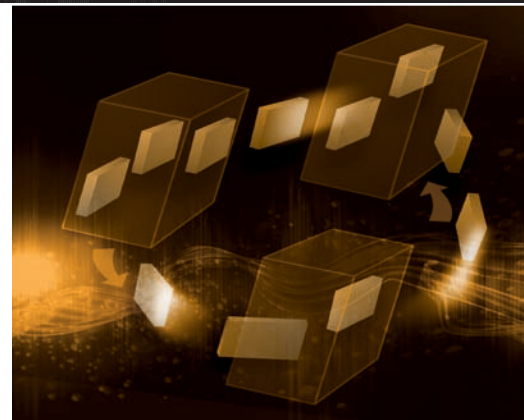


DEPLOYING SIMPLE, COST-EFFECTIVE DISASTER RECOVERY WITH DELL AND VMWARE

Because of their complexity and lack of standardization, traditional disaster recovery infrastructures often fail to meet enterprise requirements for recovery speed and integrity at a reasonable cost. By deploying VMware® vCenter Site Recovery Manager on Dell™ server and storage clusters, organizations can implement a simplified, cost-effective disaster recovery solution.



By Paul Rad
Debi Higdon
Tim Webb

Downtime, whether planned or unplanned, often translates into lost opportunities and increased costs—and for many enterprises today, any amount of downtime is unacceptable. Having an effective recovery strategy and a set of coherent disaster recovery plans is essential to helping avoid downtime during a crisis.

The need for enhanced quality, efficiency, and predictability for disaster recovery and business continuity has increased significantly, highlighting the necessity of a well-defined set of recovery plans and regular testing. However, as the required scope of critical processes, production applications, and enterprise demands increases, sustaining the timeliness and effectiveness of a recovery plan can become increasingly difficult. For most organizations, disaster recovery is extremely labor intensive, often requiring the manual coordination of hundreds of recovery tasks. So although the importance of having an effective disaster recovery plan is clear, organizations often find it difficult to achieve the level of protection they need.

Dell and VMware have partnered to offer a cost-effective, high-availability architecture based on Dell server and storage clusters and VMware vCenter Site Recovery Manager (SRM)—one designed to minimize scheduled and unscheduled downtime caused by a variety of events, including system failures, site

disasters, user errors, data corruption, and maintenance tasks. Dell offers entry-level, mid-range, and high-end server and storage clusters built from standards-based components and designed to increase availability by removing single points of failure within the cluster. At each cluster level, Dell also provides the ability to recover from additional failures, helping protect against multiple component failures. VMware vCenter SRM is a workflow tool designed to accelerate and support successful recoveries by automating the recovery process, helping eliminate complex manual recovery steps, and enabling nondisruptive testing. By taking advantage of the inherent disaster recovery capabilities of the VMware Infrastructure virtualization platform and array-based replication using Dell hardware, this architecture can help significantly simplify the planning and execution of disaster recovery strategies.

TRADITIONAL DISASTER RECOVERY AND VIRTUALIZATION

Traditional disaster recovery plans have generally involved maintaining identical, one-to-one hardware and OS configurations at a secondary site that can enable operations to quickly resume when the primary site is unavailable. This approach, however, requires investments in servers and other hardware that then sit idle at the recovery site for much of the time. Using

Related Categories:

Dell EqualLogic storage

Dell Infrastructure Consulting
Services (ICS)

Disaster recovery

Virtualization

VMware

Visit DELL.COM/PowerSolutions
for the complete category index.

hardware that is similar but not identical, meanwhile, creates challenges related to shifting workloads to a different hardware configuration—because of restrictions in putting applications together under one OS, expensive data synchronization, and infrastructure dependencies—that can lead to complex and overly expensive recovery site investments. Given the highly distributed nature of traditional IT, often because of server sprawl and lack of a shared storage environment, it can be difficult or impossible to discover and remediate missing components using a manual approach.

In addition to complex recovery plans, other key factors in traditional disaster recovery include designating the staff members responsible for executing each step of the recovery, identifying exactly when their tasks should be executed, and establishing how the success of these tasks should be determined. Complex recovery processes and dependencies, unclear or incomplete plans, and long recovery times can lead to unacceptable

results—and these problems only worsen as organizations add business processes, applications, heterogeneous hardware, and growing amounts of data.

