# Implementing HP 3PAR Remote Copy with VMware vCenter Site Recovery Manager

**Table of contents**

Executive summary ........................................ 2
  Evolution of business continuity for VMware environments 3

Overview ....................................................... 3

HP 3PAR and VMware – business continuity building blocks 4
  HP 3PAR Remote Copy for disaster recovery 4
  HP 3PAR and VMware: Partners in consolidation and virtualization 7
  Using VMware SRM for complex DR planning and management 7

HP 3PAR Storage Replication Adapter for VMware Site Recovery Manager 8

How HP 3PAR Remote Copy benefits VMware SRM deployments 8

Implementing VMware SRM with HP 3PAR Storage 8
  HP 3PAR Remote Copy configuration 8
  Site Recovery Manager installation 11
  HP 3PAR Storage Replication Adapter (SRA) Software for VMware vCenter SRM installation 15
  Site Recovery Manager configuration 16
  Testing recovery plans 26
  Recovery and reprotect 28
  Failback 30

Site failure validation 31

Implementing a proof-of-concept 35

SPC-1 benchmark 35

Summary 35

For more information 36
Executive summary

Protecting application data from disasters is critical to keeping businesses up and running. Yet traditional disaster recovery solutions were never intended to address the needs of today’s virtualized data center. As a result, the cost and complexity of using traditional disaster recovery products to address data replication needs in highly virtualized environments forces many organizations to forego disaster recovery altogether.

The combination of HP 3PAR Storage with HP 3PAR Remote Copy Software, HP 3PAR Virtual Copy Software, and VMware vCenter Site Recovery Manager (SRM) gives organizations the ability to:

- Build resilient virtual and cloud computing infrastructures
- Protect applications at a lower cost
- Recover data more quickly and efficiently than with traditional disaster recovery solutions

Integrating HP 3PAR Storage systems with VMware vSphere 5 also enables its users to:

- Double virtual machine density
- Aid in increasing storage and server consolidation efforts by up to 50%
- Monitor and manage HP 3PAR Storage from within the vSphere console
- Preserve and reclaim free space by leveraging the HP 3PAR ASIC and HP 3PAR Thin Persistence
- Boosts VMware vSphere’s return on investment (ROI) by 50%
- Enable the reduction of storage provisioning and management time by up to 90%

This white paper outlines best practices on how to set up HP 3PAR Storage with VMware SRM as well how to take advantage of HP 3PAR’s unique features to create a world class virtualized IT and application infrastructure. The information contained in this document should be used along with the documentation set provided by HP for the HP 3PAR Storage system, HP 3PAR Storage operating system (Inform), and the documentation provided by VMware for vCenter, Site Recovery Manager, and other related products.

Figure 1: HP 3PAR Storage for VMware vSphere Environments

By integrating with software from VMware, HP 3PAR Storage provides simple, reliable, end-to-end disaster recovery for virtual and cloud computing environments. The combination of HP 3PAR Remote Copy Software and HP 3PAR Virtual Copy Software with VMware vCenter Site Recovery Manager (SRM) for automated disaster recovery management provides customers with a disaster recovery solution for their virtualized and cloud environment. HP 3PAR Remote Copy Software is remote data replication software and HP 3PAR Virtual Copy Software is a reservationless, non-duplicative, copy-on-write snapshot application.
HP 3PAR Storage offers the simplest administration of any storage platform available, allowing you to reduce provisioning and management time by up to 90%. In addition, several HP 3PAR Storage features uniquely simplify administration of VMware vSphere environments by enhancing visibility into storage resources and offering superior granularity and control over snapshots and rapid online recovery.

Integrating HP 3PAR Storage systems with VMware vSphere 5 also enables its users to double virtual machine density on physical servers, monitor and manage HP 3PAR Storage volumes to create point-in-time, VM and application aware, disk-based snapshots from within the vSphere console, and preserve and reclaim free space by leveraging the HP 3PAR ASIC and HP 3PAR Thin Persistence to detect the writing of zeros and unallocated storage in a thin provisioned virtual machine. With these unique features, HP 3PAR Storage boosts VMware vSphere’s return on investment (ROI) by 50% by enabling you to optimize your data center infrastructure, simplify storage administration, and maximize virtualization savings. (Figure 1)

HP 3PAR arrays continue to capture the SPC-1 benchmark due to its architecture with multiple storage controller nodes and wide striping over available disk drives which is crucial to VMware’s demand for low latency I/O response and HP 3PAR’s ability to double VM density compared to other arrays on the market today with fewer servers.

**Target audience:** IT Administrators planning to leverage HP 3PAR Storage within a VMware vSphere 5 environment using VMware vCenter SRM for disaster recovery.

This white paper describes testing performed in April 2012.

**Evolution of business continuity for VMware environments**

A key advantage of server virtualization is that it consolidates many dedicated physical servers to virtual machines that share a smaller pool of physical servers. However, these consolidated virtual environments increase the complexity of disaster recovery by adding an extra layer of virtualization which increases the variables required to plan, test, and manage a disaster recovery scenario. No longer is a simple mapping of application-to-host-to-volume-to-replication sufficient to manage and protect the data center. As a result, customers require specific and easy to use business continuity and disaster recovery solutions for the virtual machine infrastructure.

With the right business continuity solutions in place, virtual machines can actually ease disaster recovery challenges. By encapsulating applications and operating systems in a generic virtual machine wrapper, IT departments can leverage the homogeneity of the virtual machine environment to reduce costs, ease administration, and increase agility. Physical server technology evolves over time, requiring administrators to implement new server builds and drivers to support newer hardware. However, virtual machines offer distinct advantages since they remain predictable and unchanging, even while the physical hardware beneath them is upgraded.

