

## Fault Tolerance in a Virtual World

*How common use cases raise  
your Criticality Quotient*

## Abstract

As server virtualization goes mainstream, the workloads of virtual machines are taking on mission-critical proportions. Uses range from application-dense server consolidation, to failover and disaster recovery, to managing the virtualized infrastructure. Downtime and data loss pose harsh consequences in scenarios like these. This paper looks at five use cases to show why, where and how your business can reduce risk in your virtualization initiative by hardening your IT environment with physical servers that ensure reliability and availability.

## Virtualization in the Mainstream

Virtualization of x86 servers has already made its mark on IT, and the surge shows no indications of stopping. For example, a 2007 article in *Network World* reported that Forrester Research found use of server virtualization growing from 29% in 2005 to 40% in 2006 among North American companies that were surveyed. The percentage of companies piloting virtualization remained level at 11%.<sup>1</sup> An article in *IT Week* reported that IDC forecasts customer revenue from virtualized server sales in Western Europe will grow from \$948 million in 2006 to \$5.5 billion in 2011.<sup>2</sup>

When most virtualization initiatives were still at an early stage, the typical application involved didn't by itself consume a lot of system resources, was forgiving of slow response time and did not necessarily represent a high priority to the business. That's changing as virtualization is more widely deployed. IT managers are starting to look beyond their initial goal of hardware consolidation, and the resulting benefits of improved server utilization and better return on investment. They also want to use virtualization to achieve other goals, including higher availability and disaster recovery.

Yet putting your "eggs in one basket" should be done judiciously, even when virtualization lends resilience and flexibility to that basket. For starters, virtual machines run on physical servers, whether they are conventional servers or availability-promoting designs. And *when the hardware fails or a transient error occurs, all the virtual machines on a server may stop and must be restarted* unless you use a fault-tolerant server technology that offers the necessary protection.

Also keep in mind that the virtualization layer has the potential to be a single point of failure for all of the virtual machines it supports. The exposure rises as you run more virtual machines on a single server.

## Use Cases Raise Criticality Quotient

The next section of this paper examines five use cases where virtual machines and infrastructure assume mission-critical stature under the right conditions — even when the uses don't fit pre-virtualization notions of what is essential to the business.

What we will describe as the Criticality Quotient, or CQ, of these use cases is often relatively low when an organization first implements virtualization. The CQ rises as more of your business processes, more users and more applications depend upon virtual machines and infrastructure.

---

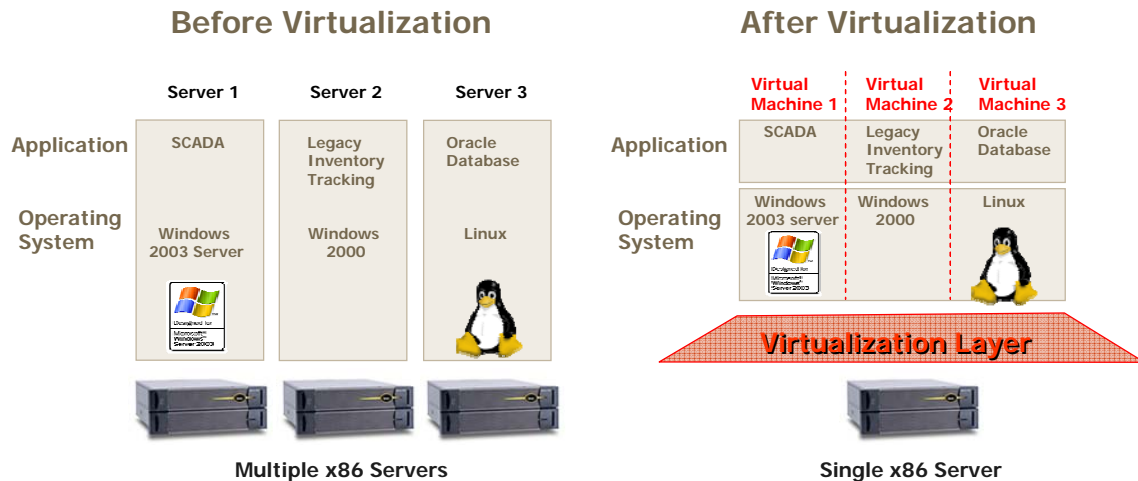
<sup>1</sup> *Network World, Server virtualization goes mainstream*, February 12, 2007

<sup>2</sup> *IT Week, European enterprises embrace server virtualisation*, May 9, 2007

## Server Consolidation

According to a 2007 report by Yankee Group, 85% of virtualization software acquired by enterprises goes to server hardware consolidation projects.<sup>3</sup> The report also states that businesses have been able to better their hardware utilization from 10% to 80% in certain instances. The resulting savings are not limited to hardware-related costs, but also extend to management costs and environmental expenses such as space, power and cooling.

