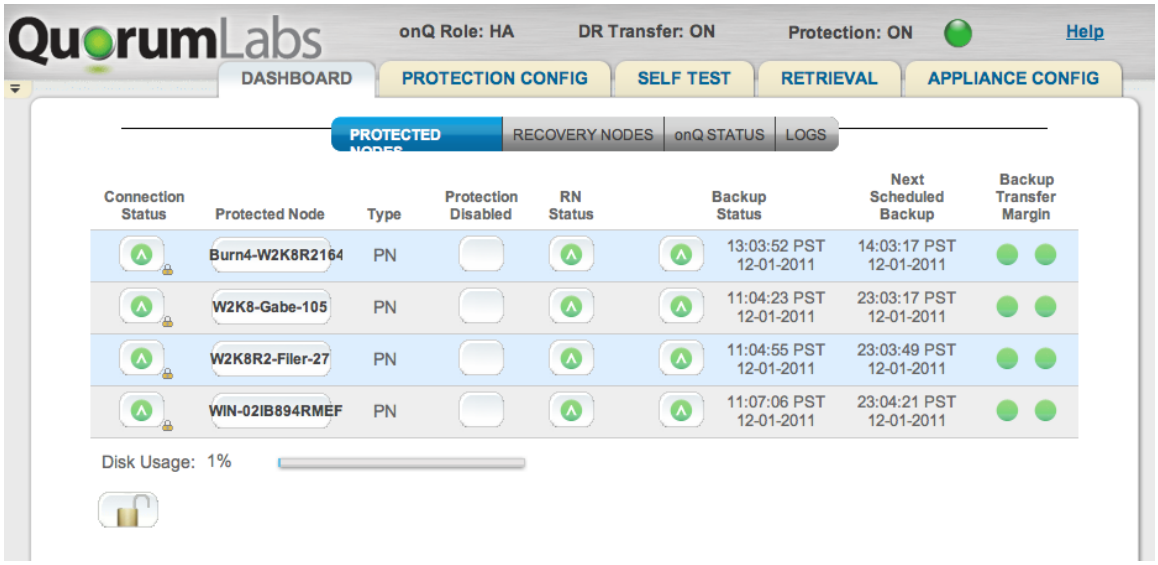
What is happening is that the onQ appliance is making physical to virtual copies of each protected server. Even if the servers are running as virtual machines (VMs) already, it still makes its own virtual copy on the onQ appliance. This makes them readily available to be run in case of an emergency, since VMs can be started quickly and without the need for matching up the original server hardware.

All of the console operations are accessible from an ordinary Web browser, so there is no software to install once you place the agents on each protected server. The central console dashboard has several options to keep track of your protection features all easily available with mouse clicks. Here you can see at a glance all of your servers that are under its protection, and how often you are backing up your data collection.

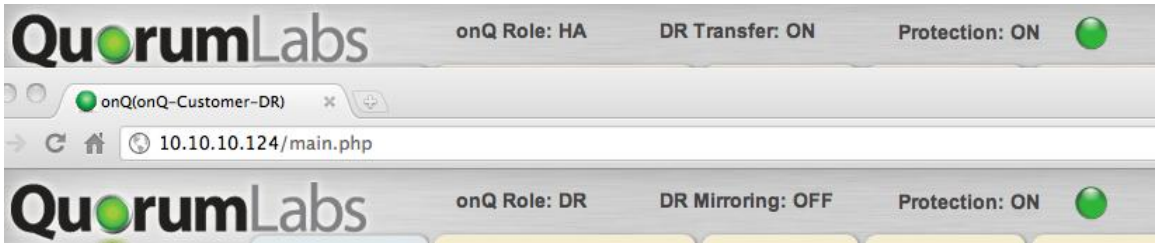
Configure Protected Nodes

Hostname	Backup Interval	Backup Retention Time	Initial Backup Time	Auto RN Creation	RN CPUs	RN MEM	RN Disks
Burn4-W2K8R2164	1 hr	40 days	ASAP	✓	1	1GB	C: 27GB
W2K8-Gabe-105	12 hr	40 days	ASAP	✓	4	6GB	C: 39GB, D: 2GB
W2K8R2-Filer-27	12 hr	40 days	ASAP	✓	1	2GB	C: 22GB
WIN-02IB894RMEF	12 hr	40 days	ASAP	✓	1	4GB	C: 39GB