Real-world environments typically require clear, concise recovery execution or automation, enabling staff members to execute the same tasks and achieve similar results. In particular, an effective disaster recovery plan must address three key goals:

- **Minimize downtime:** The consequences of extended downtime can be severe, not only in terms of lost business and lost productivity, but even in terms of survival for small organizations.
- **Minimize risk:** Not having a disaster recovery plan often constitutes an unacceptable level of risk—but simply having a disaster recovery plan in place does not eliminate risk if its reliability is uncertain.
- **Control costs:** Traditional disaster recovery plans are often limited in

scope because of the costs associated with building and maintaining a recovery site, training staff members in disaster recovery processes, testing those processes, and so on.

Virtualization can help address many of the challenges and barriers of traditional disaster recovery and help organizations meet the key goals of a viable disaster recovery plan. For example, many of the challenges that IT managers face are the consequence of the physical boundaries of equipment and application workloads. The encapsulation of virtual machines (VMs) means that rather than needing to maintain a corresponding server at a recovery site for each server at a primary site, organizations can replicate physical servers or VMs from the primary site to virtualized servers at the recovery site, helping to reduce the cost of protection or to increase the number of servers that can be protected by the existing recovery infrastructure.

INSTALLING VMWARE vCENTER SITE RECOVERY MANAGER

Before installing VMware vCenter Site Recovery Manager (SRM), administrators should be sure that the necessary prerequisites are in place, including the following:

- Array-based replication configured between the primary site and the secondary site
- VMware ESX 3.0.2, ESX 3.5, or ESXi 3.5 running on the servers hosting the VMs and VMware vCenter Server 2.5 running on a management server, including all required updates and service packs
- Network configuration that allows TCP connectivity between the vCenter Server systems and SRM systems at the primary and secondary sites
- Microsoft® SQL Server® or Oracle® database that uses Open Database Connectivity (ODBC), and SRM license files on the vCenter Server license server

Administrators should be sure to review the SRM administrator guide, which includes a detailed list of prerequisites, before proceeding with installation. They should also keep in mind that because SRM is installed at both the primary site and the secondary site, these prerequisites must be met at both sites.

When they are ready to proceed, administrators can install SRM using the following four basic steps at both the primary site and secondary site:

1. Create an SRM database. The installation wizard does not create this database, so this database must be created before running that wizard. Administrators should set up the SRM database as the SRM user's database and ensure that the SRM database user has administrative privileges for the database. Installation requires providing a data source name, database username, password, connection count, and maximum number of connections.
2. Run the SRM installation wizard to install the SRM server. As part of the installation, administrators connect to the SRM database created in step 1.
3. Use the VMware Infrastructure Client to connect to the vCenter Server system and install and enable the SRM plug-in.
4. Download and install the appropriate storage replication adapters (SRAs) for each array on the same physical server as the SRM service. SRA installation typically requires minimal or no configuration; detailed vendor-specific instructions are typically included in a readme file.

“As requirements for avoiding downtime become increasingly stringent, administrators need tools and platforms that can help them plan, design, and implement disaster recovery strategies that can meet those needs.”

This encapsulation helps simplify disaster recovery in a number of ways. For example, because the files necessary to protect a VM are typically stored within a single folder on shared storage, organizations can use array-based replication to replicate entire VMs simply by replicating the logical units (LUNs) on which they reside. In addition, administrators generally no longer need to worry about duplicating hardware at the recovery site or applying OS patches in parallel at both the primary and secondary sites. They also no longer need to rebuild the OS at the time of recovery, because it is already available in a hardware-independent form on the replication target. These advantages can enable organizations to reduce the recovery point objectives and recovery time objectives for the entire data center, not just for first-tier services—enhancing the level of protection while also helping simplify recovery plans and their execution.

VMWARE vCENTER SITE RECOVERY MANAGER

VMware vCenter SRM includes several key features designed to make disaster recovery rapid, reliable, manageable, and cost-effective:

- **Centralized management:** SRM provides a centralized place to create, test, update, and execute recovery plans throughout the enterprise.
- **Automation:** SRM is designed to automate the recovery process, helping eliminate many of the manual processes and associated errors that can lead to slow recovery or recovery failures.