**Figure 1: Server Hardware Consolidation**



At a manufacturing plant (example above) without a dedicated computer room, IT systems compete with other equipment for square footage. The savings on space, power and cooling alone can be valuable.

What's more, we have observed some companies opting to standardize on virtualization for new deployments of x86 servers. These adopters want their applications to run on a shared virtual pool of server processing and storage that can be rapidly reallocated to provide capacity while avoiding underutilization.

Virtualization leader VMware cites that 10-15 production systems may be consolidated onto one server. Even an outage of non-mission critical applications has a mission-critical impact when a large number of users are affected.

## Live Migration

Live migration allows virtual machines to be moved (in cases where the operating system is not visible to the application) with virtually no interruption to the application and little perceived impact by users. This provides the flexibility to handle peak processing loads and to shift applications for maintenance. Hardware and operating system upgrades can be accomplished without planned downtime, for example.

Live migration works by copying the system state iteratively while the application continues to run. Shortly before a final copy of the virtual machine is ready for migration, only a brief application blackout — perhaps milliseconds — is necessary to synchronize the second virtual

<sup>3</sup> Yankee Group, *Server Consolidation Creates New Opportunities for Fault-Tolerant Servers*, January 22, 2007

machine with the original. (Note that the operating system that can be upgraded is at the host OS/hypervisor layer; guest operating systems cannot be upgraded online.)

Disk storage is, of course, virtualized as well using NAS (network attached storage) or a Fibre Channel or iSCSI SAN (storage area network) to support data integrity.

But if the underlying physical server hardware, operating system or device drivers cause a conventional server or high-availability cluster to crash at an inopportune moment, the availability of your virtual machines and your data integrity take a nosedive. In-flight data not yet written to disk may be lost.

For that reason, risk management calls for assessing the worst-case scenario when a fault can't be predicted and live migration is precluded. What happens when your physical and virtual servers have to be restarted? This same exposure exists for two more use cases that rely on live migration: failover/disaster recovery and load balancing.

### **Failover and Disaster Recovery**

A shared resource pool of physical servers and storage is the mechanism that virtualization uses to support failover and disaster recovery (DR).

The process works like this: When a physical server shuts down, virtualization software can automatically (if supported by the implementation) use the SAN to retrieve image(s) of the virtual machine(s) affected, including configuration state, disk state and so on. A restart of the applications is then initiated on other server(s).

When the virtual machine images are replicated and restarted in a protected location, these failover capabilities can be used to enable DR and business continuity (BC). Data can be similarly replicated to storage elsewhere on the network.

Some virtualization software also enables point-in-time rollbacks. Useful when data corruption has occurred, rollback lets an administrator revert the virtual machine to an earlier known good state.

### **Load Balancing**

Live migration is likewise instrumental for load balancing, in which the workloads of physical servers are adjusted to match the demands of the virtual machines they host. This keeps utilization efficient while providing capacity where needed.

Consider the example of an application that always requires 50% of a physical server's processing capacity to deliver performance needed to meet a service level agreement (SLA). Without load balancing, other virtual machines coexisting on that server may infringe on those CPU cycles.

Your virtualization software may allow resources to be reallocated without action by a systems administrator, based on predefined rules. But doling out resources to virtual servers is error-prone because those rules must be based on correct assumptions.

Arriving at the right assumptions still requires technical expertise. While allocating disk and memory among virtual machines is rather straightforward and fine-grained, CPU and network resources are another matter. Assume incorrectly, and you will drag down a CPU- or network-intensive environment.

## Management and Provisioning

Savvy IT pros recommend against virtualizing the management software that orchestrates everything in the virtual pool of applications, processors and storage. You don't want a problem at the host or virtual machine level to interfere with access to management capabilities. In fact, a separate, non-virtualized management console is required for some implementations of virtualization.

For VMware, the management software is VMware VirtualCenter; for Microsoft, it is Microsoft System Center Virtual Machine Manager (SCVMM).

Centralized management and provisioning represents a single point of failure unless you mitigate the exposure with an availability-boosting server.

When you use a golden image of a virtual machine to provision an essential application, safeguarding the availability and integrity of that image does not just save time; it reduces risk and may alleviate the need for labor-intensive revalidation. The virtual machine can be qualified and tested to ensure it will execute as expected upon deployment. In regulated industries such as life sciences, pre-validation of the platform may be required prior to production use.

