IT Resiliency in a Complex World

Challenges and Solutions in the Virtual, Cloud and Mobile Era
Table of Contents

Introduction ............................................................................................................................................................................................... 3
System Continuity Risks of Virtualization .............................................................................................................................................. 3
Greater Impact with Cloud Computing .................................................................................................................................................. 4
Integrated System Continuity .................................................................................................................................................................. 5
Fast Local and Remote Recovery ........................................................................................................................................................... 6
Options for Data Mirroring ...................................................................................................................................................................... 6
Flexible Configurations ............................................................................................................................................................................ 6
Keeping Up with Mobility ......................................................................................................................................................................... 7
Conclusion ................................................................................................................................................................................................ 8
About NEC ExpressCluster Solution ...................................................................................................................................................... 9
Introduction

Dramatic changes in virtualization technologies, cloud computing and smart mobile devices and applications have created more value, as well as greater complexity for IT management. This new era of hardware consolidation and virtualization have improved overall system flexibility and resource utilization in data centers, and fortified the cloud computing revolution. In its purest form, cloud computing offers convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, software and services) that can be provisioned quickly and released with minimal effort. Cloud computing has in turn facilitated cost-effective access to mobile application services through smart mobile devices, which are propelling disruptive transformation across many industries.

The promise of massive cost savings and increased IT agility is attractive; however consolidating multiple virtual systems onto a single physical host server presents a significant continuity risk. In essence, a single point of failure is created that can result in a potentially disastrous result if that physical server fails. A single virtualization host server failure presents far-reaching damages that can bring down many critical applications, losing precious data at the same time.

This paper will outline the risks, considerations, and optimal approach to ensure IT resiliency and business continuity in a complex world.

System Continuity Risks of Virtualization

IT departments around the globe continue to struggle with system continuity issues in virtualized environments. While solutions on the market claim to solve the problem, in many cases operational complexity and the high cost of ownership are serious deterrents to adoption.

In order to realize the benefits of virtual system consolidation, while minimizing the risk of business disruption due to system failures, an integrated system continuity solution is required. Critical applications and data must be protected with system-wide disaster recovery (DR) with high availability (HA) in any non-trivial virtual system environment.

Virtual servers have several glaring vulnerabilities; the most significant is having a single point of failure. Experience has taught us to not put all of our eggs in one basket. Failure of a single virtual server running multiple virtual machines (VMs) can literally halt critical business operations in its tracks by losing data, damaging or freezing critical applications, and dropping communications and messages. Routine server maintenance caused a series of network switch failures that knocked four major cloud computing providers – BlueHost, HostGator, JustHost and HostMonster – offline for 8 hours.
Although the companies responded quickly, customers experienced significant business disruption and were concerned that multiple cloud computing providers were sharing critical network infrastructure.

In another example, a basic environmental error, accidentally triggering the server room’s fire extinguishing system, took France’s state financial system offline for four days, and damaged several major components of a storage bay holding critical data. Without the right DR system in place, it took days to restore the system.

Such disruptions quickly ripple through the entire organization causing lost business opportunities, less revenue generation activities, and damage to the company’s reputation. Outages cost money and stall growth. The world’s largest domain name provider, GoDaddy, made reparations to its customer by giving a 30 percent across-the-board discount as an apology for an outage that knocked out the company’s services for several hours.

Increasing the management workload is another likely problem with some virtual systems. IT teams are already stretched, and likely do not have the bandwidth to nurture customized virtual systems. Further, virtual servers can experience performance bottlenecks from limitations of physical server resources, such as memory and CPU performance. However, these issues pale in comparison to the potentially devastating effects of system level service outages. Among the major types of failure that could cause system level service outages are:

- **Physical host machine failure** – Whole machine failure such as an unexpected system shutdown due to a power supply failure.
- **Physical host machine component failure** – Individual component failures, such as disk I/O and media failure, memory errors, network I/O failure or fan failure, that cause degraded system performance or partial machine failure. Typically, component failures are warning signs for impending machine failure.
- **Network failure** – Network equipment failures and connectivity disruption, such as accidental cable cuts, can make some application systems or entire sites unavailable to client systems and users.
- **Virtual server failure** – Virtual server software itself could fail due to causes including design or implementation defects, resource (e.g., memory, disk) exhaustion, and malicious attacks (e.g., virus).
- **Virtual machine failure** – Each virtual server will typically run multiple VMs, and each VM can crash and fail just like physical machines.
- **Virtual machine component failure** – Each VM contains various virtual components, such as virtual disks and virtual network interfaces, which can fail causing system level service outages.
- **Application failure** – Applications running in a VM can fail and cause system level service outages.

In general, virtual systems are already fairly complex to implement and maintain properly due to resource sharing and related interactions, even without system continuity concerns. In the end, selecting a comprehensive system continuity solution that is able to quickly detect and automatically recover from all major types of failure is necessary to effectively mitigate the system continuity risks of virtualization.

