

WHITE PAPER

Making Your Business Disaster Ready with Virtual Infrastructure



Table of Contents

The Need for Business Continuity..... 3

Assessing the Impact of an Outage 3

Commercially Feasible Business Continuity Strategy..... 3

Virtual Infrastructure in the Enterprise 4

 VMware ESX Server 5

 VMware Server 5

 VMware VirtualCenter and VMotion..... 5

How Virtualization Helps Business Continuity 6

 Pain Points in Current Implementations of Business Continuity..... 6

 Built-in Continuous Availability..... 7

 Hardware Independence..... 7

 Hardware Consolidation..... 7

Business Continuity Solutions with Virtualization 8

 High Availability Without Complex Configurations 8

 Cost Effective Failover Clustering 9

 Continuity with Virtual Machines on Storage Area Networks 9

 Storage Array Based Replication 10

 Virtualized Failover Site 11

 Backup Operations 12

Before and After Examples 13

 Online Hot Site..... 13

 Tape Backup and Recovery..... 13

 Disaster Recovery with Tapes for a Virtual Infrastructure..... 13

Benefits of Virtualization for Business Continuity 14

Insourcing vs. Outsourcing Trend 15

Expanding Business Continuity Coverage..... 15

Conclusion and Next Steps..... 16

List of Acronyms and Abbreviations 16

Making Your Business Disaster Ready with Virtual Infrastructure

The Need for Business Continuity

Business continuity and disaster recovery (DR) planning are critical to managing risks in a successful business. Between 60-90% of companies that don't have a proactive disaster plan find themselves out of business within 24 months of experiencing a major disaster¹. However, implementation of a reliable recovery strategy with fast time to recovery is expensive largely because it involves maintaining recovery equipment that mirrors the equipment in the primary data center. Upgrades to both primary and recovery target equipment must occur in lock-step, hence many companies forgo the process.

Yet, companies that make compromises in disaster recovery strategy such as limiting the disaster coverage to only the most critical applications, employing manual processes to recover on dissimilar equipment, or outsourcing to discount DR centers risk insufficient disaster protection in terms of application coverage, acceptable downtime, and reliability of recovery.

This compromise is not necessary. In this paper we will discuss how to make disaster recovery cost effective with virtual infrastructure.

Assessing the Impact of an Outage

Business operations that are heavily dependent on information systems may be significantly impacted even by a brief application outage. Impact of a data loss is even more drastic. IDC estimates that in a disaster situation, the average loss is \$3 million per incident and \$381,000 per hour.

To develop an effective business continuity strategy, businesses must evaluate their IT applications and assess how critical each application is to the business operation.

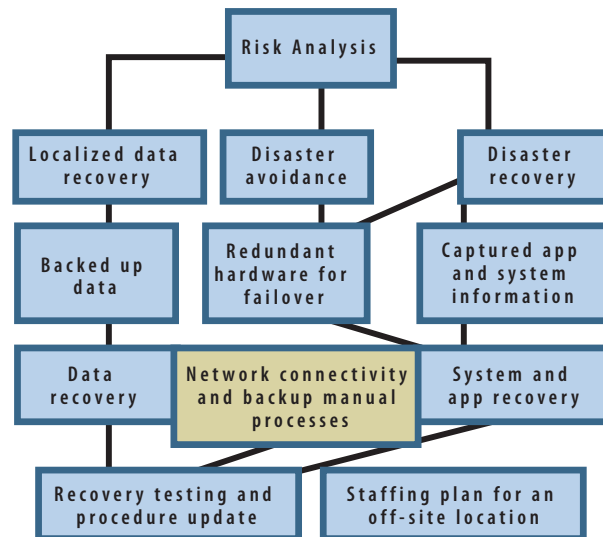
This assessment may include:

- Hourly cost of outage (especially critical in revenue generating systems such as e-commerce and CRM)
- Reliability of recovery (especially critical in financial systems)
- Existence of alternative or manual processes that can be temporarily used in case of disaster

A comprehensive business continuity strategy includes a combination of disaster protection methods for different applications ranging from disaster prevention to hot sites and data backups, as well as a staffing plan for disaster situations, a well documented plan of action, and audit and testing processes.

Specifically, the cost of including a specific application or

system in the disaster protection plan (under the umbrella of the larger business continuity plan) should be gauged against the potential risk and impact of the outage of this application. It is only sensible to implement disaster recovery for the applications where such solution costs are lower than the impact of the outage.



Commercially Feasible Business Continuity Strategy

There are several metrics commonly used in planning for disaster mitigation. Two of the most commonly used metrics are recovery point objective (RPO) and recovery time objective (RTO). Both are measured in minutes and hours. RPO describes how far the recovered data are out of synch with the production data at the time of the disaster. RTO describes how fast operations can be restored.

Other issues to consider are whether partial restoration of the IT systems such as restoration with decreased performance, decreased failure tolerance, or a partially incomplete set of data is sufficient to resume business operations after a disaster.

Methodologies for mitigating problems are as varied as the problems themselves.

Let us look at several possible information system (IS) designs for business continuity.

¹The Definitive Handbook for Business Management

- **Continuous availability.** In this architecture, the workloads are load balanced over several – often geographically distributed – platforms. Each platform is provisioned to have spare capacity. When one of the platforms fails, the workload is distributed over the remaining platforms. This approach is attractive because it allows companies to maintain business operations even after the disaster has occurred. Business operation is continuous and uninterrupted.
- **On-line and near-line hot sites.** This strategy assumes availability of a failover site, which is equipped with power, cooling, network connections, physical security, and any other critical requirements. Sufficient equipment is available to resume business operations at the failover site in case a disaster is declared. Such a site can either be owned by the business or be provided by a third party. The data, application, and system information is replicated to the failover site either by using data replication methods or by shipping media with backed up data.

This approach is attractive because it does not require a complete system overhaul like the continuous availability approach does; however, it still permits recovery from a regional disaster such as an earthquake or a hurricane.