- **Simplified setup and integration:** SRM helps simplify integration with storage replication technologies and facilitates the creation of a single comprehensive plan from existing or incomplete plans.

Planning and preparation are critical to a successful SRM deployment: before installing SRM, organizations should identify which VMs to protect, prepare data store groups, and prepare the VMware vCenter Server (formerly VMware VirtualCenter) inventory at the recovery site, following the best practices described in the “Disaster recovery planning” section in this article. (For more information on deploying SRM, see the “Installing VMware vCenter Site

Recovery Manager” sidebar in this article.) They should also be familiar with the basic components of SRM deployments (see Figure 1):

- **LUNs:** LUNs are the smallest unit of storage that can be replicated. In a VMware virtualized infrastructure, a LUN is a single SCSI storage device on a storage area network (SAN), and can be mapped to one or more VMware ESX servers. When grouping VMs on a LUN, administrators should take into account that LUNs are indivisible units—the contents of part of a LUN cannot be failed over without failing over the entire LUN.
- **Data stores:** Data stores are based on VMware Virtual Machine File System (VMFS) and can contain one or more LUNs. Like LUNs, data stores are indivisible units for storage failover. A data store spanning multiple LUNs causes those LUNs to be grouped together in a data store group; similarly, when a VM has multiple virtual disks that reside in different data stores, those data stores are forced together into a data store group to help ensure that the entire VM fails over simultaneously.