Virtual machines sever the ties between the virtual environment and the unpredictable physical environment, making them very portable. The portability of virtual machines allows administrators to develop disaster recovery plans that are more flexible in terms of the hardware deployed at both the primary and the recovery site. In addition, the capital expenditure outlay for equipment and the recurring management costs associated with that hardware both decrease with a consolidated environment. As a result, more and more enterprises are starting to see virtual machines as an ideal way to address disaster recovery challenges and are accelerating the move toward virtual machine adoption to meet business continuity requirements. This shift has increased the need for business continuity solutions specifically designed for virtualized environments to ease implementation and management of disaster recovery.

**Overview**

When supported with the correct underlying storage platform, server virtualization delivers greater consolidation, administrative efficiency, and cost savings. As a result, server virtualization is not only transforming the data center, but also the businesses that those data centers fuel. However, these transformative results depend on enterprise storage to deliver the performance, availability, and flexibility to keep up with the dynamic and consolidated nature of virtualized server environments.

HP 3PAR Storage was built from the ground up to exceed the economic and operational requirements of even the most demanding and dynamic IT environments, and to support a converged infrastructure by providing the SAN performance, scalability, and availability that clients need to transform the data center. The next generation of federated Tier 1 storage, HP 3PAR Storage delivers 100% of the agility and efficiency demanded by virtual data centers and cloud computing environments as part of an HP Converged Infrastructure. It does this through an innovative system architecture that offers storage federation, secure multi-tenancy, built-in thin processing capabilities, and autonomic management and storage tiering features that are unique in the industry.
When deployed together, VMware vSphere and HP 3PAR Storage deliver a compelling virtual data center solution that increases overall resource utilization, provisioning agility, and administrative efficiency, while reducing capital and operating costs.

HP 3PAR Storage uniquely enhances the flexibility and return on investment (ROI) of VMware vSphere deployments in the following ways:

**Greater virtual machine (VM) density:** The unique HP 3PAR Architecture stripes volumes widely across all drives to deliver maximum I/O throughput and minimum latencies, which mitigates server memory bottlenecks and traditional storage constraints. Increased array performance cannot only boost VM-based application performance, but when paired with the superior reliability of the HP 3PAR Storage System and advanced support of VMware’s vSphere Storage APIs – Array Integration (VAAI) capabilities, can result in higher VM density. This benefit enables organizations to double virtual machine density on physical servers, placing twice as many VMs on physical servers as with traditional storage platforms.

**Simplified storage administration:** HP 3PAR Storage reduces storage administration time by up to 90%. Rapid provisioning, autonomic load balancing, and software management products such as HP 3PAR Autonomic Groups automate repetitive storage administration tasks. Autonomic storage tiering tools like HP 3PAR Dynamic Optimization Software allow administrators to tune storage allocations without interruption to servers. Storage federation capability enables data and workloads to be simply and fluidly shifted between storage arrays without disruption.

**Integration with VMware vCenter Server:** The HP 3PAR Management Software Plug-In for VMware vCenter allows administrators to monitor HP 3PAR Storage volumes from within the vSphere console. HP 3PAR Recovery Manager Software for VMware vSphere uses HP 3PAR Virtual Copy Software to create point-in-time, VM- and application-aware, disk-based snapshots giving VMware administrators a simple process for recovering whole Virtual Machine Disks (VMDKs), individual VMs, or even individual files.

**Simplified disaster recovery:** HP 3PAR Replication Adapter Software for VMware vCenter SRM provides simple and reliable replication and disaster recovery for VMware vSphere environments based on HP 3PAR Remote Copy Software.

**Broader VMware vSphere deployment through cost-effective HP 3PAR Thin Provisioning Software:** HP 3PAR Storage enhances flexibility and reduces physical storage capacity needs in VMware vSphere environments by leveraging the cost-effective usable capacity delivered by Fast RAID 5 and RAID 6 (also called RAID Multi-Parity or RAID MP) and HP 3PAR Thin Provisioning Software. Thin Provisioning allows clients to safely over-allocate capacity upfront and then purchase actual physical capacity incrementally and only for written data. The result is a savings of 50% or more on purchased capacity as compared to traditional storage platform – guaranteed1.

**HP 3PAR support for VMware end-user computing initiatives:** HP 3PAR Storage provides rapid provisioning of both storage and virtual desktops for VMware View and VMware View Composer deployments. Together, these solutions provide storage efficiency for boot images as well as user data and deliver the performance, scalability, and high availability demanded by enterprise end-user computing deployments.

**HP 3PAR and VMware – business continuity building blocks**

HP 3PAR Storage and VMware vSphere bring unique capabilities that positively change how disaster recovery is planned, tested, implemented, and managed. Understanding these unique qualities is key to appreciating why HP 3PAR and VMware work together to deliver an ideal combined disaster recovery solution.

**HP 3PAR Remote Copy for disaster recovery**

HP 3PAR Remote Copy Software provides enterprise and cloud data centers with autonomic replication and disaster recovery technology that allows the protection and sharing of data from any application simply, efficiently, and affordably. Remote Copy Software dramatically reduces the cost of remote data replication and disaster recovery by leveraging thin copy technology, enabling multi-site and multi-mode replication with both midrange and high-end arrays, and reducing the need for professional services. Its supported native IP implementation eliminates the need for protocol extenders or converters for long distance replication.