- **Backup to tape.** Finally, there is the well-understood method of backing up the data to tape using one of the popular backup management software packages. With this methodology, the backup is performed on a file-by-file basis. The backup may be full (all files are backed up), incremental (only files that have been modified since the last backup are saved to tape), or differential (all files modified after the last full backup are saved to tape). The tapes can then be stored in an off-site location for disaster mitigation.

This approach is the least expensive and allows the use of the same methodology for discreet data problems (i.e. accidentally deleted files) and recovery in the case of a major disaster.

However, a simple backup schedule does not amount to a comprehensive business continuity plan. It also doesn't encompass a plan to recover potential data loss which makes it difficult to predict the time it will take to resume the business operations.

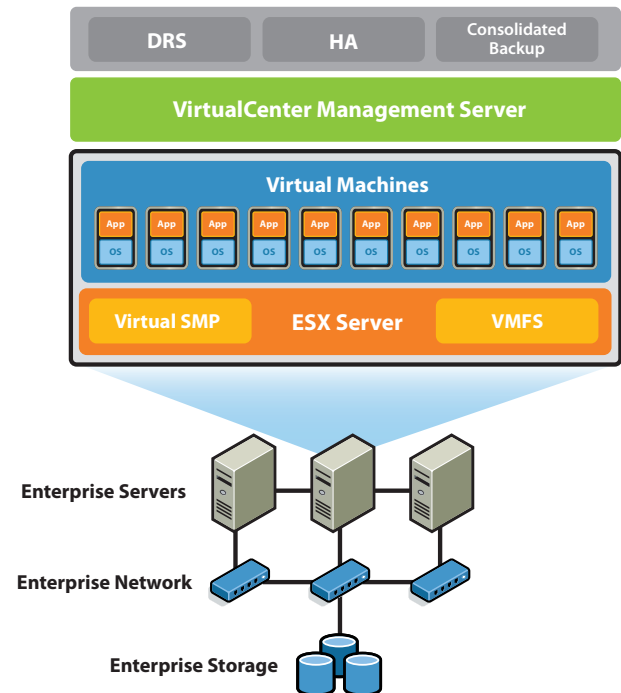
A commercially feasible business continuity strategy represents a fine balance between the cost of implementing the business continuity plan and the impact and likelihood of the potential outage. The more cost effective methods allow IT professionals to put in place continuity plans with wider application coverage, allowing near uninterrupted operations.

Virtual Infrastructure makes business continuity commercially feasible for mid-size enterprises and provides coverage beyond the top 5% of the most critical IT applications.

Virtual Infrastructure in the Enterprise

Virtual infrastructure provides a layer of abstraction between the computing, storage, and networking hardware, and the software that runs on it. Virtual infrastructure simplifies IT computing architecture, so companies can leverage their storage, network, and computing resources to control costs and respond faster. With virtual infrastructure, applications and services can be provisioned to any x86 system and easily moved between servers when conditions change. Virtual infrastructure aggregates industry-standard servers and their attached network and storage into unified resource pools. Servers are encapsulated into hardware-independent virtual machines that can run on any host in a resource pool using pre-defined resource allocations. VMware virtual infrastructure delivers a dynamic mapping of IT resources to the business. Virtual infrastructure is far more flexible and easily managed than conventional physical servers, allowing administrators to manage and optimize services globally across the enterprise.

VMware Infrastructure



The VMware Infrastructure product suite provides the server virtualization and management software needed to build a virtual infrastructure. VMware Infrastructure enables businesses to lower IT costs through increased efficiency, flexibility, and responsiveness. IT organizations can provision new services and change the amount of resources dedicated to a software service. The data center can be treated as a single pool of processing, storage and networking power.

Adopting VMware Infrastructure lets IT be responsive to business needs, including:

- 60-80% utilization rates for x86 servers—up from today's 5-15%
- Provisioning times for new applications measured in tens of seconds, not days
- Response times for change requests measured in minutes
- Zero-downtime hardware maintenance without waiting for maintenance windows
- Continuous, automated balancing of server workloads across resource pools to optimize service levels as demand varies
- High availability for all applications in the data center without extra configuration effort or added cost

The VMware virtual hardware platform implemented by VMware virtual machines makes virtual infrastructure possible. It creates a uniform hardware image—implemented in software—on which operating systems and applications run. On top of this platform, the VMware Infrastructure suite of products provides management and provisioning of virtual machines, continuous workload consolidation and balancing across physical servers, and VMotion™ technology for live migration of virtual machines.

With VMware Infrastructure, IT organizations can provision new services and change the amount of resources dedicated to a software service. Hardware management is completely separated from software management, and hardware equipment can be treated as a single pool of processing, storage, and networking power to be allocated and de-allocated on the fly to various software services.

VMware ESX Server

VMware ESX Server is the foundation for delivering virtualization-based distributed services to IT environments. A core building block of VMware Infrastructure, ESX Server is a robust, production proven virtualization layer that abstracts processor, memory, storage and networking resources into multiple virtual machines that run side-by-side on the same physical server. Sharing hardware resources across a large number of virtual machines increases hardware utilization and dramatically decreases capital and operating cost. Virtual

machines can be equipped with high availability, resource optimization, operational automation and security features that provide service levels even to the most resource-intensive mission critical applications. ESX Server delivers the highest levels of performance, scalability and robustness required for enterprise IT environments.

With VMware ESX Server:

- Applications running on dedicated systems can be moved into separate virtual machines on a single, more reliable, and scalable system.
- Servers can be remotely managed from any location, simplifying server maintenance.
- Service levels can be guaranteed with advanced resource management.

VMware Server

VMware Server is a free virtualization product for Windows and Linux servers. It enables companies to partition a physical server into multiple virtual machines and to start experiencing the benefits of virtualization. VMware Server is a robust yet easy to use product for users new to server virtualization technology and is based on VMware's proven technology, which has been used by thousands of customer for more than six years.