You can start and stop protecting particular servers, and you can easily see if the recovery time window that you anticipate will be possible given the amount of data that you need to restore and your network bandwidth, as you can see in the screen below (the double green dots at the end of each line indicate that the window is adequate):



You can see that the dashboard for the offsite DR appliance has mostly the same set of controls, with the difference being the labels for the indicator lights across the top.

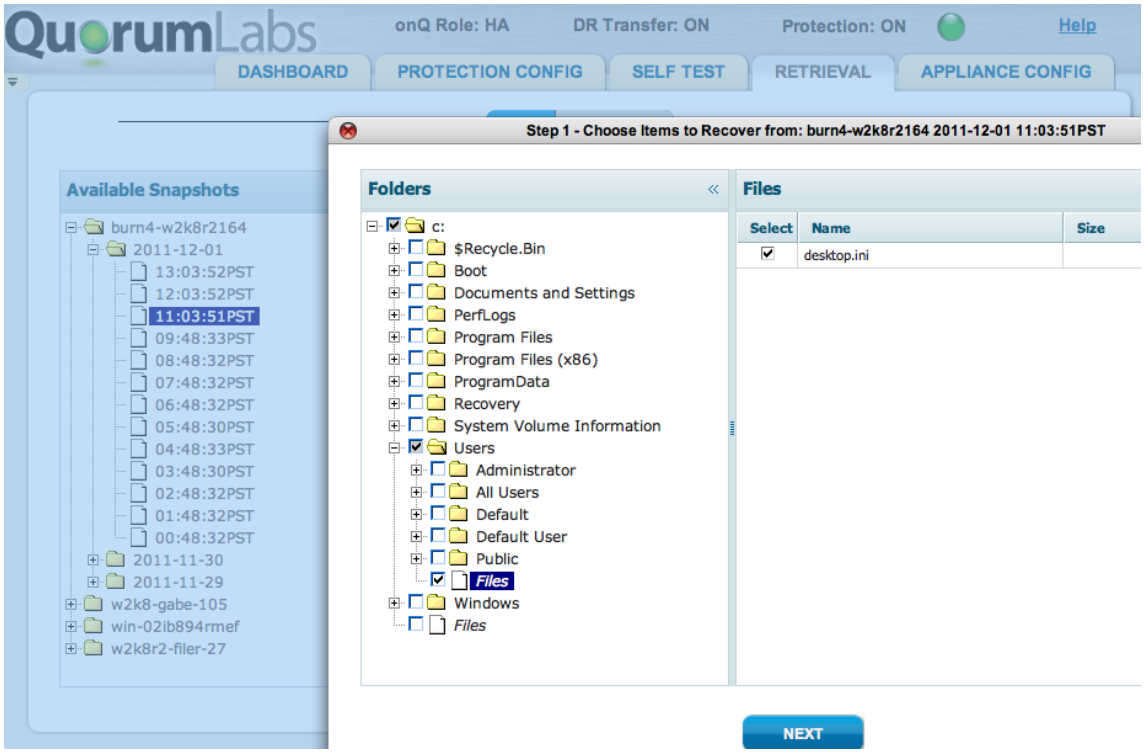


To bring a downed server back onto our production network is just a matter of a few mouse clicks. There is quite literally nothing for you to do, as it's brought back online. How is this possible?

onQ uses virtualization technology to make virtual machine copies of all of your Windows server collection – both existing physical servers as well as those VMs that you are running. Once the server is protected by onQ, in case of accident or disaster, you can recover either a single file or the entire image and bring it up on your production network within a few minutes to replace a failed server. First, it can be **brought up on a special test network** that can't be seen by any ordinary user, other than the onQ administrator. This is useful if you want to quickly try out a new patch or an upgrade to your application without messing with your existing production network. You can take this a step further, and recreate your entire production domain as part of this special test network inside the onQ appliance.