### Greater Impact with Cloud Computing

More enterprises are relying on availability and performance for competitive advantage. Cloud computing is an option to quickly scale and achieve higher performance with significantly lower capital expense than traditional internal data centers. According to a study conducted by Neovis, research found that 54% of organizations are already using public or private clouds.

To gain a clear understanding of cloud computing environments, there are four cloud computing models defined by the National Institute of Standards and Technology (NIST):
• **Public Cloud** – Open use for the general public and easy to use, this virtualized environment might be owned, managed and operated by a business, academic or government organization or some combination, but it exists on the premises of the cloud provider. Amazon Elastic Compute Cloud (EC2), which offers resizable computing capacity via the Web, is an example of a public cloud service. EC2 allows users to rent virtual computers to run their own computer applications.

• **Private Cloud** – This virtualized computing environment is for the exclusive use of a single organization. It might be owned, managed and operated by that organization, a third-party or a combination of the two. It might exist on or off the organization’s premises.

• **Community Cloud** – For exclusive use by a specific community of users from organizations that have shared concerns, such as mission, security requirements, policy and compliance considerations. It is owned, managed and operated by one or more of the organizations in the community, a third-party or some combination of them, and it might exist on or off the community’s premises. Microsoft and IBM both operate scalable, on-demand community cloud services tailored to government customers.

• **Hybrid Cloud** – This virtualized environment includes two or more distinct cloud infrastructures (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables the portability of data and applications.

In “cloud bursting,” an organization uses their own computing infrastructure for normal usage, but accesses cloud services from providers to handle high/peak load times. This ensures that a sudden increase in computing requirement is managed seamlessly.

In our uncertain world, enterprises should also protect business critical applications and data against cloud service provider anomalies. Cloud computing is most commonly built on virtualization technologies to minimize cost and maximize flexibility across the various cloud computing models. As such, to avoid unexpected restrictions, the corresponding system continuity solution needs to be very flexible to support environments that range from physical data centers to cloud services settings, and can be used to protect applications from cloud to cloud.

As an example, Nirvanix, a cloud-based storage service for enterprise-level customers, ceased operations unexpectedly providing customers very little time to migrate to a new cloud storage service provider. To avoid issues with abrupt cloud service interruptions or shutdowns, the optimal HA/DR system continuity solution should be able to be deployed across VMs hosted by different cloud providers to enable fast migration with minimal business disruption.

Cloud standby servers and storage can also be used to lower the cost of remote DR for on-premise production application systems and accelerate solution deployment.

---

**Integrated System Continuity**

When evaluating virtual system continuity options, it is recommended to focus on integrated application and data protection and recovery solutions since they minimize additional workload to IT support teams. With a comprehensive solution, there should be no need to support a custom or proprietary solution that demands ongoing development and maintenance. Simple manageability means less strain on IT personnel, less chance of human errors, and more time supporting IT initiatives that contribute to business growth.
Every detail can affect continuity; in one instance, a simple system configuration mistake caused a two-and-a-half hour outage for Windows Azure public cloud customers in Western Europe. A “safety valve” mechanism designed to prevent cascading network failures was not configured properly. When there was a surge in usage, the threshold was exceeded, which generated a storm of network management alerts. The increased management traffic, in turn, triggered bugs in some of the hardware devices.

A solution that automatically recovers the affected application systems to an alternative cloud infrastructure, including another cloud infrastructure provider, could have minimized the cloud customer’s business disruption due to the failures.

**Fast Local and Remote Recovery**

Clearly, data and application outages should be minimized against all failure types to avoid business disruption, which demands a fast local and remote recovery solution. A solution that supports both local and remote recovery capabilities offers the fastest approach for system recovery.

Maximum system continuity is achieved through continuous application monitoring and data mirroring between primary and standby systems for fast automated failure detection and recovery with little or no loss of stored data. All application processes and resources, including mirrored data, are activated on the standby system so business critical applications and data can be recovered quickly. Once a failed system is repaired, the system can be restored automatically to normal operating state without manual intervention.

For local system failures, such as hardware or software failures on the primary system, automated recovery can be performed from shared or mirrored storage. Automated recovery from shared storage utilizes a local standby system at the same site with access to the same shared storage system as the primary system.

Alternatively, data can be mirrored from the primary to the standby system to support automated recovery based on system needs. For site-wide failures, such as site network disruption or facility disasters, automated recovery should be performed to a remote standby system at the remote standby site with access to the mirrored data.

**Options for Data Mirroring**

Virtual system continuity solutions should provide users the option of synchronous and asynchronous data mirroring modes to enable fast data recovery with minimal loss across a wide range of data protection and recovery needs.

- **Synchronous data mirroring technology** enables full data protection by ensuring data written to the mirrored disk on the primary system is also written to the mirrored disk on the standby system in real-time as a single transaction. Under normal operating conditions, applications will only identify successful data write operation results if data has been successfully written to both the primary and standby systems.

- **Asynchronous data mirroring** differs from synchronous data mirroring by waiting for the data write operations to complete to the mirrored disk on the primary system, but not the standby system. Instead, data write operations to the standby system are first queued then performed on a best-effort basis depending on system and network conditions. As such, less demanding network requirements come at the risk that some data will be lost if the primary system fails before the queued write operations to the standby system can be completed.