With VMware Server you can:

- Streamline software development and testing by allowing developers to create multiple environments with different operating systems on the same server.
- Evaluate software in ready-to-run virtual machines without installation and configuration.
- Re-host legacy operating systems such as Windows NT Server 4.0 and Windows 2000 Server in virtual machines running on new hardware and operating systems.
- Simplify server provisioning by building a virtual machine once and deploying it multiple times.
- Leverage pre-built, ready-to-run virtual appliances that include virtual hardware, operating system and application environments. Virtual appliances for Web, file, print, DNS, email, proxy and other infrastructure services are available for download on VMware's Virtual Machine Center at www.vmware.com/vmtrn/appliances.

VMware VirtualCenter and VMotion

VirtualCenter delivers centralized management, operational automation, resource optimization and high availability to virtualized IT environments built with VMware Infrastructure. These virtualization-based distributed services equip the dynamic data center with unprecedented levels of serviceability, efficiency and reliability. Centralized management capabilities provide a unified view of the entire environment and operational automa-

tion enables rapid provisioning, increased productivity, and improved responsiveness to business needs. Resource optimization delivers the highest virtual machine to physical server ratio while improving service levels to software applications. VMware DRS aligns available resources with pre-defined business priorities while maximizing hardware utilization. Migration of live virtual machines across entirely separate physical servers with VMware VMotion makes the maintenance of IT environments non-disruptive. VMware HA enables broad-based, cost-effective application availability independent of hardware and operating systems. VirtualCenter exposes a rich set of programmatic Web Service interfaces for integration with third party system management products and extension of the core functionality. VirtualCenter delivers the highest levels of simplicity, efficiency, security and reliability required to manage virtualized IT environment of any size.

How Virtualization Helps Business Continuity

Pain Points in Current Implementations of Business Continuity

There are many varied tools available for business continuity, however, due to the specifics of the Windows operating system design, even the most advanced tools can only provide a seamless restoration when the target and source physical platforms are identical. Maintaining identical physical platforms at the failover site means lock-step hardware upgrades in the primary and fail-over locations, which is prohibitively expensive. If no failover site is available, it can be impossible to locate identical hardware. Even hardware of the same series that is purchased from the same manufacturer is likely to have different firmware revisions, stepping levels, BIOS settings, or support lifecycles. Restoration to different platforms is often unreliable

and includes complex manual steps. These manual elements and the need to troubleshoot problems cause long recovery times and lack of repeatability.

To assist enterprises in disaster recovery planning, operating system vendors, applications vendors, and backup management software vendors have developed specialized APIs, tools, and best practices. As a rule, these practices involve separate processes for backing up and restoring system information, operating system information, applications, and data. Some applications and data, for example Microsoft Exchange, have modules that exhibit significantly different behavior, requiring each module to have a different disaster recovery strategy. Furthermore, each mission critical application has a different backup and recovery API. The differences are especially significant if the application needs to remain accessible for the duration of the backup. With a plurality of tools, enterprise IT managers have to learn new tools and design new strategy for each of the applications covered by the disaster recovery strategy. To complicate the situation even more, the methodologies and the APIs can change completely from one version of the application to the next. For example, a disaster recovery strategy for Exchange 2003 based on native Exchange APIs is entirely different than a disaster recovery strategy for Exchange 2000.

Because of the differences in applications and tools, disaster recovery strategy often includes several application-specific plans. Each plan has variations that have to be tested. In addition, if the strategy does not include a failover site, locating hardware to test the recovery can be a challenge.

Method	Target Recovery Time	Pain Points
Recovery from tape using backup agent native functionality	over 24 hours	Failover hardware not available for testing. Not suitable for mission critical applications.
Application specific backup agent deployed in conjunction with shadow storage volumes	4 – 24 hours	Many complex diverse application specific processes, manual processes to address dissimilarity of recovery hardware reduce reliability, separate processes for system, application, and data recovery.
Failover software with storage & server mirroring	Under 4 hours	High ongoing capital costs to maintain identical servers at the failover site. High management and maintenance expenses.

Built-in Continuous Availability

VMware Infrastructure provides inherent high availability at several levels. By their nature, virtual machines leverage high availability features in a physical server across all the virtual machines on that server. Fault-tolerant hardware features such as teamed network interfaces, multiple SAN storage adapters and redundant power supplies and memory may be prohibitively expensive for a server running a single application, but they become economical when their costs are divided between many virtual machines. VMware Infrastructure changes the way information systems are designed. Featuring such advanced capabilities as migration of virtual machines between any virtualization platforms, snapshotting, automated restarts on alternate hosts in a resource pool and VMotion, VMware Infrastructure creates environments where outages are limited to brief restarts at most. For a continuous availability solution to guard against application or hardware failure, VMware HA provides easy to use, cost effective protection for applications running in virtual machines. In the event of server failure, affected virtual machines are automatically restarted on other physical servers in a VMware Infrastructure resource pool that have spare capacity. VMware HA minimizes downtime and IT service disruption while eliminating the need for dedicated stand-by hardware and installation of additional software. VMware HA provides uniform high availability across the entire virtualized IT environment without the cost and complexity of failover solutions tied to either operating systems or specific applications.

Where continuous availability solution without application interruption is required, N+1 clustering between virtual machines hosted on different physical hardware platforms can be implemented with substantially fewer servers than normally required with conventional failover clustering. Finally, if regional disasters are a concern, Virtual Infrastructure in conjunction with SAN and data replication technology offers the highest degree of protection. Customers can use data replication between primary and failover storage arrays and bring up virtual machines at the consolidated failover site.

Hardware Independence

One of the main benefits of virtualization for business continuity is independence of the recovery process from the recovery hardware. Because virtual machines encapsulate the complete environment, including data, application, operating system, BIOS, and virtualized hardware, applications can be restored to any hardware with a virtualization platform without concern for the differences in underlying hardware. The physical world limitation of having to restore to an identical platform does not apply.

Not only does hardware independence allow IT managers to eliminate manual processes associated with adjusting drivers

and BIOS versions to reflect the change in platform, it also eliminates Windows registry issues and plug-and-play issues.

