

Disaster Recovery Solutions from VMware

Transforming Disaster Recovery - VMware Infrastructure for Rapid, Reliable and Cost-Effective Disaster Recovery

Disaster Recover Challenges Today

In today's business environment, having robust disaster recovery is no longer a luxury, it is a necessity. Given the high probability and variety of events that cause outages, including natural disasters (hurricanes, earthquakes, snow storms, flooding) and man made events (power outages, terrorism, viruses) a disruption to business systems is not a question of if, but when. Disaster recovery needs to be core to your IT strategy.

With the increasing number of x86 based servers running mission critical applications—such as Microsoft SQL Server, Exchange Server, CRM applications, Oracle databases—the need for disaster recovery has never been more relevant and urgent. Additionally with multi-tier dependencies, many unprotected lower tier applications (eg., DNS, AD) will compromise recovery for your dependent Tier 1 service (e.g., database). IT and business executives often struggle to protect their IT infrastructures due to a lack of pragmatic, cost-effective and reliable solutions.

While the need for protecting IT resources from disasters is a business imperative, IT managers are faced with many obstacles when developing a traditional disaster recovery plan, including:

Traditional Disaster Recovery is Expensive

- Ensuring successful recovery requires identical hardware configurations at the recovery site, which often mandates expensive new server purchases.
- Disaster recovery sites are often dormant or idle, yet still occupy precious real estate, require periodic management and incur high power and cooling costs.

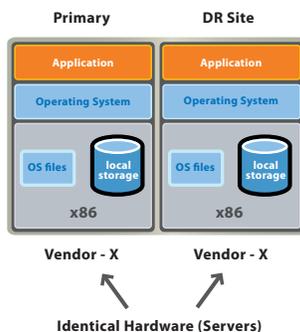


Fig 1. Traditional 1:1 hardware dependence at the primary and disaster sites quickly translates to expensive hardware costs, complex recovery tools and processes, and difficulty in testing disaster recovery plans.

Traditional Disaster Recovery is Complex and Slow

- Complex tools and processes such as system imaging tools, tape backups and bare-metal restore processes for system, application and data recovery require specialized skills and resources that are difficult to acquire and maintain
- Application, system and configuration data needs to be saved and cloned or replicated using unique and complex processes.
- Provisioning physical systems for recovery (see figure below) and configuring these systems is time consuming. In addition, application and data recovery can take from several hours to several days for each system, significantly limiting your ability to meet a recovery time objective (RTO), which is the maximum outage duration that your end users can withstand without being disruptive to your business. This problem is worsened when each unique piece of hardware requires a separate image.
- Traditional methods of recovery such as tape recovery or system image recovery have a high rate of failure, impacting the ability to recover and compromising your recovery point objective (RPO), which is the amount of data loss your operation can tolerate without it being disruptive to your business.

Physical Recovery Process

Recovery in Several Hours!



Fig 2. Physical to physical recovery process is complex and includes unreliable recovery steps that often require server rebuilds and significantly slows down recovery.

Existing Disaster Recovery is Unreliable

- Traditional disaster recovery solutions are a challenge to test especially when multi-tier applications are involved
- Complex tools and unique processes for system, application and data recovery make disaster recovery testing tedious and time-consuming, leading to infrequent or incomplete testing
- An untested disaster recovery plan can lead to a false sense of security and will often not perform when required. Strict hardware dependencies often impede the reliability of recovery.

Given the costly, growing number of x86 servers in most business environments, many IT managers save expenses by protecting only a few mission critical applications and accepting higher recovery time objectives (RTO) for other applications. The downside to this approach is that “privileged” applications are often tied to lower tier applications so when unprotected systems go down your privileged applications are exposed to extended downtime risk.

Transforming Disaster Recovery with VMware Infrastructure

VMware Infrastructure¹ is transforming the way disaster recovery is done today and in the future. It changes the disaster recovery paradigm to one that is cost effective, rapid and reliable. It enables recovery for all of your production applications across your x86 infrastructure and allows you to increase application coverage for disaster recovery by protecting all your important applications (Tier 0, 1, 2), not just a handful of privileged Tier-0 applications.

Core Properties of VMware Infrastructure

To understand the transformative value VMware[®] Infrastructure brings to disaster recovery, it is important to briefly cover the four core properties of VMware Infrastructure that enable a new approach to disaster recovery.

PARTITIONING. Partitioning enables consolidation of multiple applications and operating systems on the same machine, which drives up server utilization. This lowers capital costs and provides significant operational savings that will help fund your disaster recovery plan thereby making disaster recovery more affordable.