HP Remote Copy Software offers fast, autonomic disaster recovery configuration that can be set up and tested in minutes, from a single window. With support for synchronous long distance replication, customers now have an affordable, multi-site alternative for achieving low recovery time objectives (RTOs) and zero-data-loss recovery point objectives (RPOs) with complete distance flexibility.

1 Get Thin Guarantee: [hp.com/storage/getthin](http://hp.com/storage/getthin)
The combination of the HP 3PAR Remote Copy Software, HP 3PAR Software Replication Adapter for VMware vCenter SRM, and VMware vCenter SRM enable simple, efficient, and affordable disaster recovery management across data centers that utilize VMware vSphere consolidation solutions.

**VMware vCenter Site Recovery Manager**

VMware vCenter SRM provides business continuity and disaster recovery protection for VMware virtual environments. Protection can range from individual virtual machines (VMs) residing on a single, replicated datastore to all the VMs in a data center. VMware SRM helps IT administrators plan, test, and execute the recovery of virtual machines between the protected site and the recovery site.

VMware SRM coordinates the recovery process with HP 3PAR Remote Copy Software to ensure that the virtual machines at the protected site are shut down cleanly (in the event that the protected site virtual machines are still available when recovery is invoked) so that the replicated virtual machines can be recovered and powered up at the recovery site. Recovery of protected virtual machines to the recovery site is guided by a recovery plan that specifies the order in which virtual machines are started up. The recovery plan also specifies network parameters, such as IP addresses, ensures the replicated storage holding the protected VMs is brought online and presented to the recovery hosts properly, and can contain user-specified scripts that can be executed to perform custom recovery actions.

After a recovery has been performed, the running virtual machines are no longer protected. To address this reduced protection, SRM supports a reprotect operation for virtual machines protected on array-based storage. The reprotect operation reverses the roles of the two sites after the original protected site is back up. The site that was formerly the recovery site becomes the protected site and the site that was formerly the protected site becomes the recovery site. At this point a planned migration back to the original site can be scheduled, if desired.
Figure 2: VMware SRM Deployment

Protected Site
- vSphere Client
- SRM
- vSphere Client with SRM plugin
- VMware vCenter Server and SRM Server
- Protected Virtual Machines
- Servers running VMware ESXi 5
- HP 3PAR Storage

Recovery Site
- vSphere Client
- SRM
- vSphere Client with SRM plugin
- VMware vCenter Server and SRM Server
- Protected Virtual Machines
- Servers running VMware ESXi 5
- HP 3PAR Storage

Site Recovery Manager

Replication via 3PAR Remote Replication
HP 3PAR and VMware: Partners in consolidation and virtualization

HP 3PAR Storage is highly virtualized storage built from the ground up to enhance the benefits of VMware vSphere in data center consolidation efforts. HP 3PAR Storage combines highly virtualized, autonomically\(^2\), managed, and dynamically tiered storage arrays with advanced internal virtualization capabilities to increase administrative efficiency, system utilization, and storage performance. As a result, HP 3PAR Storage boosts VMware vSphere’s Return on Investment (ROI) by enabling optimization of the data center infrastructure, simplified storage administration, and maximized virtualization savings.

Table 1 is based on documented client results that are subject to unique business conditions, client IT environment, HP products deployed, and other factors. These results may not be typical; your results may vary.

Table 1: HP 3PAR and VMware Virtualization Benefits

<table>
<thead>
<tr>
<th>Storage Consolidation with HP 3PAR</th>
<th>Server Consolidation with VMware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cut storage TCO</td>
<td>Cut server TCO</td>
</tr>
<tr>
<td>Increase capacity utilization</td>
<td>Increase CPU utilization</td>
</tr>
<tr>
<td>Reduce storage administration</td>
<td>Improve server to administrator ratio</td>
</tr>
<tr>
<td>Provision new storage in seconds</td>
<td>Provision a new server in minutes</td>
</tr>
<tr>
<td>Optimize service levels / rebalance resources with one command</td>
<td>Optimize service levels / rebalance resources by dragging and dropping</td>
</tr>
<tr>
<td>Cut storage power requirements</td>
<td>Cut server power requirements</td>
</tr>
</tbody>
</table>

Significant reduction in floor space

Simple and efficient disaster recovery for better and broader application recoverability

Using VMware SRM for complex DR planning and management

Management of a multi-layered, highly virtualized disaster recovery environment is challenging if the system administrator must coordinate actions through multiple management applications across the various components of the solution. For example, mapping the applications and virtual machines down through storage fabric zoning to the physical array volumes and VMware VMFS file systems can be difficult because it is often a many-to-many relationship. To accomplish this, the administrator must map the array volumes between sites, and again those volumes must be associated with physical servers and their specific virtual machines. If a VMware vSphere administrator migrates virtual machines between datastores, this can easily disrupt the carefully crafted mapping for array-based replication. Failure to monitor and maintain the end-to-end mappings results in loss of availability of the application at the remote site.

To alleviate these challenges associated with manual disaster recovery planning, VMware introduced VMware vCenter Site Recovery Manager (SRM) to provide end-to-end management of array-based replication and virtual machine failover for VMware vSphere environments. VMware SRM enables system administrators to discover which array volumes are protected via replication, to manage the testing and production failover of these volumes, and to restart the virtual machines at the remote site. As part of the storage discovery, VMware enumerates the volumes on each site and ensures that, for any given virtual machine requiring remote replication, all the necessary virtual machine components, datastores, and disk assets are properly mapped and accessible at both sites.