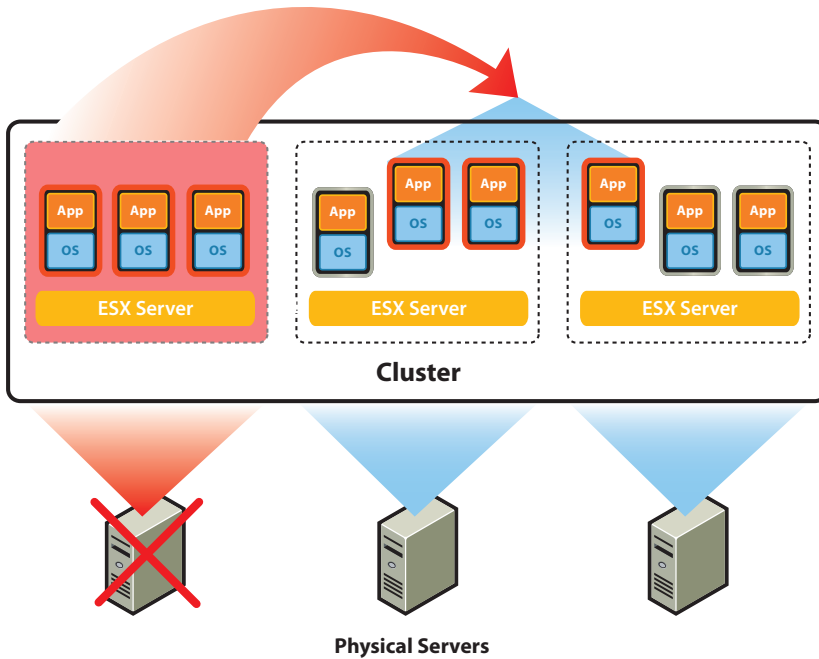
Hardware Consolidation

VMware enterprise customers actively take advantage of VMware consolidation benefits for their production and staging servers. The consolidation benefits are even greater for the failover hardware. Because it is extremely unlikely that all the workloads will fail at once and it is often acceptable to provide somewhat lower application performance in the failover facility on a temporary basis, customers experience a consolidation ratio of failover equipment that often reaches twice the consolidation ratio of the primary data center. The unexpected outcome of workload mobility and high hardware consolidation is that enterprises are able to oversubscribe hardware to multiple workloads with very little performance impact, which in turn makes in-sourcing a disaster recovery model much more economically attractive.

Business Continuity Solutions with Virtualization

High Availability Without Complex Configurations

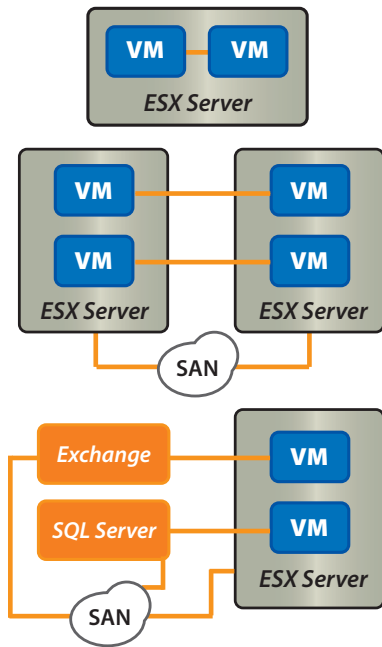
VMware HA continuously monitors all servers in a resource pool and detects server failures. An agent placed on each server maintains a “heartbeat” with the other servers in the resource pool and loss of a “heartbeat” initiates the process of restarting all affected virtual machines on other servers. VMware HA ensures that sufficient resources are available in the resource pool at all times in order to be able to restart virtual machines on different physical servers in the event of server failure. Restart of virtual machines is made possible by the VMFS cluster file system that allows multiple ESX Server installations to have read-write access to the same virtual machines file simultaneously. VMware HA is easily enabled in VirtualCenter to protect all the virtual machines in a resource pool. Compared to failover clustering solutions, VMware HA is much easier to configure and requires none of the cost and complexity of cluster-aware operating systems and applications.



Cost Effective Failover Clustering

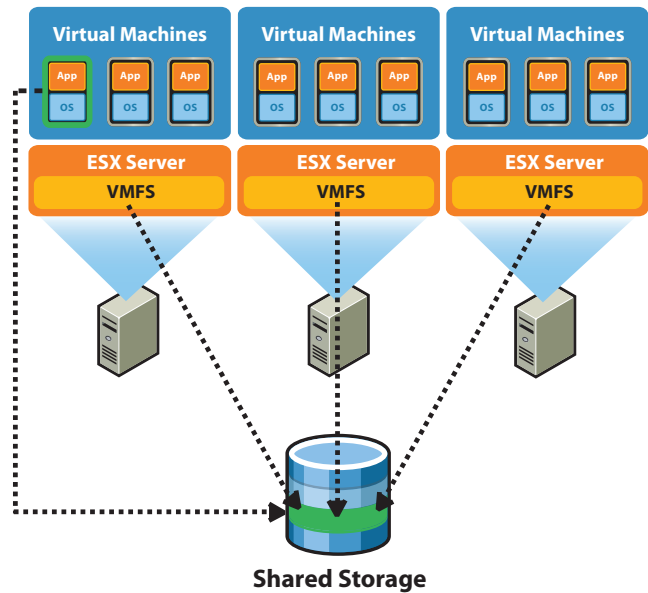
When 100% uptime is imperative, IT managers are able to create a cluster between a physical machine running mission critical workloads and a similarly configured virtual machine. The virtual machines do not consume computing resources in standby mode and can be consolidated to one or a few physical platforms at a very high consolidation ratio. As a result, the enterprise is able to realize high availability benefits without having to invest in twice the amount of hardware or having to manage and patch sprawling servers. Redundancy is reduced from 2N to N+1.