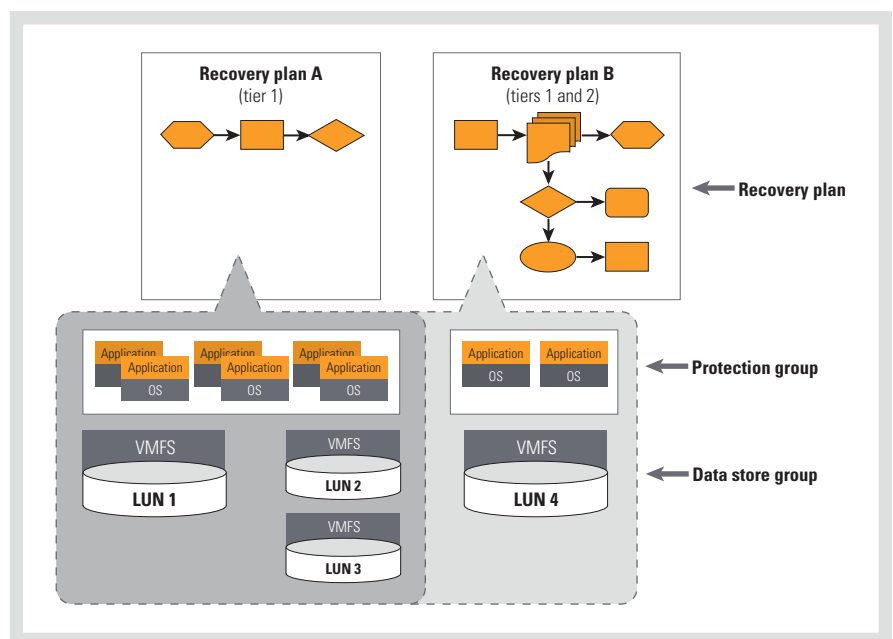


Figure 1. Basic components of a VMware vCenter Site Recovery Manager deployment

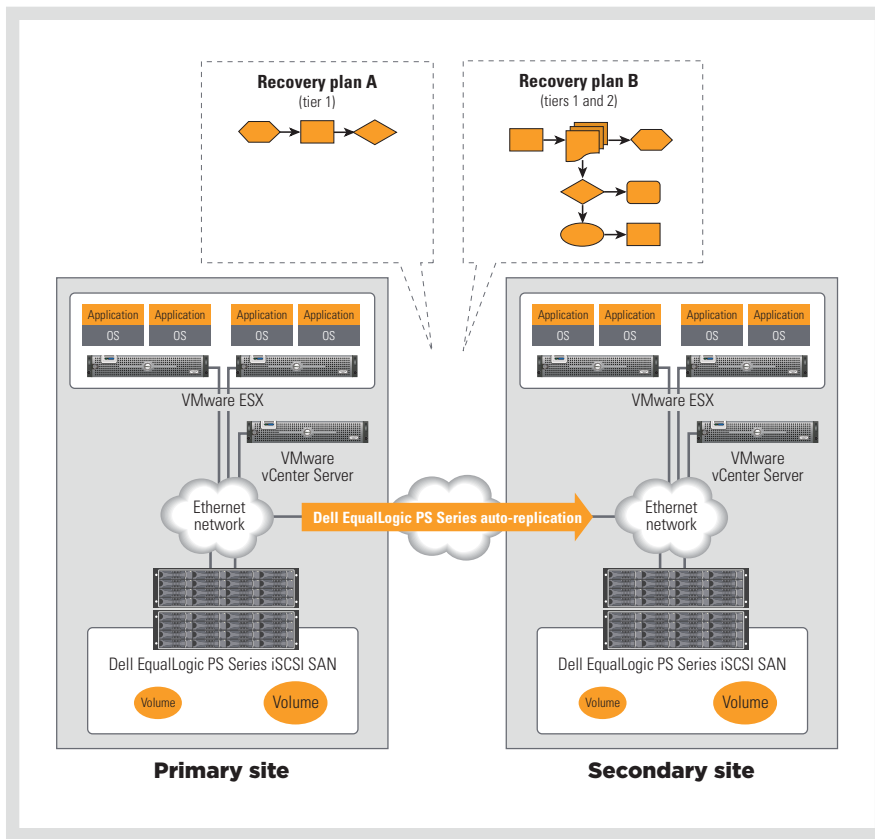


Figure 2. Example disaster recovery architecture using VMware vCenter Site Recovery Manager and Dell EqualLogic iSCSI SAN arrays

- **Data store groups:** Data store groups are auto-generated collections of one or more data stores. Like LUNs and data stores themselves, data store groups are indivisible units for storage failover.
- **Protection groups:** Protection groups are collections of all VMs in a data store group. When configuring a protected site, administrators create protection groups with a one-to-one mapping to data store groups. Protection groups are the actual unit of VM protection and recovery.
- **Recovery plans:** Recovery plans contain one or more protection groups. They comprise a list of VMs from the protection groups, a startup order for those VMs, and any custom steps added before or after VM startup—providing a comprehensive list of the

automated steps to be executed during disaster recovery tests and actual disaster recovery failovers.

Figure 2 illustrates a disaster recovery architecture based on SRM and the auto-replication features included with Dell EqualLogic™ PS Series Internet SCSI (iSCSI) SAN arrays. Administrators can configure SRM and group VMs into failover units at the primary site, and create and manage disaster recovery plans at the secondary site. The protected VMs reside at the primary site and are replicated to the secondary site.

Understanding how SRM integrates with array-based replication components is key to a successful deployment. As shown in Figure 2, primary VMs hosted on ESX servers are stored in an EqualLogic

PS Series SAN array. The array replicates shadow VMs to the array at the secondary site. Administrators should keep in mind that the storage subsystem manages and executes replication. Replication is not performed inside the VMs or by the VMware kernel or service console. SRM interfaces with the EqualLogic PS Series replication software through storage replication adapters (SRAs).¹

Each site includes its own vCenter Server system; if one site fails, the other site must have its own vCenter Server system to start the failover process and manage the ESX servers. Each VMware Infrastructure client/server pair manages the disaster recovery tasks relevant to its own site. The SRM server is a server process with its own database, and both SRM and its database are separate from vCenter Server and its database.

Once administrators have deployed the VMware software at the primary and secondary sites and established array-based replication between the sites, they can then use SRM to create disaster recovery plans that designate failover instructions. If a disaster occurs, administrators are notified and must decide whether to initiate a failover. If they initiate a failover, SRM implements the disaster recovery plan, generally following four basic steps:

1. At the primary site, SRM shuts down the VMs, starting with those designated as the lowest priority. If SRM cannot connect to the site, it notifies the administrator that it cannot power down the VMs and proceeds to the next step.
2. At the secondary site, SRM prepares the data store groups for failover.
3. At the secondary site, SRM suspends VMs designated as noncritical to provide additional resources.
4. At the secondary site, SRM restarts the VMs from the primary site, starting with those designated as the highest priority.