HARDWARE INDEPENDENCE. VMware virtual machines are hardware independent and can run on any x86 hardware without requiring any changes or modifications. This property significantly accelerates recovery by simplifying system startup and configuration (for recovery) at the disaster recovery site. It also minimizes the complexities, slowness and uncertainties of using traditional recovery mechanisms such as system images, bare-metal restore, and error prone tape recovery. You can also use any server hardware for recovery at your disaster recovery site, thus making it possible to avoid the cost of purchasing identical brand new servers for recovery.

ENCAPSULATION. Encapsulation means that an entire server–operating system image, application, data, configurations, and state—is now simply stored as a file on disk. This encapsulation property transforms and simplifies tasks such as server migration, backup and recovery, replication and disaster recovery server provisioning. These tasks can instead be treated as a simple data migration, file copy or file export activity. There is no need to build an image from scratch or use multiple complex tools for recovery of system state and configuration.

86% of VMware customers use VMware Infrastructure in production; 55% of VMware customers use VMware Infrastructure for Business Continuity and Disaster Recovery.

VMware customer survey (Sept 2006)

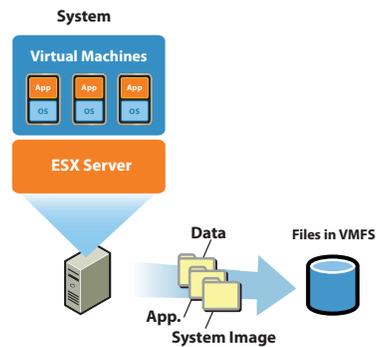


Fig 3. Encapsulation of system, data and application into a single file accelerates the reliable provisioning of recovery systems.

ISOLATION. Changes or instability in one virtual machine are completely isolated from other virtual machines on the same host. In the VMware Infrastructure environment, you can run disaster recovery tests on the actual disaster recovery hardware without impacting the ability to recover production virtual machines if your production site fails during a disaster recovery test. You can also eliminate idle hardware at your disaster recovery site by simultaneously running a test-dev or batch program workload, enabling you to maximize the utilization of your IT assets.

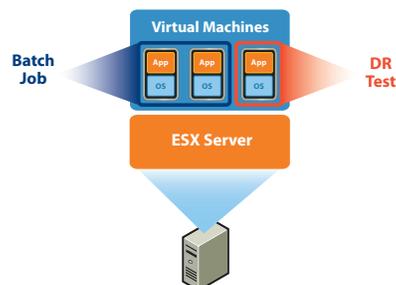


Fig 4. Tight isolation between virtual machines delivers application stability for multiple workloads and reduces security vulnerabilities.

Comparing Physical Recovery Process and Virtual Recovery Process

Virtualization makes it easy to copy, clone and replicate system resources—all essential to system and application recovery. This property significantly benefits the provisioning and recovery processes of a disaster recovery scenario whether it is backup and recovery or remote disaster recovery using replication. The conceptual diagram below provides an example from a real VMware customer of how their time to recovery was improved from over 40 hours in their prior physical-to-physical recovery scenario to 4 hours in a virtual-to-virtual recovery process.

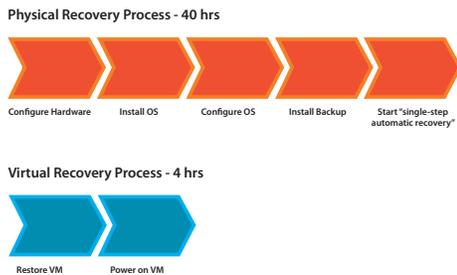


Fig 5. Virtual to virtual recovery significantly accelerates the recovery process at the disaster recovery location.

Because complex operating system files can now be stored on shared storage, transferring them to your recovery site is dramatically simpler. You can employ a wide variety of replication and backup technologies to copy systems and data offsite, an intrinsic component of your disaster recovery plan. Because complex operating system files can now be stored on shared storage, transferring them to your recovery site is dramatically simpler. You can employ a wide variety of replication and backup technologies to copy systems and data offsite, an intrinsic component of your disaster recovery plan.

End-to-End Disaster Recovery Solutions with VMware Infrastructure

VMware Infrastructure enables simpler and faster processes that allow organizations to perform easier backup and recovery as the first step to disaster recovery. For more stringent RTO and RPO scenarios, VMware Infrastructure integrates with key host-based and array-based replication technologies. VMware Infrastructure-based disaster recovery solutions also simplify the process of periodically testing your disaster recovery plan, a must for reliable disaster recovery.