## How to Harden Where Essential

As the previous use cases show, the Criticality Quotient of common virtualization scenarios may be higher than it appears. In addition to gauging your "CQ," a risk assessment should identify new points of vulnerability introduced when your business starts relying on virtual machines and infrastructure on a significant scale. Hardening against those exposures offers assurance in situations where downtime and data loss are expensive and unacceptable.

High-availability server clusters and fault-tolerant servers are two approaches that organizations evaluate when they seek to ensure uptime and data integrity for traditional mission-critical applications. The two are not equally good companions for virtualization, however.

### High-Availability Server Clusters

A high-availability cluster links two or more computer servers with software programs and physical connections so that when a failure occurs on one, its workload fails over to a server that is still operating.

Note that high-availability clusters are designed to *minimize unplanned downtime through quick recovery from failure*. They do not shield users and applications from noticing downtime or slower performance while a faulty server is offline. Predicted availability for a server cluster can be around 99.99% when supported by attentive configuration as well as ongoing administration and maintenance.

What's more, implementing virtualization on a high-availability cluster adds another layer of complexity on top of managing the cluster itself. Putting the cluster software and hardware together, testing them for proper failover and maintaining them must be handled by an experienced IT department or systems integrator. Software applications must also be made cluster-aware.

You should also expect performance overhead with a cluster, on top of any performance overhead that may accrue from virtualization alone.

This high-availability type of cluster differs from clustering done within the virtual environment at the guest operating system level. The second form, called virtual clustering, does not alleviate problems at the physical server level.

**Figure 2: High-Availability Clusters and Fault-tolerant Servers at a Glance**

High-Availability Cluster	Fault-Tolerant Server
99.99% uptime achieved only with meticulous setup, ongoing administration and maintenance 1+ hour unplanned downtime annually Failover delays (typically 30 seconds or more per event) Significant planned downtime required for software upgrades and periodic cluster testing	99.999% or better uptime achieved with no special effort 5¼ minutes or less unplanned downtime annually Non-stop processing during component failure, hardware replacement and OS hot fixes Planned downtime required for software upgrades is virtually eliminated with online upgrade technology
In-flight data lost on failure No guarantee of data integrity	In-flight data preserved at all times Data integrity guaranteed
Throughput may be affected during server outage	No performance degradation, even with component failure
Requires cluster system design, cluster-aware applications, failover script writing, careful implementation and extensive testing Versions for Windows® or Linux® operating systems	Out-of-the-box operation Runs standard Windows or Linux applications (no modifications needed)
Administration of multiple servers, ongoing testing to ensure proper operation, post-failure maintenance and re-testing of cluster software Changes require failover script update and testing	Operates as a single Windows or Linux system No special administration or operational support is required
All upgrades must be performed on multiple server systems Redundant nodes must be synchronized Scarce cluster expertise puts serviceability at risk	Self-diagnostics isolate fault to component level and automate problem reporting Hot-swappable hardware Enables remote problem investigation and resolution
Duplicate OS licenses, cluster design and implementation incur additional upfront costs Administration and ongoing change management incur recurring high-cost labor	Cost of continuous availability is built into one-time hardware cost — not recurring costs Total cost of ownership lower than alternatives, when cost of downtime and skilled personnel is included