\(^2\) A storage platform with built-in self management and optimization features that does not require administrator intervention
HP 3PAR Storage Replication Adapter for VMware Site Recovery Manager

HP 3PAR Storage Replication Adapter (SRA) Software for VMware vCenter Site Recovery Manager (SRM) integrates VMware SRM with HP 3PAR Storage and replication software to provide a complete and integrated business continuity solution. The solution offers centralized management of recovery plans, non-disruptive testing, automated site recovery, and failback and migration processes. The HP 3PAR SRA software combines HP 3PAR Remote Copy Software and HP 3PAR Virtual Copy Software with VMware SRM to ensure the highest performing and most reliable disaster protection for all virtualized applications.

How HP 3PAR Remote Copy benefits VMware SRM deployments

Combining HP 3PAR Remote Copy and VMware SRM to protect VMware vSphere assets creates a best-of-breed solution that provides users with simplified disaster recovery and flexible replication options. In conjunction with VMware SRM, the HP 3PAR Replication Adapter enables users to replace independent storage and server disaster recovery processes with a single automated process and centralized interface, ensuring rapid and reliable recovery. Together, HP 3PAR and VMware ensure that recovery time and recovery point objectives can be met simply and predictably.

This combined solution also provides a new level of replication flexibility not possible with traditional disaster recovery solutions. With HP 3PAR and VMware, organizations can easily recover virtual machines on different server hardware. HP 3PAR Remote Copy enables customers to flexibly replicate between HP 3PAR Storage Systems of any model and between different service levels (for example, RAID level or drive type) for greater infrastructure agility.

The combination of HP 3PAR Remote Copy and VMware SRM blends the unique capabilities of each company for compelling disaster recovery for VMware deployments. Even customers with stringent disaster recovery requirements can implement the automated, easy-to-use solution.

Implementing VMware SRM with HP 3PAR Storage

HP 3PAR Remote Copy makes configuring the replication piece of the disaster recovery solution simple and possible to be completed without the need to hire professional services with a basic knowledge of VMware and HP 3PAR Remote Copy. Once the HP 3PAR arrays are installed, replication between the two sites can be easily configured. Remote Copy can be configured, managed, and tested in a matter of minutes. The need for costly and prolonged professional services engagements, common with other replication technologies, can be avoided. Special extenders or converters to permit long distance replication are also not needed.

HP 3PAR Remote Copy configuration

Setting up a basic HP 3PAR Remote Copy configuration can be accomplished by first selecting and configuring the ports to be used for Remote Copy functions, the ports can either be Fibre Channel or Ethernet. Once the port type is selected, change the “Connection Mode” to Remote Copy over Fibre Channel (RCFC) or Remote Copy over IP (RCIP), and then proceed with configuring the interface. It is recommended and a best practice to configure two ports (of the same type) on each HP 3PAR array from the same node pair. For more information on this topic please reference the HP 3PAR Remote Copy Software User’s Guide which can be found in the For more information section of this paper.

Once the ports are configured for Remote Copy, establish an array relationship by configuring the logical links. For VMware SRM a one-to-one Remote Copy relationship is recommended. While other relationships other than one-to-one are possible, a one-to-one relationship is a best practice and shown in this paper. A one-to-one Remote Copy relationship involves two HP 3PAR Storage systems. Depending on how the one-to-one Remote Copy relationship is configured, one server can serve as the primary (source) server and the other as the backup server (unidirectional), or both servers can serve as both the primary and backup servers (bidirectional). In order to enable SRM to be able to fail over to either site, a bidirectional relationship is required.
To configure a one-to-one Remote Copy configuration with the HP 3PAR InForm Management Console (IMC),

1. In the Manager Pane, click **Remote Copy**.
2. In the Common Actions panel, click **New Configuration**.
3. The **New Remote Copy Configuration** wizard appears.
4. Under **Select a Topology**, click **1-1**.
5. Under **Assign Systems**, click a storage server icon. In the menu that appears, select a storage server to assign. Repeat for the other storage server icon. (Figure 3)
6. Optionally, define the **System’s Location** and/or the **Target Names**.
7. Click **Next**.

Figure 3: Configure Relationship
8. A graphical representation of each system’s Remote Copy ports appears under **Create Links**. Click and drag from one port on one system to a port on the other system. Repeat for the second port. (Figure 4)

9. **Configure interconnect links**
   a. For IP links, in the IP Settings groups for each system/port, all fields are automatically populated based on the link relationship established under **Create Links**.
      i. (Optional) Enter the gateway address for each system/port.
      ii. (Optional) Click **Apply** to test the link configuration, or **Ping** to test the communication between the links.
   b. For Fibre Channel links, in the **Settings** group for each system/port:
      i. Connection Type - Select **Point** for point-to-point mode or **Loop** for arbitrated loop mode.
      ii. Configured Rate - Select 1, 2, 4 Gbps, or **Auto** (default).
      iii. Click **Apply** to test the link configuration, or **Ping** to test the communication between the links.

10. Click **Next**.

Figure 4: Configure Links
11. In the **Source** group section:
   a. **System** - Select the system on which the Remote Copy group will reside.
   b. **Domain** - Select the domain in which the Remote Copy group will reside. If not using a Virtual Domain configuration, this step can be skipped.
   c. **Group** - Enter a name for the Remote Copy group.
   d. Enable **Start group after completion** (default).

12. In the **Backup** group section:
   a. **Name** - The system NOT selected as the source system, automatically appears.
   b. **Mode** - Select Synchronous (default).

13. Click **Add**.

14. Repeat the steps above for the other array using it as the source array and the array just configured above as the backup array.

Once the array relationship is established, the next step is to select the virtual volumes that will be replicated.