¹SRAs are created by array vendors to help ensure tight integration with SRM, and enable SRM to support many different arrays without hard-coding specific array knowledge into the SRM binary. As a result, SRAs can be released separately from the rest of the SRM product and downloaded by administrators from the VMware Web site. SRAs are developed, tested, and supported by the storage vendors, which helps ensure a high level of reliability and support.

DISASTER RECOVERY PLANNING

Disaster recovery planning can be overwhelming, and it can be difficult to know where to start. Organizations should begin by answering one important question: what will the costs in lost revenue be if a real disaster occurs? Determining lost revenue can help identify the impact of a catastrophic event and the level of disaster recovery needed.

Conducting a business impact assessment in the early phases of disaster recovery planning assists with mapping business processes to applications and helps define expectations. In addition, organizations should classify applications according to their importance and financial impact, and determine their recovery point objectives and recovery time objectives. These steps help clearly define which applications must be up and running first and how quickly this must occur, and also help determine the appropriate disaster recovery solution for each application—a recovery time objective of four hours requires a very different disaster recovery solution than a recovery time objective of two weeks.

Other key best practices for disaster recovery planning include the following:

- **Closely analyze single points of failure:** A single point of failure in a critical component can disrupt well-engineered redundancies and resilience in the rest of a system.
- **Plan for worst-case scenarios:** Downtime can have many causes, including operator error, component failure, software failure, and planned downtime as well as building- or city-level disasters. Organizations should be sure that their disaster recovery plans account for even worst-case scenarios.
- **Clearly document recovery processes:** Documentation is critical to the success of a disaster recovery program. Organizations should write and maintain clear, concise, detailed steps for failover so that secondary staff members can manage a failover should primary staff members be unavailable.
- **Centralize information:** In a crisis situation, a timely response can be critical. Centralizing disaster recovery information in one place, such as a Microsoft Office SharePoint® system

or portal, helps avoid the need to hunt for documentation, which can compound a crisis.

- **Create test plans and scripts:** Test plans and scripts should be created and followed step-by-step to help ensure accurate testing. These plans and scripts should include integration testing—silo testing alone does not accurately reflect multiple applications going down simultaneously.
- **Retest regularly:** Organizations should take advantages of opportunities for disaster recovery testing such as new releases, code changes, or upgrades. At a minimum, each application should be retested every year.
- **Perform comprehensive practice:** Organizations should practice their master recovery plans, not just application failover. For example, staff members need to know where to report if a disaster occurs, critical conference bridges should be set up in advance, a command center should be identified, and secondary staff resources should be assigned in case the event stretches over multiple days. In environments with many applications, IT staff should be aware of which applications should be recovered first and in what order. The plan should not assume that there will be enough resources to bring everything back up at the same time.
- **Track audit scores:** Organizations should maintain scorecards on the disaster recovery compliance of each application, as well as who is testing and when. Maintaining scorecards generally helps increase audit scores.

For a summary of key considerations recommended by Dell when planning a disaster recovery implementation, see the “10 best practices for disaster recovery planning” sidebar in this article.

EXPERT GUIDANCE FROM DELL SERVICES

Dell Global Infrastructure Consulting Services can help organizations identify,

10 BEST PRACTICES FOR DISASTER RECOVERY PLANNING

Adhering to best practices can be critical to the success of a disaster recovery implementation. The following are 10 of the most important considerations identified by Dell when planning such a deployment:

1. Articulate the need in financial terms.
2. Use hard data to create a risk profile.
3. Identify the critical resources.
4. Think beyond the data center.
5. Eliminate or mitigate single points of failure.
6. Assume that everything is going to fail.
7. Consider a virtualization data center strategy.
8. Recognize potential vendor weaknesses.
9. Keep disaster recovery capabilities up-to-date.
10. Perform tests on a regular basis.

design, and implement comprehensive virtualization solutions for their environments at a number of levels:

- Workshops:** Workshops can help organizations understand the potential of virtualization technology, including how it can help meet current and future requirements. Disaster recovery planning workshops can assist with determining the best strategy based on the level of disaster recovery capability needed.
- Assessments:** Assessments are designed to help organizations make informed decisions to help maximize the advantages of virtualization in specific environments. The assessment enables Dell to identify the scope of relevant solutions and make deployment recommendations. Using automated processes, Dell gathers up-to-the-minute information about the server environment, including key data on system inventory and up to one business cycle of performance data. Dell can then analyze the data, assess the situation, and outline options available in the existing infrastructure (see Figure 3).
- Design:** Design services can provide a comprehensive, detailed server consolidation architecture and implementation plan based on field experience, and can help organizations understand how the solution can be implemented successfully with minimal end-user disruption.
- Implementation:** Dell can implement the virtualization solution—both hardware and software—to help organizations quickly realize the advantages of virtualization in their environment.