Physical-to-virtual machine clustering supports the same clustering software as physical-to-physical machine clustering. In fact, the same clustering software is supported for virtual machines as for their physical equivalent including Microsoft clustering, Veritas clustering, and Legato AAM, so no IT ramp-up is required. At the same time, reduced cost allows implementation of high availability and Service Level Agreements (SLAs) for more workloads.



Continuity with Virtual Machines on Storage Area Networks

Virtual Infrastructure deployed in conjunction with a Storage Area Network (SAN) has an additional built-in level of robustness. Any virtual machine that resides on a SAN can survive a crash of server hardware, which runs this virtual machine, and can be restarted on another ESX Server either manually, or under automated control with VMware HA. Better yet, VMware VMotion technology allows migration of a workload off a physical machine prior to a planned outage with no user downtime. Furthermore, virtualizing IT infrastructure improves the business case for increased SAN deployment. Because each server and associated host bus adapters (HBAs) are shared between multiple workloads, the per workload cost of SAN attachment is reduced dramatically. In addition, using multiple HBAs for failover and multi-pathing becomes more affordable, thereby improving availability and eliminating single points of failure.



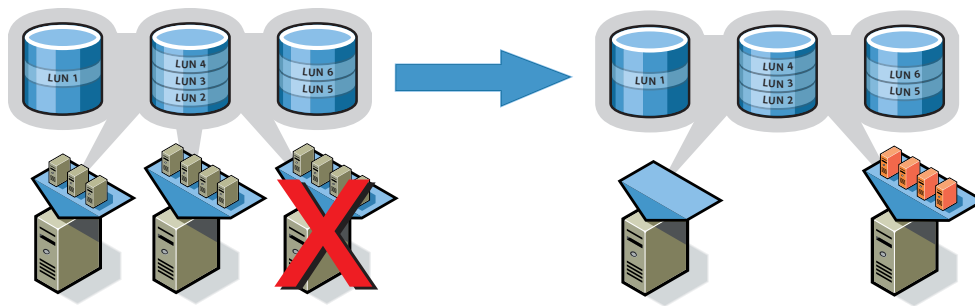
Storage Array Based Replication

For the most critical applications, many enterprises turn to storage array based data replication to a failover site. This approach provides the most up-to-date copy of the data and applications at a remote location, thereby protecting data from a regional disaster as well as from a hardware failure.

However, the question of how quickly the operations can be restored at the secondary site remains to be answered. If only storage arrays are maintained at the secondary site, the servers needed to run the applications must be procured if a disaster is declared. This configuration results in recovery time ranging from days to weeks. Also, the recovery to dissimilar hardware is a very risky manual process and in some cases is not possible.

For guaranteed recovery within hours, server hardware at the secondary site must be upgraded in lock-step with the primary data center equipment. Even this approach may not meet recovery time objectives for the more demanding workloads.

Virtual Infrastructure combined with array based replication allows enterprises to replicate the encapsulated virtual machine to the secondary site and bring it up at the secondary site in a programmatic way, without human intervention, on any available ESX Server. The hardware-independence of virtual machines means the ESX Server hardware at the secondary data center does not need to match the ESX Server hardware configuration at the primary data center. Furthermore, a higher ratio of server consolidation can be maintained at the secondary site.



Virtualized Failover Site

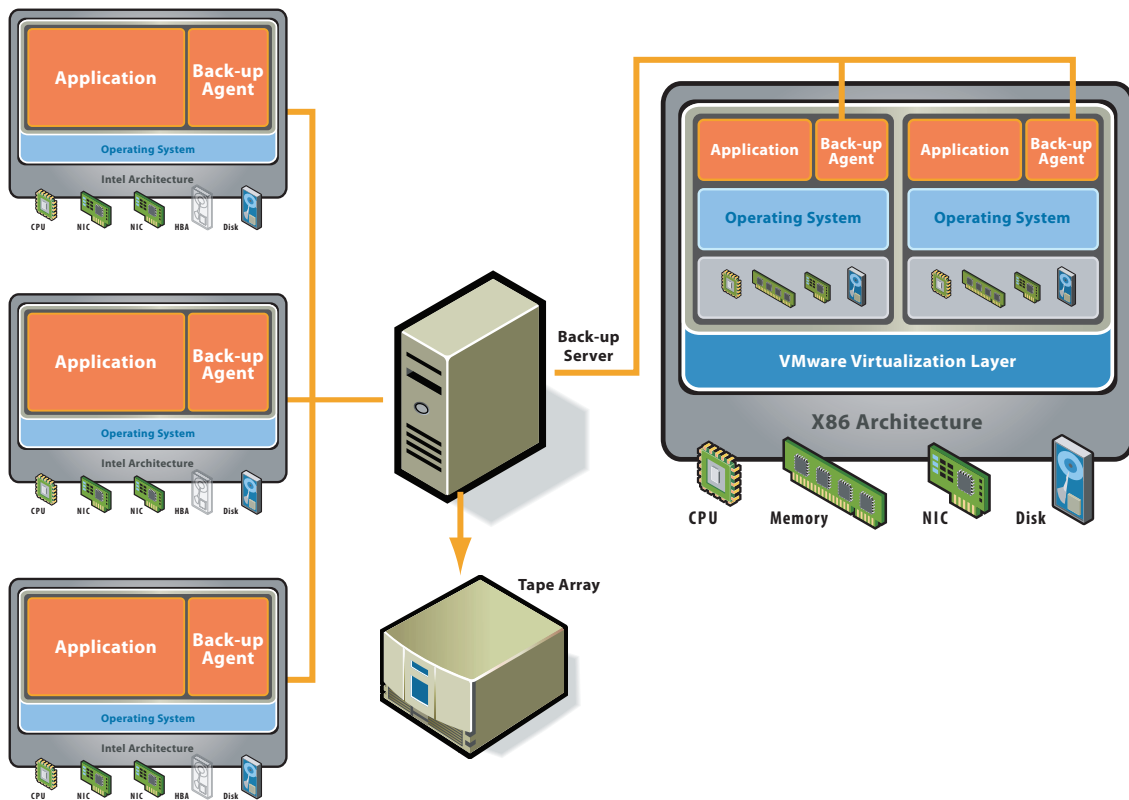
To test data restoration, IT administrators need to locate a test failover server for each of the backed up machines, install the operating system and backup agent, and then try to adjust the Windows registry and other system configurations on the test failover server. If system adjustments are successful, the backup server and the backup agent can be used to test data restoration.