### Fault-tolerant Servers

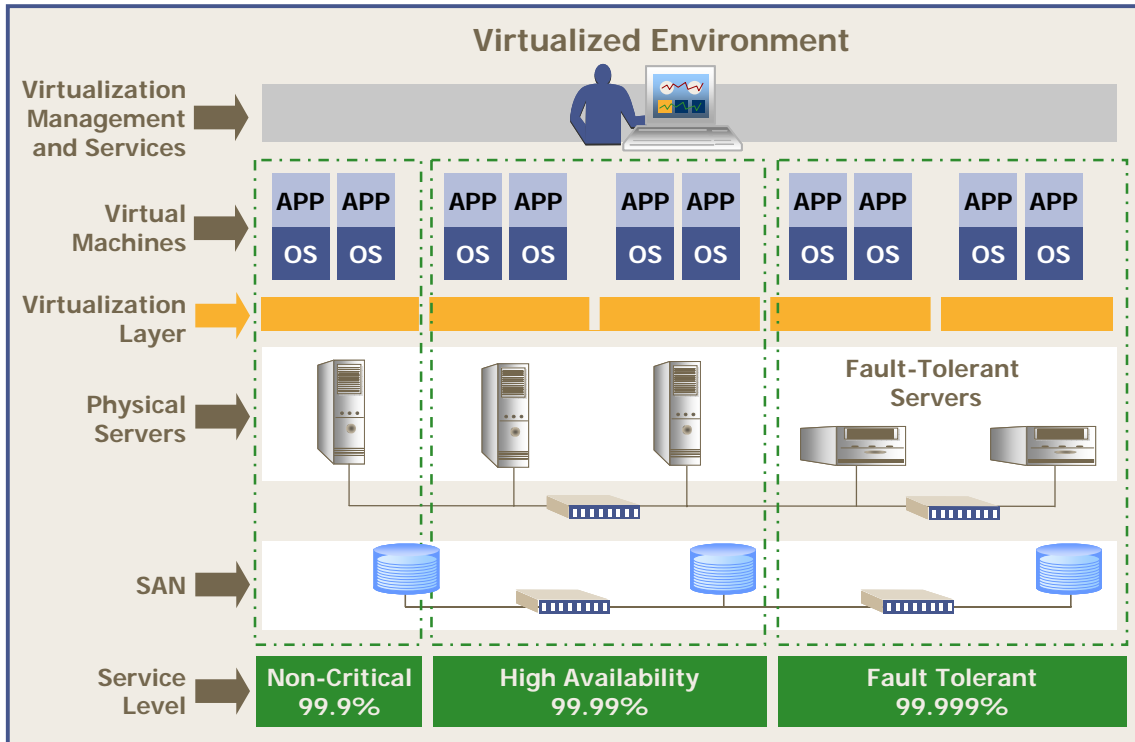
Fault-tolerant servers offer an effective means of hardening a virtualized environment without adding to the complexity inherent in implementing and maintaining high-availability clusters and without modifications to the applications.

Fault-tolerant systems are characterized by component and functional redundancy within the footprint of a single server. The operating system sees a “single-system image.” With an optimal fault-tolerant architecture, software applications do not need to be modified in any way to benefit from the server’s reliability and availability features.

If one of the server’s components fails, its duplicate *keeps the server processing without interruption or degradation in performance*. The 99.999% or better availability that certain fault-tolerant systems provide is described as continuous availability.

The internal redundancy of a fault-tolerant server architecture also maintains the integrity of committed (completed) transactions and preserves in-memory data not yet written to disk, despite a component failure or transient error such as a driver malfunction.

**Figure 3: Hardening a Virtual Environment with Fault-Tolerant Servers**



*Deploying fault-tolerant servers as part of a virtual resource pool hardens your environment at otherwise vulnerable points. You are also positioned to support tiered levels of service, with the agility to upgrade virtual machines to a higher level of availability when needed.*

**Be Prepared for Virtual Complexity**

Finally, remember that in the virtual world you trade physical complexity for complexity in a virtual dimension. Virtual machines have the means to proliferate fast, and maintaining a stable environment under the abstraction of server virtualization can be difficult. An IT staff may not have enough highly skilled professionals on board to do it all. A professional services provider with mission-critical expertise can be a welcome ally when virtualization raises the CQ of your environment.

**Conclusion**

Because virtualization changes how x86 servers and applications are deployed, previously non-mission-critical uses are taking on mission-critical characteristics. Organizations adopting server virtualization on a large scale should assess the Criticality Quotient of their usage in areas including server consolidation, live migration, failover and disaster recovery, load balancing and management and provisioning. Where the risks of downtime and data loss are unacceptable, choosing fault-tolerant server hardware hardens against new vulnerabilities and complements the resilience provided by virtualization.

## **About Stratus Technologies**

Stratus Technologies is a global solutions provider focused exclusively on helping its customers achieve and sustain the availability of information systems that support their critical business processes. Based upon its 25 years of expertise in server and services technology for continuous availability, Stratus is a trusted solutions provider to customers in manufacturing, life sciences, telecommunications, financial services, public safety, transportation & logistics and other industries.

For more information, visit [www.stratus.com](http://www.stratus.com).

Specifications and descriptions are summary in nature and subject to change without notice.

Stratus is a registered trademark, and Active Upgrade and the Stratus Technologies logo are trademarks, of Stratus Technologies Bermuda Ltd.

Microsoft, Windows and Windows Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. The registered trademark Linux is used pursuant to a sublicense from the Linux Mark Institute, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis. All other trademarks and registered trademarks are the property of their respective holders.

© 2007 Stratus Technologies Bermuda Ltd. All rights reserved.  
X942