**Flexible Configurations**

A virtual system continuity solution should be flexible and easily configurable with a variety of environments, including virtual server clustering, virtual machine clustering, and physical and virtual machine clustering.
• **Virtual Server Clustering** – Virtual server clustering can be performed with a single system continuity solution across two or more virtual servers (i.e., physical hosts) running on separate physical host machines with shared external storage. The virtual server, as well as each individual VM running on the virtual server, would be monitored and protected.

In case of a virtual server or VM failure, the system continuity solution should be able to automatically failover the failed virtual server or VM to the standby machine.

• **Virtual Machine Clustering** – Unlike virtual server clustering, virtual machine clustering monitors and protects the application resources inside VMs on a more granular scale. The VM can also have a dedicated guest OS with optional virtual disks that mirror each other.

In virtual machine clustering configurations, the system continuity solution would be able to monitor and detect specific resource (e.g., virtual disk, application) failures within a VM and recover the application and resources in a running standby VM typically on a different physical host server.

• **Physical and Virtual Machine Clustering** – A system continuity solution should be able to be used to provide cost-effective standby server consolidation. Each primary physical server should be able to be clustered with a standby VM.

This protection prevents the need for a one-to-one physical server ratio when addressing system continuity concerns. Minimizing the requirements for physical servers lowers the total cost of ownership.

---

**Keeping Up with Mobility**

Business productivity today requires the flexibility of instant access to applications and data through mobile devices, such as smartphones, tablets and other tools. This mobile computing trend is driving the need for even greater application system availability and reliability.
There are more devices accessing applications and data – hosted in data centers or cloud environments – more frequently than ever before. No longer are users limited to notebook or desktop computer access, and there is reduced tolerance for downtime. As the load increases, cloud computing must meet demand as a dynamic infrastructure that can scale easily without sacrificing availability.

Business revenue and growth are increasingly dependent on this mobile computing edge, including sales force automation applications. Take, for example, a pharmaceutical sales representative who visits medical offices and must be prepared to present prospects and clients both quotes and proposals real-time.

Mobile computing is anytime and anywhere access from remote devices that IT cannot necessarily reach to reconfigure. Mobile remote access is a priority, and a system continuity solution must be flexible, fast and practical to enable recovery without requiring IT to reconfigure mobile devices.

**Conclusion**

Virtualization and cloud computing offer enticing flexibility and resource optimization value for many organizations, but it must be approached with systems continuity in mind. Beyond the additional management burden and potential performance bottlenecks, the risk of a seemingly minor failure could have a ripple effect that brings business to a standstill.

Virtual system continuity solutions should be evaluated closely to determine whether the solution can adequately detect and automatically recover from the major types of failure that could cause system level service outages. This level of fast and automatic recovery helps to minimize business disruption, improve manageability, and lower the cost of ownership.

Automated, remote DR with HA is essential to avoid data or application loss. A fully integrated, ready-to-go virtual system continuity solution saves time spent managing a custom, proprietary system. Support for various configuration options is central to a flexible and responsive system.

By focusing on the characteristics of a simple and effective system continuity solution, and remaining aware of common pitfalls, any business can enjoy the benefits of a virtualized or cloud computing environment by managing the risks.
ExpressCluster Solution

Highlights

- Fully automated local HA or remote DR software solutions for physical and virtualized systems
- Continuous application and data resource monitoring and fast recovery within minutes
- Flexible mirroring protection of data across a broad range of network environments
- Unified monitor and recovery management for multiple application systems
- Support for standard application, OS, virtualization hypervisor, and hardware for low TCO

Learn more about the NEC ExpressCluster solution at www.ExpressCluster.com or sign-up for a free 30-day trial software download at www.ExpressCluster.com/Eval

About NEC ExpressCluster Solution

The long innovation track record of NEC and its advanced technologies make the company an appealing solutions provider. For more than 15 years, NEC has been developing its ExpressCluster® Disaster Recovery/High Availability solutions for customers around the world. The NEC ExpressCluster solution is especially well-suited to reduce operational complexity and total cost of ownership by providing a comprehensive business critical system continuity solution for virtual and physical systems.

The NEC ExpressCluster solution consists of a family of integrated high availability and disaster recovery software solutions that provides continuous protection and fast recovery of applications and data required to sustain business productivity and continuity. ExpressCluster solution helps minimize business disruption due to application service outages caused by unplanned hardware, software and site failures and/or planned hardware, software and site level maintenance.

Issues with abrupt cloud service interruptions or shutdowns may be avoided because ExpressCluster software can be deployed across VMs hosted by different cloud providers. In short, the NEC ExpressCluster solution is an easy to deploy and cost-effective continuity solution for business critical systems running standard applications on major OS and virtualization platforms.

Learn more about the NEC ExpressCluster solution at www.ExpressCluster.com or sign-up for a free 30-day trial software download at www.ExpressCluster.com/Eval