1. Select a Remote Copy group from the **Group** list.
2. Under the **Source Volume** list, select a virtual volume.
3. Under the **Backup Volume** list:
   a. Select either **Existing** or **New**.
      i. **Existing**, select a backup virtual volume.
      ii. **New**:
         1) **Name** - Enter a name for the backup virtual volume.
         2) **CPG** under **User CPG** - Select a CPG from which the volume’s user space is allocated.
         3) **CPG** under **Copy CPG** - Select a CPG from which the volume’s copy space is allocated.
         4) (Optional) In the **Allocation Warning** and **Allocation Limit** text boxes, enter the appropriate information.
   4. Click **Add**.
5. Repeat steps 1 through 4 to add additional virtual volumes to the Remote Copy group(s).
6. Click **Finish**.

The two 3PAR systems are now configured in a bi-directional one-to-one remote copy configuration.

**Site Recovery Manager installation**

VMware vCenter Site Recovery Manager integrates tightly into VMware vSphere Client. When installed, a new management view is available in VMware vSphere Client where administrators can create, manage, and execute disaster recovery plans. The Protection Setup and Recovery Setup options will guide you through the wizard-based process of configuring VMware SRM. The first step in the Protection Setup process is to establish a connection between the protected and the recovery site (Figure 5).

1. Run the VMware vCenter Site Recovery Manager installer and go through the windows and the agreement until the Destination Folder window is reached.
2. In this window, select the location to install SRM; by default, it is installed into `C:\Program Files (x86)\VMware\VMware vCenter Site Recovery Manager`.
3. Click **Next**.
4. On the vSphere Replication window select **Install vSphere Replication**.
5. Click **Next**
6. In the following window, complete the vCenter Server Credentials for the local site similar to Figure 5. This will register SRM with vCenter.

Figure 5: Entering Credentials for VMware vSphere Registration of SRM

7. Click Next
8. If prompted to accept the vCenter Server certificate/thumb print, click YES to proceed.
9. The next several screens will assist in either creating or importing a certificate. The certificate is used by SRM for authentication. Either Automatically generate a certificate or Use a PKCS#12 certificate file depending on how you want to configure this step.
10. In the VMware vCenter Site Recovery manager Extension window, fill in the information for the local site as in Figure 6.
   a. **Local Site Name**: User defined string for the site name. This name will show up in SRM.
   b. **Administrator E-mail**: Email address of the site administrator. This is needed to receive notification of events that happen on the site.
   c. **Additional E-mail**: This field is optional. Enter another email address here if a second person is needed to receive notifications.
   d. **Local Host**: Select the IP of the local instance of vCenter
   e. **Listener and API Listener Ports**: Leave the defaults unless there is a specific reason not to use the defaults.

11. Click **Next**

Figure 6: Info for SRM extension registration with vCenter Server
12. In the database configuration window (Figure 6), select the **Database Client** and the **Data Source Name** (DSN) of the local or remote database server. If there is not a DSN available or created for this instance, one will need to be created. A system DSN is required, and in most cases it should refer to the localhost connection of the vSphere database.
   a. If creating a new DSN, the newly added DSN will not show up in the **Data Source Name** drop down list and will need to be entered in manually
   b. Enter in the **Username** and **Password** as well as change the **Connection Count** and **Max. Connections** as needed.

Figure 7: VMware vCenter Site Recover Manager database information

13. **Click Next.**
14. Installation of SRM will now start once the **Install** button is clicked.
15. Once the installation has finished successfully, click the **Finish** button.
16. Login to the vCenter Server and enable the plugin using the Plug-in Manager, see Figure 8. To do this select Download and Install

Figure 8: VMware vCenter Site Recover Manager Extension available as a plugin

17. Repeat at the other site.

VMware SRM is now installed at both sites and imported into VMware vCenter.

**HP 3PAR Storage Replication Adapter (SRA) Software for VMware vCenter SRM installation**

Before completing the configuration of VMware SRM, the HP 3PAR Storage Replication Adapter (SRA) Software for VMware vCenter SRM (Site Recovery Manager) needs to be installed. This adapter integrates VMware SRM with HP 3PAR Storage and replication software to provide a complete and integrated business continuity solution. The VMware vCenter Site Recovery Manager communicates with HP 3PAR Remote Copy Software for storage replication through the HP 3PAR SRA. The HP 3PAR SRA provides information about Remote Copy volume groups that exist in HP 3PAR Storage systems to Site Recovery Manager. SRM identifies datastores and raw device mappings (RDMs) in the Remote Copy volume group (also referred to as consistency groups). These datastores and RDMs have corresponding virtual volumes in the Remote Copy volume group and replicates between the protected site and the recovery site.

1. HP 3PAR SRA requires the following companion packages to be installed on the host before installation:
   a. VMware vCenter Site Recovery Manager 5.0.
   b. Microsoft® .NET Framework 3.5 Service Pack 1 or above
   c. Microsoft Visual C++ 2008 Redistributable Package (x86)
2. Double-click the installation executable to launch the wizard. Click Next to continue.
   a. The HP 3PAR SRA and VMware vCenter Site Recovery Manager must be installed on the same host.
3. Click I Agree to acknowledge the User License Agreement and click Next to continue.
4. Click Next to start the installation.
5. After the installation is complete, restart the VMware vCenter Site Recovery Manager service to ensure that HP 3PAR SRA is recognized by SRM. We will configure SRM to use the 3PAR SRA in the Configure the 3PAR Storage Replication Adapter section.
For more information about the plugin and where to download it for free:
https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HP_3PAR_SRM

Site Recovery Manager configuration

Once both sites have SRM installed and registered in vCenter, then the configuration of SRM can begin. To begin, start on one of the sites, and switch to the Site Recovery plugin view (Solutions and Applications → Site Recovery). The Getting Started with Site Recovery Manager screen will be the starting point for each of the following subsections. (Figure 9)

Figure 9: Getting Started with Site Recovery Manager Window

Connect the sites

The first step is to connect the two sites.