Dell Global Infrastructure Consulting Services can also help organizations plan, design, and implement a disaster recovery infrastructure based on Dell server and storage clusters and VMware vCenter SRM.

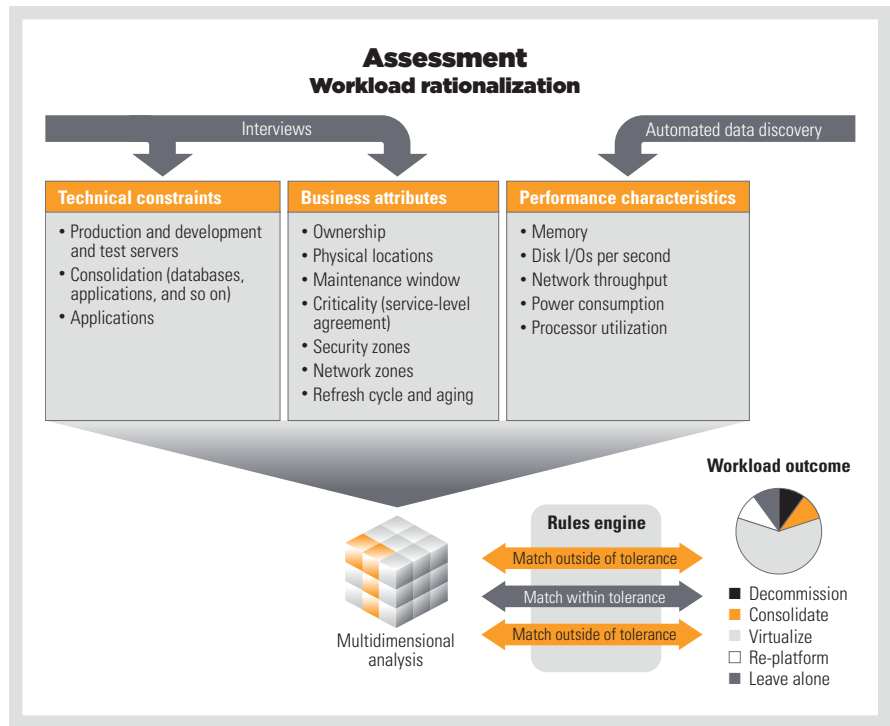


Figure 3. Example virtualization assessment process used by Dell Global Infrastructure Consulting Services

SIMPLIFIED, COST-EFFECTIVE DISASTER RECOVERY

As requirements for avoiding downtime become increasingly stringent, administrators need tools and platforms that can help them plan, design, and implement disaster recovery strategies that can meet those needs. Implementing a high-availability architecture based on Dell server and storage clusters and VMware vCenter SRM—and taking advantage of the expert guidance available from Dell Global Infrastructure Consulting Services—can provide a comprehensive solution for simplified, cost-effective disaster recovery.

Paul Rad is the practice executive for virtualization and data center optimization for Dell Global Infrastructure Consulting Services. He has master’s degrees in both Computer Engineering and Computer Science from the University of Texas at San Antonio.

Debi Higdon is the practice lead for Dell Disaster Recovery Services. She previously

spent seven years as the Dell disaster recovery test manager, facilitating the majority of Dell’s disaster recovery tests globally.

Tim Webb is the director of Dell Global Virtualization and Data Center Optimization Consulting Practices. He has a degree in Engineering from Princeton University.

MORE ONLINE
DELL.COM/PowerSolutions

QUICK LINKS

VMware vCenter Site Recovery Manager:
www.vmware.com/products/srm

Dell virtualization solutions:
DELL.COM/Virtualization

Dell Global Infrastructure Consulting Services:
DELL.COM/ICS