Ensuring Continuous Availability for Electronic Health and Medical Records

Noel Moss, Senior Professional Services Consultant, Stratus Technologies

Electronic Health Records (EHRs) and Electronic Medical Records (EMRs) are rapidly becoming common-place in the healthcare industry. Organizations such as the Certification Commission for Healthcare Information Technology (CCHIT) and regulations such as the Healthcare Insurance Portability and Accountability Act (HIPAA) mandate robust, interoperable healthcare information systems. As EHRs and EMRs are widely adopted, the need for robust platforms that ensure continuous availability and data integrity becomes paramount.

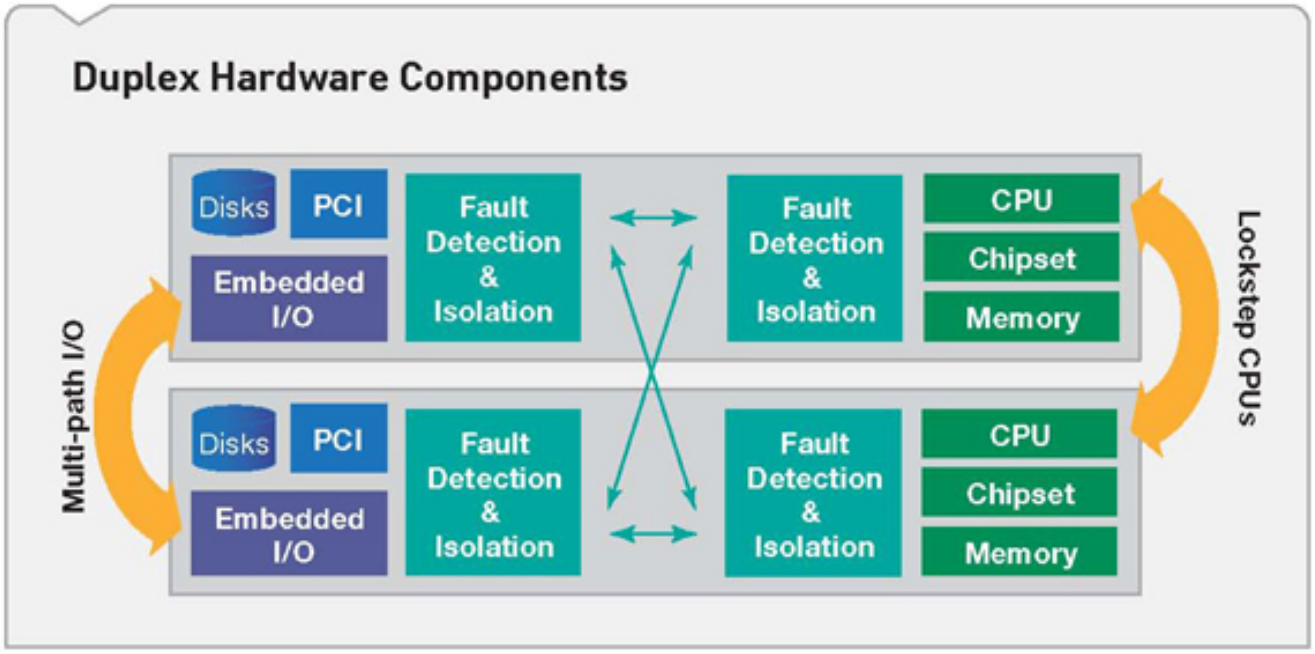
EHR and EMR systems constitute a major financial investment for health care providers and therefore these applications tend to have a long lifecycle. Indeed, some have evolved from legacy application environments. Given the relatively short lifecycle of computer hardware, virtualization offers a viable and attractive solution that preserves providers' investments in EHR and EMR software. Virtualization facilitates the extension of EHR and EMR application lifecycles by providing an operating environment which is independent of the underlying hardware platform. This hardware independent characteristic allows for simple hardware and capacity upgrades.

Hardware independence, however, does not diminish the importance of the platform itself. To the contrary, virtualization by its nature increases the importance of server availability, reliability and performance, an aspect frequently overlooked in the rush to implement EMR software. Virtualization itself does provide a level of improved availability, which comes at a cost in terms of dollars, complexity and professional skill sets. Alone, virtualization software cannot be relied on for uptime assurance that EMR software commands.

High availability clusters provide improved availability. Like virtualization HA, clustering adds cost, complexity, and management load. More important, clustering is failure recovery technology. It assumes downtime and is designed to recover as quickly as possible. During server failover and failback, EMR will be down. VMs

cannot be migrated off a dead server. Data not committed to memory, i.e. in-flight data, will be lost. Finding issue root cause is difficult and generally not done.

Coupling virtualization with the uptime assurance of fault tolerant server platforms such as ftServer systems from Stratus Technologies (www.stratus.com [1]), results in mission-critical application support designed to prevent downtime and data loss. A fault-tolerant system architecture utilizes duplicate components running in lockstep, multipath I/O and sophisticated monitoring tools which eliminate system interruptions in the event of hardware failure. There is no failover; the faulty components are automatically isolated in real-time and their redundant partners continue operating with no interruption, thus preserving business continuity. These are significant technological and operational differences from the failover and recovery, along with associated application downtime, which is characteristic of clusters.



When integrated into a well-designed HIPAA Security Rule and ePHI compliant network environment with redundant paths, industry-standard fault tolerant systems with VMware, Hyper-V or RedHat Enterprise Linux provide continuous 24/7 access to EHRs and EMRs while protecting against loss and/or corruption of health data due to hardware or software failure. This approach offers the simplicity and reliability to implement a private cloud which ensures maximum uptime, maximum data integrity and maximum data protection for EHRs and EMRs.

Links:

[1] http://www.stratus.com