The two obvious drawbacks of this approach to enabling data recovery are the need to provision several new servers and the fact that it is not always possible (or at best a long manual process) to adjust Windows registry and other system characteristics of a dissimilar failover server.

All these issues are resolved by using virtualized failover

hardware. Moreover, operating system installation, backup agent installation, and Windows registry adjustment only need to be done once. Thereafter, a fully configured virtual machine definition is stored in a virtual machine template library. For all the subsequent recovery tests the step-by-step process would be:

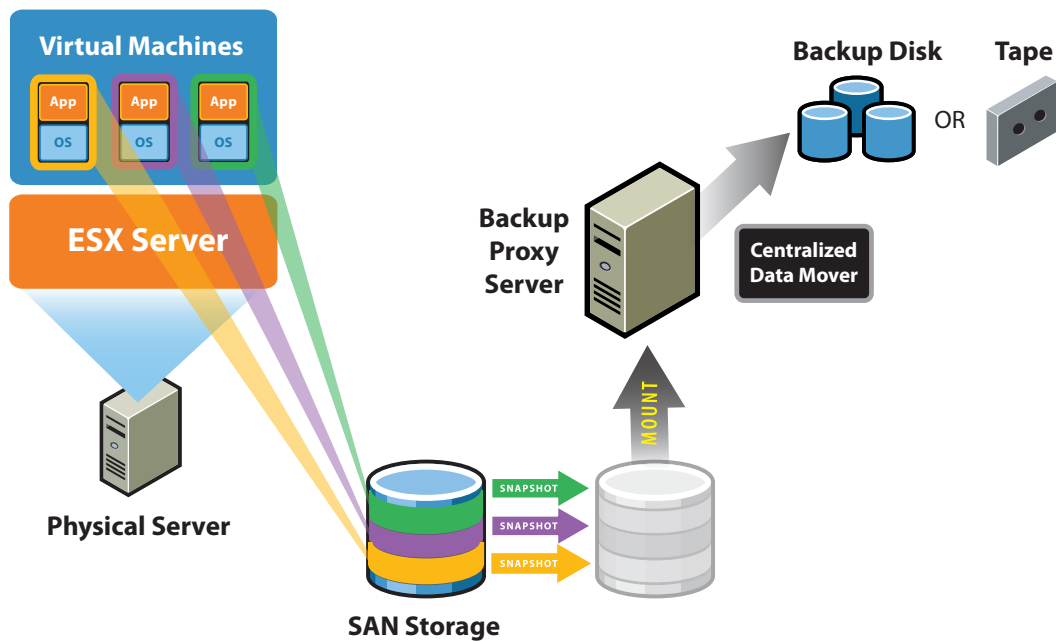
1. Source ONE physical machine, regardless of the number of servers that are slated for recovery testing.
2. Install ESX Server.
3. Copy (from a library) a virtual machine with the appropriate Windows version and backup agent pre-installed. 4. Edit IP addresses and register the virtual machine.
4. Start the virtual machine.
5. Restore (from tape) into the virtual machine using the backup agent.



Backup Operations

Backup is at the core of any disaster recovery strategy, and with virtual infrastructure, IT managers have more flexible backup options available than with physical systems. The first of those options is to continue using the existing backup processes even with virtualized hardware. VMware software supports a wide variety of backup agents operating inside VMs, which allows the backup server to control the backup and file restoration process in a consistent manner for physical and virtual servers. A second alternative is to use a backup agent in the ESX Server Management Console or on the VMware Server host operating system. This method allows IT managers to take advantage of the encapsulation property of virtual machines to capture the system configuration, the application, and the data by simply backing up the virtual disk container files.

The third and most flexible backup option is the VMware Consolidated Backup feature available with VMware Infrastructure 3. Consolidated Backup is a set of drivers and scripts that enable LAN-free backup of virtual machines from a centralized Microsoft® Windows 2003 proxy server using an industry-standard backup agent. Consolidated Backup includes pre-backup and post-backup scripts for integration with most major backup providers. The administrator creates a backup job for each virtual machine and that job is dispatched on a Consolidated Backup proxy. For virtual machines running the Microsoft Windows operating system, the pre-backup script quiesces the NTFS file system inside the virtual machine, takes a virtual machine snapshot, and mounts the snapshot to the proxy server directly from the SAN. The backup client then backs up the contents of the virtual machine—either as a set of files and directories or as a virtual disk image. Finally, the post-backup script tears down the mount and takes the virtual disk out of snapshot mode.



Before and After Examples

Online Hot Site

Let's consider a sample deployment by a VMware customer in the manufacturing industry.

The customer has implemented server consolidation with VMware Infrastructure 3 connected to an EMC Symmetrix SAN. All virtual machine images are complete with virtualized hardware, OSes, security patches, and applications residing on the SAN.

The deployment includes 78 physical dual-CPU Dell servers with VMware Infrastructure 3 installed in the main data site, and 38 HP servers in the secondary data center (17 miles away). The secondary data center is over-subscribed with the ratio of approximately 2:1. The data are synchronously replicated with SRDF (EMC remote data replication.) The two sites are connected via fiber running a dedicated OC3 connection at 155Mb/s and IP over fiber.

The virtual machines in the secondary data center are powered off during normal operation. When a disaster is declared, a script is launched that uses EMC Control Center to break off the mirroring between the SANs in the primary and secondary data centers, unlock Logical Unit Numbers (LUNs) in the secondary data center, and power on the virtual machines in the secondary data center.

