

WHITE PAPER

Improving Disaster Recovery with Virtualization



Table of Contents

Executive Summary 3

Challenges of Disaster Recovery 3

Components of Successful Disaster Recovery Plans 4

The Impact of Virtualization on Disaster Recovery 4

VMware Products for Disaster Recovery 5

For More Information 5

Executive Summary

Implementing disaster recovery plans for important IT services is a requirement for organizations today. However, most organizations find themselves unable to implement a disaster recovery plan that fully meets their needs for more than, at best, a select few applications due to a number of challenges including the following:

- The cost of traditional solutions is often prohibitive, forcing organizations to limit what they protect and how well they protect it.
- The complexity of traditional disaster recovery limits the ability of IT staff to implement and manage disaster recovery plans for more than a few applications.

To address these challenges, organizations are turning to virtualization solutions for disaster recovery. VMware virtualization software delivers unique capabilities that are enabling organizations to deliver practical disaster recovery solutions that deliver improved protection across a far greater set of IT services while reducing the cost and complexity of disaster recovery.

Challenges of Disaster Recovery

Creating and implementing disaster recovery plans for important IT services is a critical requirement for organizations. Downtime of important applications is a costly proposition, and extended downtime can even be fatal to an organization—industry research finds that a significant portion of companies that experience extended interruption to IT services soon go out of business. Although “disaster recovery” often conjures up images of catastrophic but infrequent events such as hurricanes, earthquakes, or terrorist acts, disaster recovery plans are also needed to handle a wide range of failure scenarios including power outages, cooling system failures, storage array failures, and human errors.

Even though organizations recognize the importance of having an effective disaster recovery plan for their IT services, most organizations struggle to deliver disaster recovery solutions that fully meet the following critical requirements:

- **Rapid recovery.** Traditional disaster recovery typically involves many complex and often manual steps that may include configuring hardware, reinstalling operating systems, reconfiguring applications, reconfiguring network configurations, and testing the recovered configuration before restoring service. Recovery is also slowed by common problems encountered during recovery such as discovering unrealized dependencies on other applications, starting systems in the wrong order, and incomplete documentation of the recovery process.

- **Reliable recovery.** Without thorough and accurate documentation of the process of recovery it is very difficult for the team executing a recovery plan to ensure that all steps of recovery are executed correctly. Even organizations that have created a runbook to document the steps in the recovery process find that keeping that documentation up to date and complete can be nearly impossible. Testing disaster recovery plans, although critical to ensuring that they are reliable, is challenging and requires significant equipment and personnel resources. Hardware dependencies and application dependencies also add to the complexity of recovery, increasing the risk of failures during recovery.
- **Affordable recovery.** Disaster recovery solutions become exponentially more expensive as expectations and requirements increase. For example, ensuring the fastest and easiest recovery possible with traditional disaster recovery plans requires duplicating the full data center infrastructure at the recovery site, doubling hardware and infrastructure costs for protected applications. Compounding the problem, it is quite difficult to make productive use of infrastructure at a recovery site without degrading recovery time because of the time and effort required to configure and reconfigure that infrastructure.

Amplifying these challenges, organizations’ requirements for disaster recovery continue to become more demanding. Expectations for availability of IT services have increased to meet the demands of a global array of internal and external users, reducing tolerance for extended downtime. Whereas recovery time objectives (RTOs) and recovery point objectives (RPOs) for critical applications measured in days were once acceptable, RTO and RPO requirements measured in hours and even minutes are now common for important applications. In addition, the complexity of applications and therefore of recovering those applications also continues to mount. Many applications today consist of multiple components that run on different systems and rely on other IT services. As a result, successful recovery requires understanding the interdependencies between of all these components and ensuring that the recovery plan correctly accounts for those interdependencies.

These challenges force organizations to make tradeoffs between the degree of disaster recovery protection that they implement and the cost and complexity of their disaster recovery plans. Organizations commonly are unable to thoroughly protect more than a privileged few of their production systems, putting them at significant risk of being unable to meet their recovery objectives when they need to recover from an outage. In particular, IT services running on x86 servers powered by Intel and AMD processors have become critical to the applications running on all of the other platforms in the datacenter but often are not as well protected as other parts of the datacenter.

Components of Successful Disaster Recovery Plans

Complete and effective disaster recovery plans need to address the following key areas:

- **Infrastructure.** A disaster recovery plan needs to ensure that the infrastructure—servers, storage, network, facilities—needed to deliver on recovery requirements is available at the time of recovery. It also needs to make it cost-effective to provide that infrastructure while not creating overwhelming complexity for IT staff.
- **Data.** Important data must be completely protected to enable successful recovery. This includes not only application and user data, but also operating system installation and configuration, hardware requirements, and firmware levels.
- **Management.** Equally important is ensuring that the disaster recovery solution can be effectively managed, from implementation to ongoing monitoring and updates to executing it when required. Ensuring manageability requires building a solution that does not overburden IT staff with the effort required to implement, test, update, and ultimately execute recovery plans.

The Impact of Virtualization on Disaster Recovery

Organizations are turning to virtualization products from VMware to address the challenges of traditional disaster recovery for their x86 infrastructure. VMware virtualization can help deliver the infrastructure, data protection, and management needed to deliver disaster recovery solutions that are faster, more reliable, and more affordable.

