CASE STUDY

NCTH - National Corporation of Tourism & Hotels

Discovering the Potential of Advanced BDR

The backup and disaster recovery tools of today have come a long way from yesterday’s solutions— but many organizations are still limited by yesterday’s tools. As their needs grow, many teams find themselves trying to protect and recover critical data with solutions that are too primitive to deliver the speed and efficiency they need.

The National Corporation for Tourism Hotels (NCTH) is poised to contribute to the promotion of Abu Dhabi as a tourist and international destination. And the four directions it has followed are: hotels, catering services, transport and retail. Each division is manned by an experienced management team and provides its customers with a variety of superior services, this hotel cannot afford to have single downtime that will affect the entire business operations.

Yet as with many organizations, NCTH data needs outpaced its BDR technology. “Since we started using it a few years ago, Quorum has consistently committed as promised with no problems. With Linux OS and a hyper-converged environment, the hardware is reliable and becomes even more so. We have received good post-sale technical help from individuals who are well-versed in HA and DR principles.”

Saleh Al Habshi - IT Manager

Pressure and Anxiety

33rd St, Zayed Sports City - Abu Dhabi

Infrastructure: 9 Servers including physical and Virtual. Their Virtualization is on VMware. All servers are running on windows server OS.

Data Size: 15 TB

Disaster Impact: 100%

It was a dreadful night of 13th Oct 2022. NCTH was attacked by ransomware, Then They started connecting all 9 servers one by one and found that ransomware attack had spread to this datacenter as well encrypting all files and data in NCTH. They contact **Quorum** team UAE . UAE team has Taken the remote session to check the status of the snapshots, got to know the onQ web console is not accessible, and immediately went to the customer site. Done the complete analysis of HA & DR appliance. After Analyzing both the appliance got to know that onQ's Meta Data has been deleted by the Hacker with the root password of onQ's which was saved in the customer browser cache.

The group company were attacked by ransomware striking the fear in everyone. The IT team's entire future depended on **Quorum** because it was their only line of defense against such attacks. In these circumstances, **Quorum** proved to be the finest in its class.

The **Quorum** appliance powered on all recovery servers, and production was up and running in a short period of time. By altering the credentials, etc., all required procedures were done to ensure that the network was once again secured. Due to recovery servers operating in **Quorum**, all reservations, check-ins, and checkouts were completed as usual. After cleaning the network and formatting the production servers, we began the BMR procedure to restore the beneficial data and apps to the production servers.

On the one hand, **Quorum's** production was operating smoothly, while on the other, the BMR was taking place in the background to guarantee minimal downtime and ongoing output. All of the production servers were back online and operating normally after **Quorum** had finished the restore with incremental failback.

Quorum has grown to be a crucial component of the datacenter, serving as a lifeline for NCTH. After this disaster, they would never consider operating a data center without Quorum.

Quorum One Click Instant Recovery