Back-up and Recovery for Disaster Recovery

Tape is the most common form of transport for recovery, especially for smaller sized businesses. Backup and recovery of virtual machines is an essential component of protecting your application and data. While backup and recovery is not always the safest and fastest route to effective disaster recovery it clearly has its place in an overall recovery strategy. It is however not recommended for the most demanding applications where RTO of minutes or a few hours at most are an intrinsic part of your service level agreement (SLA).

Depending on your data protection and recovery needs there are three methods for backing up virtual machines with VMware Infrastructure: backups run from within a virtual machine, backups run from the VMware ESX Server Service Console² and VMware Consolidated Backup.

Backup from within a VMware Virtual Machine

The backup agent for a third-party backup product is located within the virtual machine and the same configuration and procedure applies as backing up with physical machines. This method provides "file-level" backup and restore for the virtual machine.

Backup via the VMware ESX Server Service Console

With backup from the ESX Service Console, the agent runs within the Service Console and backs up an entire virtual machine image (by backing up the small number of files that encapsulate it). This method of back up provides a simpler way to back up full system images without affecting the applications running on individual virtual machines. It offers less granular restore than the in-virtual machine approach since you can only restore full disk images, not individual files within virtual machines. It is the preferred method if all virtual machine images need to be restored quickly and at once. In-virtual machine and in-Service Console backup are complementary and a combination of both should be used based on requirements.

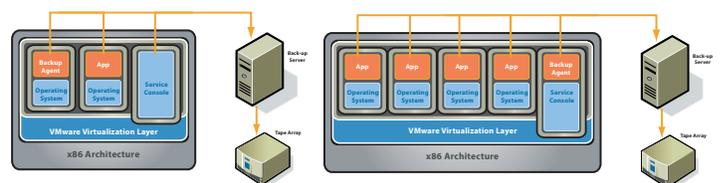


Fig 6. In-VM or Console Based Backup provides the flexibility to do file or image based backups.

VMware Consolidated Backup

Combined with backup software from a backup software provider, VMware Consolidated Backup (VCB), which is included with VMware Infrastructure Enterprise, provides a simple centralized backup facility for virtual machines. It enables virtual machine contents to be backed up from a centralized Microsoft® Windows 2003 proxy server rather than directly from ESX Server.

VMware Consolidated Backup allows IT organizations to:

- Perform full image and incremental file backup (Windows only) of running virtual machines for recovery of individual files and directories. Linux image based backups are also supported with VCB.
- Improve manageability of backup agents by using a single agent on a proxy server rather than an agent on every virtual machine.
- Eliminate backup traffic on the local area network by utilizing tape devices attached to your storage network for virtual machine backups (LAN free backup)

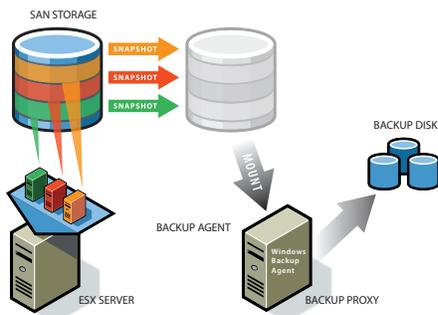


Fig 7. Shrink backup windows using image or file based backups using Centralized LAN free VMware Consolidated Backup (VCB).

Data Replication for Disaster Recovery

For applications that require much faster recovery than tape recovery can provide, replication technology is an essential component of an end-to-end, wide-area disaster recovery strategy. VMware Infrastructure works with today's leading replication technology solutions, including host (server-based) replication, array based replication and network-based replication solutions. For important mission critical production workloads like protecting an enterprise-wide CRM database or a critical email and messaging application, array and network-based replication technologies are highly recommended. Most leading replication vendors take advantage of the encapsulated files whether it is a snapshot, asynchronous or synchronous replication technology.

43% of VMware customers use VMware Infrastructure as a default policy for production servers.

VMware customer survey (Sept 2006)

Below are examples of host-based replication and array-based replication recovery approaches that work with VMware Infrastructure (please check with your storage and replication provider for specific support needs)

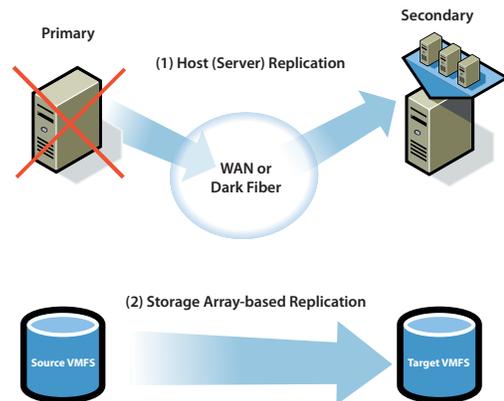


Fig 8. Use VMware Infrastructure with your server (host) or storage based replication technologies to meet your recovery point, and recovery time objectives.