1. Select Configure Connection.
2. Enter in the Address and Port of the remote vCenter Server. Once finished click Next.
   a. You may need to accept certificate errors to proceed.
3. On the vCenter Server Authentication windows, enter in the Username and Password of the vCenter Server. Once finished click Next.
   a. You may need to accept certificate errors to proceed.
4. Several tests will now be run. If all is successful, then click Finish.
5. You will now be prompted again for the credentials to the remote site. Enter in those credentials and accept any Security Warnings that appear. Once login is successful, the second site will appear in the Sites field as in Figure 10. If a local certificate is being used, mark it to accept always.

Figure 10: Both sites are now connected

Set Up Inventory Mappings
Once the sites are connected, the Inventory Mappings should be defined. Mappings provide default locations and networks for use when placeholder virtual machines are initially created on the recovery site.

Unless you intend to configure these mappings individually for each member of the group, configure inventory mappings before creating protection groups. Inventory mappings provide a convenient way to specify how resources at the protected site are mapped to resources at the recovery site. These mappings are applied to all members of a protection group when the group is created and they can be reapplied as needed, such as when new members are added. If a protection group is created and no mappings exist, the administrator must configure each protected virtual machine individually. While SRM does not enforce an inventory mapping requirement, a virtual machine cannot be protected unless it has some form of valid inventory mappings for networks, folders, and compute resources. Inventory mappings can be created at both the protection and recovery site.

1. Select a Site from the Sites section and then click Resource Mappings.
2. Click Configure Mapping and configure a mapping to the appropriate resources for the protected virtual machines when they are recovered to the other site. For example, a cluster at Site A is protected by a cluster at Site B. Once finished, click OK.
3. Select a Site from the Sites section and then click Folder Mappings.
4. Click Configure Mapping and configure a mapping to the appropriate location in the resource mapping for the protected virtual machines when they are recovered to the other site. Once finished, click OK.
5. Select a Site from the Sites section and then click Network Mappings.
6. Click **Configure Mapping** and configure a mapping to the appropriate network to be used for the protected virtual machines when they are recovered to the other site. Once finished, click **OK**.

7. Repeat steps for the second site.

**Assign Placeholder Datastores**

Once the Resource, Folder, and Network mappings are completed, Placeholder Datastores need to be set up. A Placeholder Datastore contains information about a protected virtual machine in a protection group at the recovery site. These placeholders are added to and managed as part of the recovery site's inventory.

After determining which datastore will hold placeholders, SRM reserves a place for protected virtual machines in the recovery site's inventory. This is done by creating a subset of virtual machine files on the specified datastore at the recovery site and then using that subset to register the placeholder virtual machine with the recovery site vCenter. The presence of these placeholder virtual machines in the recovery site inventory provides a visual indication to SRM administrators that the virtual machines are protected. They also indicate to vCenter administrators that the virtual machines can be powered on and will start consuming local resources when SRM tests or runs a recovery plan.

Placeholder datastores must be established at both sites. Having placeholder datastores at both sites enables reprotection by providing a location to store the identity and inventory location of the old production machine in an empty shell of a virtual machine. This placeholder virtual machine is created during the recovery workflow when the production virtual machine is deactivated. This placeholder virtual machine can then be subsequently used and eventually removed as the recovery process is completed.

Placemarker virtual machines behave like any other member of the recovery site vCenter inventory except that they cannot be powered on. When a placeholder is created, its folder and compute resource assignments are derived from inventory mappings established at the protected site. Note that any changes made to the placeholder virtual machines in the recovery site inventory override settings established by inventory mapping. These settings are preserved during the recovery or test.

When evaluating datastores in which to establish placeholder datastores, consider the following:

- For clusters, the placeholder datastores must be visible to all hosts in the cluster.
- Placeholder datastores cannot be replicated.

To configure the placeholder datastores:

1. Select a site from the **Sites** section and then click **Placeholder Datastores**.
2. Click **Configure Placeholder Datastore**.
3. Expand the folders to find a datastore to designate as the location for placeholder datastores.
4. Select an appropriate datastore. Once finished, click **OK**.
   a. Only datastores that are valid choices are displayed. For example, replicated datastores are not suitable for holding placeholder files, so such datastores are not presented as choices.
5. Repeat for the second site.
Configure the 3PAR Storage Replication Adapter

After connectivity is established between the two sites, the HP 3PAR Storage systems need be configured as array managers in vCenter so that SRM can discover the replicated devices, compute datastore groups, and initiate storage operations.

Before configuring the array managers, ensure that the 3PAR SRAs that were installed earlier are loaded into vCenter. To do this, perform the following:

1. On the left side of the Site Recovery plugin in vCenter, select Array Managers.
2. Select the SRAs tab.
3. Ensure the HP 3PAR SRA Software version 5.0 that was installed earlier is displayed (Figure 11). If it is not, click the Rescan SRAs button.
4. Repeat for the second site.

Figure 11: HP 3PAR SRA loaded into vCenter

Now that the SRAs are properly loaded, the array managers can be configured.

1. Under the Array Managers configuration group select the Getting Started tab and click Add an Array Manager.
2. In the Array Manager Information window, enter the following:
   a. Display Name: Use any descriptive name that makes it easy to identify the storage associated with this array manager.
   b. SRA Type: Select HP 3PAR SRA Software version 5 (default).
   c. Click Next.

