Quorum

The Case Study

> “I’ve done a lot of BDR before coming to Quorum and the simplification of steps with onQ is very attractive. Something that used to take hours with other solutions is now done with a click of a button.”

Practicing What We Preach: Lessons Learned from a Quorum Outage

It’s said that plumbers have the worst pipes and the cobbler’s kids have no shoes. Organizations fail to practice what they preach, in other words, usually because they’re so busy solving other teams’ problems. But is that ever true for IT? Yes, as Ed Keller, Quorum cloud architect, learned during a Quorum outage.

Responsible for designing and maintaining Quorum’s cloud environment, Keller also oversees the network and all internal IT. Like any team, Quorum protects its resources with a backup and disaster recovery solution—which is our own onQ solution.

Here’s a backstage secret you probably already know: IT companies often merge their own solutions with others when it comes to their internal needs. But when Keller came on board, he refused to consider another vendor. “I’ve done a lot of BDR before coming to Quorum and the simplification of steps with onQ is very attractive. Something that used to take hours with other solutions is now done with a click of a button.”

At the time of the outage, onQ was protecting all business-critical resources. Those resources were used by Quorum employees and they consisted of file shares, web servers, FTP and other systems.

As BDR experts, the team considered their assets well protected—but the outage illuminated the flaws of their strategy.

Weekend Education

“The outage happened on a Saturday evening. Our CTO contacted me on Skype asking if there was a problem with email,” Keller recalled. “There was and it wasn’t just the email server—it was five servers, including our virtual Exchange server, all running on a VMware host.”

Because it was a weekend, there wasn’t quite as much impact as there would be during the work week. So while Keller knew he had the onQ recovery node as a fallback, he decided to minimize data loss by trying to repair and bring the Exchange server up in its current state. That was the idea, anyway.

“It was just a driver bug. I repaired the corruption to the Exchange database but once we got the hardware performing correctly, there were other knock-on effects.” After laboring over his original plan, he decided his most valid option was to boot up the onQ recovery node. "Everything just worked on the first try. At that point, I realized I could have saved two days of work by going to the recovery node first instead of trying to breathe life into the crashed system for such a long time."

Lessons Learned

The outage helped Keller and the Quorum team become aware of a few areas on their BDR strategy that could use improvement. For example, the team got a more accurate idea of how often they should be snapshotting their servers. At the time of the outage, they were snapping the Exchange server every twelve hours. This translated into an issue during the outage. The last successful backup occurred around 6 p.m. Friday evening; the next backup began at 6 a.m. Saturday morning but wasn't able to finish. The server stopped responding entirely at 9 a.m. Keller attempted to retrieve those 15 hours of email until Sunday evening before giving up and resorting to the recovery node.

"The other servers impacted weren't terribly important—our FTP server, our backend VMware management server, one of our four domain controllers and an up-down monitoring server in partial production. So they were fine on a 12-hour snapshot schedule; Exchange was the one bleeding transactions. Having gone through this, I would recommend 4-6 snapshots a day or even hourly for critical resources if you have the storage. Then you're only losing an hour's worth of email."

While Keller realized later he should have turned the recovery node on sooner, he believes snapshot frequency is ultimately a judgement call. "It comes down to circumstances," he said. "How much data are you ok losing? That decides the backup frequency."

While the Exchange recovery node booted up on the first try, Keller experienced a few backup failures for the other servers. "It had to do with drive space—the drives were too tight so we expanded them," he said. "And once I got the backups running, I found out one wasn't sending us alerts, so I corrected that."

He realized he had also failed to take the company's advice given to customers. "We tell customers to check spinup reports every day—but ours go to a folder I don't check," he admitted. "In other words, we're no different from a lot of companies."

The outage also reminded the team they had forgotten to upgrade their internal onQ appliance, as they were still running on the 3

> "Everything just worked on the first try. At that point, I realized I could have saved two days of work by going to the recovery node first instead of trying to breathe life into the crashed system for such a long time."

ED KELLER
Cloud Architect

Quorum®
1-Click Instant Recovery

series appliance. “onQ is very “set it and forget it”, which means we had it running for four years. It kept working smoothly, which is great—but we realized that we needed to upgrade to use the bells and whistles on new versions.”

From Outage to Insight

The experience confirmed some positive findings as well. The onQ appliance is renowned for its simplicity and ease of use, something Keller found to be true. Without any training or experience, he was able to handle failing over on his own. “This was the first time I used internal onQ. I didn’t do the deployment, installation or configuration—but as soon as I got the call, I was able to log in, spin it up and get it recovered.”

“This was the first time I used internal onQ. I didn’t do the deployment, installation or configuration—but as soon as I got the call, I was able to log in, spin it up and get it recovered.”

He was also surprised the recovery nodes spun right up and worked perfectly. “We deal with customer support issues every day so we expect failures. It’s what we’re used to,” Keller said. “But the node actually spun up right away and worked on the first try—and that’s what it does for most customers.”

Performance was another positive surprise. The Exchange server ran on the onQ server for more than a month. Not only was there zero performance degradation—users reported that the recovery node was faster!

The experience ultimately shaped the Quorum team’s backup and disaster recovery strategy. At the time of the outage, they followed best practices by having a local hardware appliance and offsite hardware appliance, with onQ appliances for the Exchange server at the datacenter and the DR server in their rack at the office. However, the outage propelled them to rethink that configuration and expand to cloud.

“This was an opportunity for us to revisit our internal infrastructure,” said Keller. “Our product systems live in the colocation but we remotely access them through the VPN tunnel. Now we want to bring some systems back into the office to improve speed and reduce latency by replicating our DR back to the cloud. That’s one of the plans for our refresh.”

It’s not always easy to admit your own mistakes. But the Exchange outage ultimately taught the Quorum team valuable lessons about strengthening our own backup and disaster recovery. By discovering the weaknesses in our BDR configuration and recovery strategy, we were able to design a faster and more efficient system—and share that knowledge to protect our customers.