Testing Disaster Recovery to Ensure High Reliability

Having a disaster recovery plan and not testing it is nearly equivalent to not having a disaster recovery plan at all. In fact, an untested disaster recovery plan can be riskier than not having a plan because of the false sense of security it can provide.

VMware Infrastructure makes disaster recovery testing very simple and is built around a premise that disaster recovery tests should be conducted as part of the periodic maintenance of any reliable recovery plan. Moreover, using the properties of isolation between virtual machines discussed earlier, VMware Infrastructure enables disaster recovery servers to run multiple workloads at the disaster recovery site. This prevents the "idling" of your expensive DR server resources.

The figure below shows a typical VMware Infrastructure based disaster recovery test configuration. The use of virtual machines makes it possible to simultaneously and quickly provision a disaster recovery test, run a batch or test workload, and provide a "live disaster recovery" stand-by configuration to take over should a real disaster occur. The test steps would typically include snapshot and cloning

of the replicated data to create test virtual machines, connecting test virtual machines to an isolated network, powering up test virtual machines to validate recovery and deleting virtual machine clones after testing. Because the process of testing is less complex, and provisioning of your disaster recovery site is faster, it minimizes the hurdle of testing, and encourages IT to test their disaster recovery plan more frequently. A well tested plan delivers greater reliability to your overall disaster recovery plan.

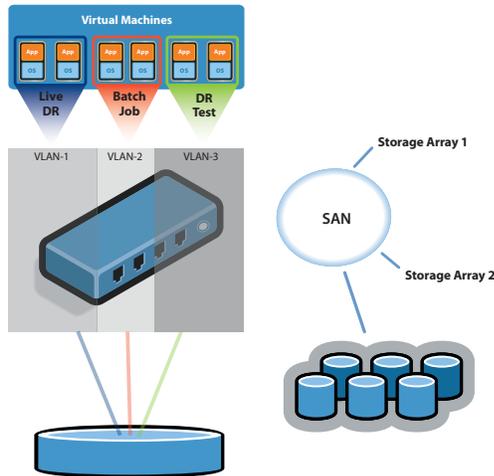


Fig 9. Reliable non-disruptive testing of your DR plan using isolated test zones alongside other productive workloads, ensures DR confidence and eliminates idle DR site resources.

Summary

VMware Infrastructure transforms disaster recovery by providing you rapid, reliable and cost-effective disaster recovery:

- Makes disaster recovery affordable through consolidation savings and re-use of existing servers for your disaster recovery site
- Provides rapid recovery that is hardware independent, simpler to backup and recover, and enables quick provisioning of your disaster recovery site
- Simplifies the ability to test thereby enhancing disaster recovery plan reliability

Next Step: Getting Started with VMware Disaster Recovery

VMware and its partners have specific services to assess your environment, specifically for disaster recovery, and design an appropriate roadmap to implement a robust disaster recovery solution.

Learn more about getting a VMware assessment at: <http://www.vmware.com/services/consulting.html>.

Contact VMware sales directly at: http://www.vmware.com/contact/contact_sales.html

Or call 1-877-4VMWARE to purchase the VMware Disaster Recovery Starter Kit, a convenient bundle of the products and services that you need to get started with a proof-of-concept or pilot of a disaster recovery solution built with VMware Infrastructure.

Evaluate VMware Infrastructure for Free

Try VMware Infrastructure software today by registering for a free 30-day evaluation license at: www.vmware.com/download/vi/eval.html

Using VMware virtual infrastructure, we can offer the same levels of service and more flexibility for up to 40 percent lower server and operating system costs.

Rob Jones, Director of Technology, Northern Europe ALSTOM

¹VMware® Infrastructure provides built-in management, resource optimization, application availability and operational automation capabilities that deliver transformative cost savings as well as increased operational efficiency, flexibility and IT service levels. A core component of VMware Infrastructure is ESX Server; VMware ESX Server is a robust, production proven virtualization layer that abstracts processor, memory, storage and networking resources into multiple virtual machines.

²The service console is a specialized virtual machine running Linux, which provides a management interface to ESX Server and the virtual machines running on it.