Now that the SRAs are properly loaded, the array managers can be configured.
3. In the **HP 3PAR Storage System Setup** window enter the following (Figure 12):
   a. **Host name or IP Address of HP 3PAR Storage System**
   b. **User name of HP 3PAR Storage System**
   c. **Password of HP 3PAR Storage System**
   d. **Click Next**.

   ![Add Array Manager - Site Recovery for 10.127.44.210](image)

   **Figure 12:** Configuring the HP 3PAR Storage System for SRM use

4. **Click Finish** once the Add Array Manager wizard is successful.
5. Repeat steps 1 through 4 for the other site and its array.

**Note**
It is only needed to configure array based replication for the vSphere Cluster and the HP 3PAR array at the same site. It is not needed to configure array based replication for a vSphere cluster at one site with the array at the other site as it is not directly attached to that storage and using its resources.

What needs to be configured in this section:
- Site A's vSphere Cluster to Site A's HP 3PAR Array
- Site B's vSphere Cluster to Site B's HP 3PAR Array
Once completed, both array managers are displayed (Figure 13).

Figure 13: Array Managers configured in SRM
Enable SRM to manage the arrays. (Figure 14)

1. Select one of the arrays from **Array Managers**
2. Click on the **Array Pairs** tab
3. Under the **Actions** column click **Enable**
4. It is only needed to click **Enable** on one of the sites, the other site is automatically enabled.

Figure 14: Array pairs enabled for use with SRM
Create a Protection Group

Protection groups provide coverage for all virtual machines in the group. For array based replication, SRM organizes datastore groups to collect all files associated with protected virtual machines. These datastore groups are then associated with protection groups. All virtual machines in a datastore group replicate their files together and failover together. It is possible to have a virtual machine with files on different datastores. In such a case, SRM combines the datastores that contain files for a single virtual machine to create a datastore group.

1. From Sites in the left pane select the Getting Started tab and click Create a Protection Group (Figure 15).

2. In the Select Site and Protection Group Type window
   a. Select the Local site from the Protection Site group box.
   b. Select Array based replication (SAN) from the Protection Group Type group box.
   c. Select the appropriate array from the list for the local site.
   a. Click Next.

Figure 15: Example of a Protected Site configuration

3. In the Select One or More Datastore Groups select the datastore(s) to be protected by SRM. All VMs under the selected datastore(s) will be protected. Click Next.

4. In the Name and Description window, enter in an appropriate Protection Group Name and Description. Click Next.

5. In the Ready to Complete window, click Finish.

6. Repeat for the second site. Once finished, a screen similar to Figure 16 will be displayed for each of the protection groups.
**Note**
If a virtual machine cannot be mapped to a folder, network, and resource pool on the recovery site, it is listed with a status of “Mapping Missing”, and a placeholder cannot be created for it and SRM will not protect that VM.

If after configuring the protection groups if there are unresolved devices with a virtual machine, those issues need to be resolved before continuing. A possible example of this would be an attached ISO that is not available at the remote site.

Figure 16: Successful protection configuration

In the **Host and Clusters** view in vCenter for each site, placeholders are now visible for each of the protected VMs at that site. (Figure 17)
Figure 17: Placeholder for SRM protected virtual machine at the recovery site.

Create a recovery plan

In order to recover a protection group in the case of a planned or unplanned event, a recovery plan needs to be established that lays out how virtual machines are recovered. A basic recovery plan includes a number of prescribed steps that use default values to control how virtual machines in a protection group are recovered at the recovery site. Users can customize the plan to meet their needs for their environments. Recovery plans are different from protection groups in that recovery plans indicate how virtual machines in one or more protection groups are restored at the recovery site.

1. From Sites in the left pane select the Getting Started tab and click Create a Recovery Plan.
2. Select the Local site from the Recovery Site group box and click Next.
3. In the Select Protected Groups window, select the Protection Group(s) to include in the recovery plan. Click Next.
4. In the Test Networks window, select the Recovery Network for the VMs. Click Next.
5. In the Name and Description window, enter in an appropriate Recovery Plan Name and Description. Click Next.
6. In the Ready to Complete window, click Finish.
7. Repeat steps 1 through 6 for the other protection groups. Once finished, there should be a list of recovery plan(s) with a Plan Status of Ready (Figure 18).
VMware SRM is now configured and should now be tested before performing a planned or unplanned recovery to ensure that everything was configured properly.

**Testing recovery plans**

Once VMware SRM configuration is complete, testing of the recovery plan can be initiated at any time without impacting the virtual machines at the protected site.

When a recovery plan is tested, a test network and a temporary snapshot of replicated data at the recovery site is used. No operations are disrupted at the protected site.

Testing a recovery plan runs all the steps in the plan with the exception of powering down virtual machines at the protected site and forcing devices at the recovery site to assume ownership of replicated data. If the plan requests suspension of local virtual machines at the recovery site, they are suspended during the test. A test makes no other changes to the production environment at either site.
**Prerequisites**

Before proceeding with the testing, as well as performing any planned and unplanned failover events, you need to ensure that your HP 3PAR arrays are running one of the following versions of the InForm OS.

- 2.3.1 MU5 with patch P32 or greater
- 3.1.1 MU1 with patch P13 or greater

Failing to meet this requirement will cause testing and failover actions to fail with failure message “Invalid Metadata” when trying to create a writeable snapshot as part of a recovery action. If you are unsure of the version of your HP 3PAR Storage system or need the InForm OS upgraded, contact your HP Services representative or your HP partner (hp.com/large/contact/enterprise/index.html) for assistance.