VMware solutions deliver the following critical benefits for disaster recovery:

- **Eliminate hardware dependencies.** VMware virtual machines are completely hardware-independent. That means that applications running in virtual machines can be recovered to any x86 server without requiring any changes and without requiring a re-install or reconfiguration of the operating system and application. This dramatically simplifies the cost and complexity of the infrastructure required for recovery—you no longer need to duplicate the primary site hardware at the recovery site, and you no longer need to make sure that that hardware is updated in lock-step with changes made at your primary site.
- **Reduce infrastructure requirements.** Because VMware virtualization enables you to safely consolidate servers, you can reduce your infrastructure requirements and the associated costs for both production and recovery. You can even take servers that you freed up by consolidating your production environment and use them for your disaster

recovery site so that you don't need to buy additional servers for that site. You also have the flexibility to recover your applications to a smaller number of servers at the recovery site initially and then add additional servers later and start taking advantage of them immediately.

- **Make productive use of recovery infrastructure.** VMware also makes it easy to eliminate the cost of not fully utilizing your recovery site infrastructure. Because virtual machines are hardware-independent, you don't have to reconfigure the recovery site hardware in order to be able to use it for other workloads and you don't need to reconfigure it for recovery. For example, you could use your recovery infrastructure for running test and development workloads during normal operation. The resource management capabilities in the VMware platform make it possible to ensure that each different type of workload on that shared infrastructure gets the right share of resources. For example, you can put your test and development workloads into a resource pool that's given a smaller share of resources compared to the resource pool that will be used to recover virtual machines if needed. While not in a failover scenario, those test and development workloads will be able to use all of the resources that are available. When you execute a recovery, the virtual machines being recovered will get the share of the total resources that you specified while the test and development workloads will be automatically limited to the share of the total resources that you configured earlier.

As mentioned earlier, protecting data is critical to ensuring successful recovery. Virtual machines store everything about a system—hardware configuration, operating system installation, application installation and data—as data files on disk. That means that any tools and processes you use to protect data can be used to protect entire systems. In a VMware environment you can easily do full-image backups that back up everything that you need to restore a virtual machine. Then when you need to recover that virtual machine at a recovery site, you don't need to spend time reinstalling the operating system and applications. For more aggressive RPO goals, replication can also be used to protect data in a virtual environment. By replicating the small number of files that make up a virtual machine, you can ensure that all of the data that you need for recovery is available at the recovery site.

VMware virtualization also enables organizations to deliver a disaster recovery plan that is significantly easier to manage. Virtualization helps to eliminate many of the time-consuming manual steps in the disaster recovery process. For example, it eliminates the need to reinstall and reconfigure operating systems and applications because everything about a virtual machine—hardware configuration, firmware level, system and application installation and data—is stored in a small number of files on disk. VMware products also make it possible to

automate the recovery process, eliminating the complexity of documenting and maintaining disaster recovery procedures in runbooks. Because VMware software simplifies disaster recovery processes, errors during recovery are much less likely, testing of disaster recovery plans is simpler, and training personnel in disaster recovery procedures is easier.

VMware virtualization can enable a better disaster recovery plan whether or not organizations have virtualized their production servers. Physical servers can be recovered to virtual machine recovery targets in a “physical-to-virtual” recovery scenario, providing the benefits of simpler and hardware-independent recovery. Even greater simplicity, reliability, and cost savings can be realized in a “virtual-to-virtual” recovery scenario where virtual machines in production are recovered to virtualized recovery target servers.

VMware Products for Disaster Recovery

VMware Infrastructure is VMware’s award-winning platform for virtualization. More 50 percent of customers recently surveyed by VMware are using VMware virtualization in their business continuity and disaster recovery plans. The VMware Infrastructure platform provides hardware-independent recovery, encapsulates virtual machines into just a few files on disk, and provides resource pools that can be used to simplify managing and utilizing infrastructure for disaster recovery. VMware VirtualCenter is an essential complement because it provides centralized management of VMware Infrastructure environments, making it easy to manage and monitor your entire virtual infrastructure.

VMware Site Recovery Manager builds on top of VMware Infrastructure by providing disaster recovery management and automation that is tightly integrated into the virtualized environment. Site Recovery Manager integrates seamlessly with VMware Infrastructure and VMware VirtualCenter to make recovery plans significantly easier to manage and update. It guides users through the process of building, managing and executing disaster recovery plans. It also integrates easily with storage replication software from leading storage vendors to simplify the use of advanced replication software with your VMware virtual infrastructure. As your virtualized production environment continues to grow, automating and simplifying the management of disaster recovery plans for that environment becomes increasingly crucial for ensuring successful recovery.

For More Information

VMware virtualization products provide proven solutions used by over 100,000 companies today. Customers of all sizes and industries are using VMware software to deliver faster, more reliable, and more affordable disaster recovery solutions for their x86 systems. To learn more about how VMware can help you to build a better disaster recovery solution, visit the VMware web site at <http://www.vmware.com/solutions/continuity> or contact VMware at 1-877-4VMWARE (outside of North America dial 1-650-427-5000).



VMware, Inc. 3401 Hillview Ave Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2008 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,961,806, 6,961,941, 6,880,022, 6,397,242, 6,496,847, 6,704,925, 6,496,847, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,944,699, 7,069,413, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,268,683, 7,275,136, 7,277,998, 7,277,999, 7,278,030, 7,281,102, 7,290,253; 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. All other marks and names mentioned herein may be trademarks of their respective companies.

