VIRTUAL MACHINE HIGH AVAILABILITY FOR VIDEO SURVEILLANCE AND IoT APPLICATIONS

INTRODUCTION

Video surveillance, building automation, and IoT sensor data processing are critical functions. Gaps in monitoring, control, and data collection can represent security and liability risks, as well as lost opportunity. To minimize downtime, applications and data storage systems in these environments must be resilient in the face of typical hardware and software failures.

At the heart of Quantum's VS-Series appliances is the Quantum Cloud Storage Platform (QCSP), a software-defined storage and compute platform. QCSP's embedded clustering, monitoring, and virtualization enable VS-Series appliances to provide high availability (HA) for critical applications, maximizing uptime.
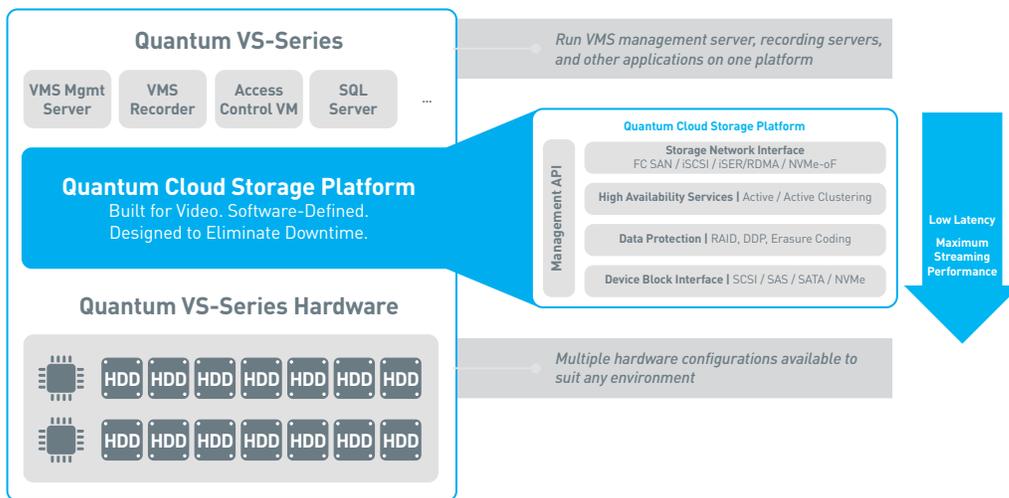

Figure 1. QCSP and VS-Series Architecture

QCSP provides HA for hosted VMs using a cluster of VS-Series nodes. Multiple layers of protection are provided against both hardware and software failures, as summarized in Figure 2 below and Table 1 on next page.
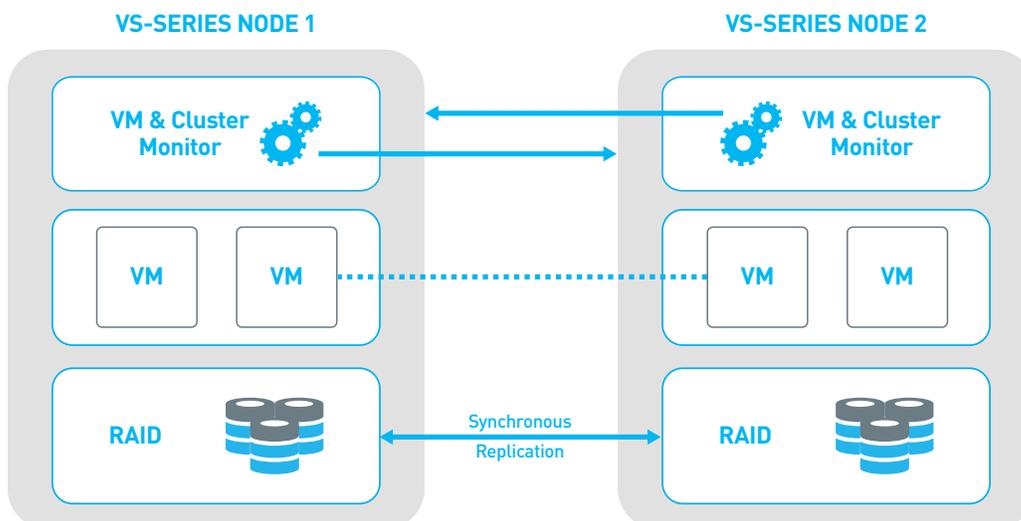

Figure 2. VS-Series Cluster Architecture

Peril Protected Against	Protection Mechanism
Drive Failure	RAID
Node Failure	Synchronous Replication, Node Monitoring
Data Loss	RAID, Synchronous Replication
VM Failure	VM Process Monitoring

Table 1.

DRIVE FAILURE PROTECTION

To provide high availability for a hosted VM running a critical application, the underlying storage must be redundant. To protect against drive failure and the associated data loss, each drive on every VS-Series node is protected with RAID. If a drive fails or loses connectivity, all hosted VMs continue to run uninterrupted, all data remains safe, and both the system administrator and Quantum are notified of the failure. Various RAID levels are used depending on the VS-Series appliance model.

NODE FAILURE AND RECOVERY

To protect against more serious component failures or the failure of an entire VS-Series node, replication is employed. The storage for HA VMs is synchronously replicated from the primary VS-Series node to a secondary node over dedicated high-speed links. With synchronous replication, writes must be successfully committed to storage both on the primary node and the secondary node before being acknowledged to the application. This ensures that no data is lost in transit during a failure, and the secondary copy is always completely up to date. To maximize efficiency and performance, only changed blocks are replicated.

QCSP monitors the nodes in the cluster. If the primary node becomes unresponsive for any reason (power loss, OS hang/crash, system shutdown, etc.) the secondary node responds by starting any HA VMs that were running on the failed primary node. Because the storage is synchronously replicated, the VM sees the failover as a crash followed by a restart, and the data is crash consistent.

When a failed node is restarted, it will communicate with the other running node and rejoin the cluster. Synchronous replication will sync any blocks that changed while the node was down. The HA VMs will not automatically fail back to the restarted node, as this would cause an interruption in service. If a VM fails from Node 1 to Node 2, Node 1 is repaired, and Node 2 later experiences a problem, the VM will fail over to Node 1. There is no requirement or advantage to move VMs back to their original primary node, but if this is desired a "VM Move" operation may be initiated from the UI.

VM FAILURE AND RECOVERY

Deploying redundant hardware is necessary, but it is not enough. Operating systems and applications are complex and can also fail. Therefore, QCSP also monitors the running state of hosted VMs. If an HA VM fails (due to a crash, shutdown, or other reason), QCSP will detect the failure and automatically restart the VM. If the restart fails, or the VM fails too many times, the VM is started on the other node.

Future software releases will include options for more granular service monitoring and recovery.

Visit www.quantum.com/vs-series for more information about Quantum VS-Series appliances.