The complete time to recover is now 16.5 minutes.

Before this system was implemented the disaster recovery was outsourced and a tape restore method was used on mismatched hardware. The estimated time to recover was 6.5 days. Recovery tests were never successful.

The new default IT policy states that every new application installed in the data center will be provisioned in a virtual machine and be covered under this disaster recovery strategy.

In this customer scenario, great improvements in TTR were realized, the process was made programmatic and more reliable, and per application protection costs were reduced. As a result, the customer is able to provide disaster recovery coverage to a wider range of applications.

Tape Backup and Recovery

Let's consider a pre-virtualization disaster recovery procedure with tapes.

A customer's data center applications are deployed on 15 physical servers. A backup server/agent solution is deployed.

A complete system backup-up is performed weekly, and an incremental file level backup is performed nightly.

If the server is not taken offline during a full backup, its performance is significantly impacted. Complete time to create tape backup of a 300GB data center can be estimated at 600 minutes (~500MBpm). For each server, there are three tapes (system, application, and data). Incremental backup is performed nightly. Assuming 10% of information has changed, the nightly backup window is on the order of 60 minutes.

For a disaster recovery plan that includes a secondary data center, tapes of the backup data need to be shipped to the secondary data center.

Restoration would involve locating the same number of available servers in the secondary data center (15 servers in this case). Subsequently, for each server, the IT administrator would have to assemble all the media pertaining to this server, make adjustments to the partition scheme and BIOS configuration, install the operating system, install the necessary patch level, configure networking and driver replacements, and then install the backup agent and restore the system, applications, and data from the last full backup. This work is likely to take about five hours per server. If the RPO requirement is not met, additional data can be recovered from file-based backup.

Disaster Recovery with Tapes for a Virtual Infrastructure

Now let's look at how disaster recovery procedures can be improved if the data center infrastructure is virtualized. Other data and recovery architectures are possible depending on customer-specific configurations and requirements.

In this scenario, the original 15 physical servers in the customer's data center are consolidated into 15 virtual machines on three physical servers with VMware Infrastructure 3 installed.

On a weekly basis, a full backup of the virtual disks used in each Windows virtual machine is made using VMware Consolidated Backup, and incremental backups are made nightly. Those backups are managed from a Windows backup server with an off-the-shelf Windows backup agent and VMware Consolidated Backup installed. VMware provides Consolidated Backup integration modules for a variety of commercial backup products to simplify operations with pre-configured pre- and post-backup scripts.

VMware Consolidated Backup minimizes backup windows by taking a snapshot of a virtual machine's virtual disk and generating the backup from that snapshot. Because snapshots can be created quickly with the VMware VMFS file system, operations on the virtual machine are only briefly interrupted. Consolidated Backup also ensures file integrity for backups by quiescing the virtual machine's file system prior to taking the snapshot. Virtual machine snapshots are made by putting the primary virtual disk file in read-only mode and capturing all subsequent disk writes in an appended redo log file. The snapshot

only slightly increases disk space requirements. Once the virtual disk snapshot is made, the backup agent in the Consolidated Backup server mounts it with file-level visibility to the contents of the virtual disk. Depending on the backup job setup details, the Windows backup agent can make a full or incremental backup from the virtual disk snapshot and write that backup to conventional disk or tape media. Once the backup is completed the contents of the snapshotted virtual disk's redo log is committed back to the primary virtual disk file, the redo log is deleted and the virtual disk resumes operation in its normal persistent mode.

With VMware Consolidated Backup, all backup activity is kept off the VMware Infrastructure host processors and local area network connections. Although, the backup process will take approximately the same time as in the scenario without virtualization, the backup will result in little service performance impact. There is also no need to install a backup agent in each virtual machine.

In the secondary data center, two physical servers are pre-configured with VMware Infrastructure 3. We are able to provision fewer physical servers in the secondary data center because virtual machines can be restored to any of the servers and moved between servers when utilization on one of the physical servers peaks, so a higher consolidation ratio for the secondary data center is acceptable.

The recovery will now take about five hours per physical server because of large amount of data that needs to be restored. However, because there are only two physical servers in the secondary data center now, we have reduced recovery time from 65 hours to 10 hours. We have additionally removed manual elements (hardware configuration and operating system installation) from the restoration process and made it much more reliable.

What has improved:

- Cumulative number of servers in primary and secondary data center was reduced from 30 to 5 servers.
- Recovery time was reduced from 65 hours to 10 hours + tape shipment time.
- Impact of backup process on application performance and availability was minimized.
- Fewer backup agents were required.
- Manual elements were removed from the recovery process and it was made more reliable.

An additional performance gain for recovery can be achieved by using virtual tape devices, so server backups are not interleaved on the final backup tape.

Benefits of Virtualization for Business Continuity

If the recovery time objective for recovery to the state of the last full backup is under one hour, the only successful recovery strategy is to maintain a secondary data center equipped with the same model hardware as the primary data center, server for server.

A bare metal restore tool can be used in conjunction with backup or disk replication software to restore each of the mission critical servers – complete with the operating system and the mission critical application – to the corresponding server in the secondary data center.

The recovery procedure is specific to each server, so each server recovery has to be tested separately.

When the secondary data center is virtualized, there are three immediate benefits:

- There is no need to maintain the same model hardware because IT managers can restore applications encapsulated into virtual machines to any x86 architecture hardware, and they don't need to license specialized bare metal restore tools.
- IT can pool together all the data center hardware and realize economy of scale benefits.
- IT managers only have to manage a single type of data—encapsulated virtual machines—for capture and recovery. This approach drastically simplifies management complexity compared to the traditional approach of having to deal with disparate systems, applications, and data.

The secondary data center doesn't need the same model hardware, so upgrades of the secondary data center do not need to be done in lock-step with the primary data center. While servers in the primary data center are replaced on average once every three years, the servers in the secondary data center may have a life of six years. As servers in the primary data center are phased out, they can be redeployed to the secondary data center to augment capacity.