Second, onQ **automatically tests each protected image daily** (or on a schedule you specify) to ensure that it can boot and operate correctly. It does this without any intervention on your part, and in the background. If something fails, you will get notified via an email message and this gives you time to fix the problem before an actual disaster strikes.

Finally, you can **restore individual files or folders**, just like you could with a traditional backup solution. You can navigate down a file/folder tree view as most of the current products have, select a particular file from an available snapshot, and restore it back to the protected server in a matter of seconds.



Alternative recovery approaches

Of course, onQ isn't the only way you can do disaster recovery. Let's briefly touch on the various alternatives that are available.

First is the traditional backup software approach, which uses products that have been available for decades. These are great tools for making cheap copies of your data, and have stood the test of time. They can deduplicate files, make copies of open databases, and even handle VMs intelligently, too. But what they aren't good at is being able to restore an entire downed server without first finding matching hardware and getting the bare-bones OS set up to receive the backup file set. This could take days or weeks in some situations. There is also no easy way to test the backup integrity other than going through a laborious restoration process, which could also take days too. Pulling together the various duplicate hardware, restoring its OS, and then finding the right backup aren't easy, especially when this all has to be done under the shadow of debugging why the server crashed in the first place and fixing it as quickly as possible!

A second approach is to use one of the various cloud-based backup services. These are very easy to use for making backups of single machines, but they have their issues too when it comes time to do restorations because of bandwidth limitations. They also can provide a false sense of security and take days if not weeks to complete.

At the other end of the scale is **a duplicate datacenter**. This is tremendously expensive, not just for the replicated hardware but the various specialized tools that are needed to keep servers in lock step between the sites. Plus, when a server goes down in the main site, you still have some work to repoint domains or redo IP addresses to ensure that the DR site can step in and assume the production role.

Finally, there are **various virtualization solutions** that can do some of the pieces of what onQ is doing. But it is far from a simple process. You have to build a storage network, have servers that have enough power and memory to support multiple VMs, install a replication solution to populate your DR site, migrate your physical servers to the corresponding VMs, and monitor everything to ensure that you can bring up the DR site live when disaster strikes.

For example, VMware certainly has a collection of tools that can convert physical to virtual machines and orchestrate these VM to step in for downed servers. They have published a 200+ page paper that describes this process here: *http://www.vmware.com/files/pdf/practical_guide_bcdr_vmb.pdf*

The only trouble is this is a very unworkable solution for the vast majority of businesses that don't have the deep technical skills or don't want to spend hours assembling the series of seven different tools and hundreds of lines of scripts in this

document. Wouldn't it be easier to just click on an icon and let onQ do the rest? Not to mention all the licensing fees to acquire all the assorted tools, too.

Summary

Quorum' onQ is the first one-click site-based recovery solution that focuses on the recovery process, not just making backups. It can restore an entire data center's collection of Windows servers, both physical and virtual, in a matter of minutes. And like the traditional backup software products, it incorporates deduplication and sophisticated archiving to save on storage space. If your computers can't be offline, take a closer look at what they offer.

For more information

You can try out onQ for yourself in a virtual lab that Quorum has set up. Here is a descriptive video explaining the process:
http://www.youtube.com/watch?v=qJng5FRzM24

You can also register for various webinars and trial software on their website, *http://Quorumlabs.com*

Author Bio:

David Strom is the business channels editor of ReadWriteWeb.com, a leading Web technology news and analysis blog for IT workers. He has had a long career in IT publishing, as the founding editor-in-chief of *Network Computing* magazine, the author of two computing books, and a contributor to the New York *Times* and dozens of other Web and print publications.