The ability to pool hardware resources together and balance all the mission critical workloads across the different servers in the data center results in an increase in the consolidation ratio in the secondary data center with minimal impact on the availability. For example, a twofold increase in consolidation ratio may only result in a decrease in availability from 99.98 to 99.95 in the restored applications, even in a case where all the DR-protected applications failed at once.

Reducing the server population immediately results in lower TCO because of lower power and cooling requirements, facilities requirements, wiring and networking elements, and savings on hardware maintenance.

More IT effort is saved because there is less need for hardware upgrades (longer hardware life), simplified recovery testing (test once to recover all virtual machines), and shorter personnel training (uniform processes for all the applications)

Figures gathered from typical VMware customers using virtualized business continuity solutions show these total cost savings given the same level of protection:

- Capital cost reduction: 50-70% a year
- Variable cost reduction: 60-80% a year
- IT resource requirement reduction: 70-90% a year

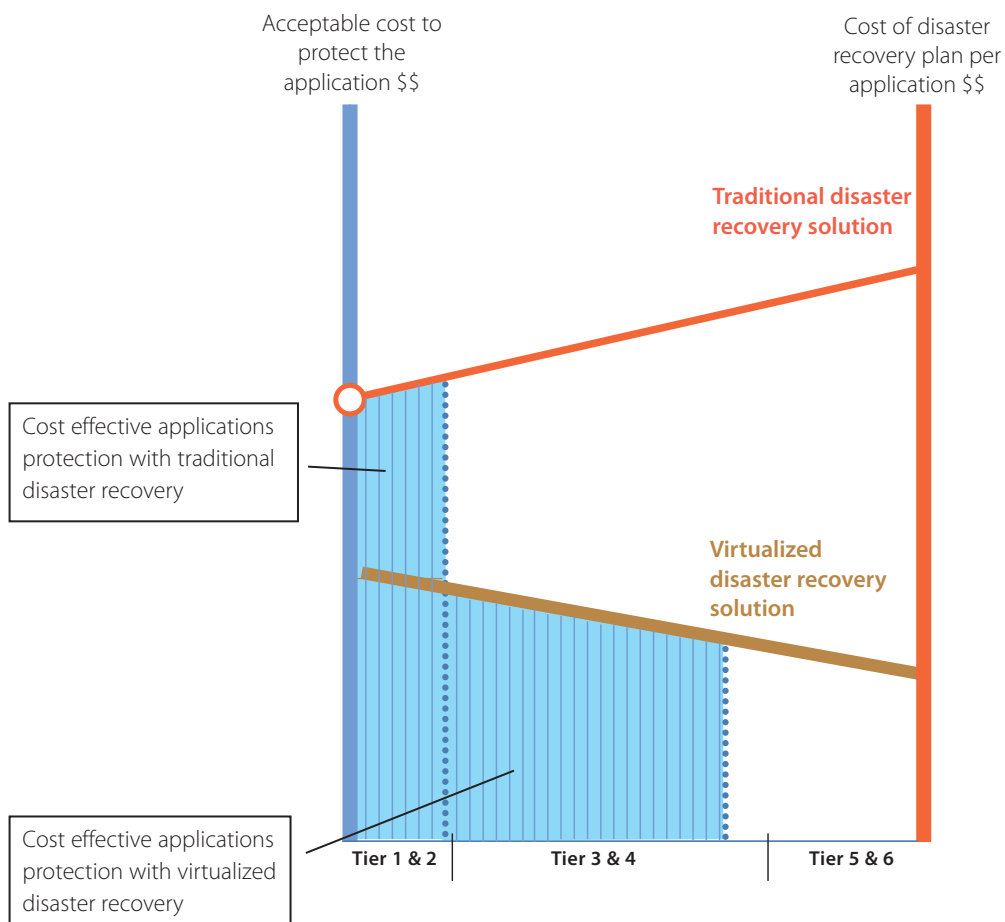
Insourcing vs. Outsourcing Trend

Outsourcing disaster recovery facilities, popular among medium size enterprises in the last several years, has been decreasing lately. The reason for the trend reversal is both the tendency of

the leading outsourcers to over-extend their resources, decreasing the quality of service, and the first-come/first-served policies that create additional risk in regional disaster situations. Virtualizing failover facilities and consolidating failover servers to fewer physical boxes allows enterprises to insource, while maintaining the same or better cost structure as with an outsourcing model, and remain in control and avoid risk.

Expanding Business Continuity Coverage

Incorporating virtualization with business continuity planning results in much lower fixed costs for implementing a hot failover site. In addition, per application business continuity TCO is lower because business continuity processes are standardized.



Conclusion and Next Steps

Using virtualization for disaster recovery allows companies to extend the disaster coverage to more applications while reducing the recovery time and making the process more reliable. To learn more about business continuity solutions with virtual infrastructure, visit <http://www.vmware.com/solutions/continuity/>. To get help implementing business continuity solutions in your environment, email sales@vmware.com or call 877-4VMWARE. VMware and VMware Authorized Consulting partners offer Disaster Recovery and Backup workshops and customized services to assist new and experienced virtual infrastructure users in planning business continuity solutions.

List of Acronyms and Abbreviations

API – Application Programming Interface

BC – Business Continuity

CRM – Customer Resource Management

DR – Disaster Recovery

ERP – Enterprise Resource Program

IT – Information Technology

IS – Information Systems

RTO – Recovery Time Objective

RPO – Recovery Point Objective

TTR – Time To Recover

SAN – Storage Area Network

SI – System Integrator

SLA – Service Level Agreement

VM – Virtual Machine

VMware VMFS – Proprietary file system optimized for VMware ESX Server Virtual Machines



VMware, Inc. 3145 Porter Drive Palo Alto CA 94304 USA Tel 650-475-5000 Fax 650-475-5001 www.vmware.com

© 2006 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156 and 6,795,966; patents pending. VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation. Linux is a registered trademark of Linus Torvalds. All other marks and names mentioned herein may be trademarks of their respective companies.