The appropriate licensing for the HP 3PAR arrays is also required. Please contact your HP Sales Representative if you have any questions or are missing the required licenses listed below on your HP 3PAR arrays. The exact licenses needed depend on the array and disk configurations. Refer to the HP 3PAR Software Products QuickSpecs (http://h18000.www1.hp.com/products/quickspecs/13964_na/13964_na.html) for more information.

- HP 3PAR Remote Copy Software
- HP 3PAR Virtual Copy Software
- HP 3PAR Recovery Manager Software for VMware vSphere

**Initiating a test**

In the vSphere Client click **Recovery Plans** in the left pane, click a **Recovery Plan** and then click **Test**.

1. In the **Testing Confirmation** window, determine whether to enable the **Replicate recent changes to recovery site** option when the plan runs. Enabling this option ensures the recovery site has the latest information, but the synchronization may take additional time. Click **Next**.
2. Click **Start** on the confirmation window.
3. Progress and completion of the recovery test can be viewed by looking at the **Recovery Steps** tab. (Figure 19)
Once the test has completed successfully, click **Cleanup** to remove the test environment and reset the plan to the Ready state.

**Recovery and reprotect**

After ensuring that all the recovery plans test successfully, the Recovery and Reprotect actions can be leveraged when needed for an actual failover for a planned migration or as part of disaster recovery. During failover, Site Recovery Manager shuts down virtual machines, promotes the replicated copy of storage, attaches it to the ESX servers at the recovery site, brings up the virtual machines, and generates reports about the recovery process.

All that is required to begin a recovery in the event of a real disaster is to click the Recovery button. Although Site Recovery Manager provides notification when it loses contact with the primary site, the administrator must initiate recovery. The administrator declares that a disaster requiring recovery has occurred, and then Site Recovery Manager takes over and executes its recovery process.

1. Click **Recovery Plans** in the left pane, select a recovery plan and click **Recovery**.
2. Confirm the request to initiate recovery.
3. Since this is a **Planned Migration**, select that option from the **Recovery Type** group box, and click **Next**.
4. Click **Start** on the confirmation window.
5. Progress and completion of the recovery test can be viewed by looking at the **Recovery Steps** tab.
Once finished, the **Recovery Complete** message will be displayed similar to Figure 20. The VM from Site B is now running on Site A (Figure 21).

Figure 20: Successful site recovery

![Successful site recovery](image1.png)

Figure 21: VM from site B running on site A

![VM running on site A](image2.png)

Now that the primary site has been migrated to the recovery site it is no longer protected against failure. To reestablish the protection of the VMs at the new site, the "Reprotect" action must be executed. Reprotection results in array-based SRM protection groups and recovery plans being reconfigured to work in the opposite direction. This provides the option of failing virtual machines back to the original site, if desired. Note that the reprotect workflows are designed for use when the physical infrastructure at both sites is intact. If the failover was unplanned and physical site and equipment loss has occurred (specifically the replicated storage layer) at one of the sites, then the reprotect workflows cannot be utilized.
Reprotecting is only applicable in cases where array based protection has been established, a failover has been completed, and there is a need to re-establish protection. If an unplanned failover has occurred, a planned failover must be completed before attempting reprotection. This action is needed to ensure the original protected site has been restored, and a planned failover is completed to ensure both sites are fully aware of the current status. If errors occur during such an attempted planned failover, the errors must be resolved, and the failover re-run until the failover succeeds. Running a planned migration after a failover will NOT affect the running of the recovered VM’s but is needed to allow SRM to reset certain aspects of the configuration in readiness for reproprotect.

---

**Note**
Running a planned migration after a failover will NOT affect the running of the recovered VM’s but is needed to allow SRM to reset certain aspects of the configuration in readiness for reproprotect.

---

To initiate a reproprotect of a site:

1. Click **Recovery Plans** in the left pane, click the **Recovery Plan** that was executed previously, and then click **Reprotect**.
2. Select **I understand that this operation cannot be undone** and click **Next**.
3. Click **Start** on the confirmation window.
4. Once complete, the recovery site’s plan will be modified to work in the reverse direction and set back to normal. Now both VMs are on the same site and protected.

**Failback**

To fail Site B’s VM back to Site B, just rerun the same recovery plan, and then reprotect again on Site B to re-establish protection.
In the following scenario, we will test a power failure at Site A. A power failure at Site A means that all communication with Site A over the Ethernet network will be lost (Figure 23). Once Site B sees that it has lost communication with Site A, a message on Site B (Figure 24) will be displayed indicating it has lost communication with Site A.
Figure 23: Failure at Site A

Figure 24: Lost of connectivity to Site A
Just as in the Recovery and reprotect section, the same steps will be performed to recover Site A with a few differences. Since this is an unplanned failure, select Disaster Recovery in the Recovery Type group box (Figure 25). By selecting Disaster Recovery, the recovery actions will attempt to talk to the Protected Site to replicate any recent changes, however if it cannot it will continue if there are errors. In a planned migration, errors would stop the operation.

Figure 25: Executing a Recovery Plan in a Disaster Recovery scenario

If a Disaster Recovery is performed and the Recovery Site cannot talk to the Protected Site during a failover, a message dialog will be displayed (Figure 26) and the Recovery action will have to be run again once the sites are reconnected to ensure the VMs at the failed site have been shut down and placeholders are created for them.

Figure 26: Disaster Recovery warning that SRM could not shut down the original protected VMs
The recovery completed successfully (Figure 27) and the warning shown in Figure 26 was displayed since communication between Site A and Site B was lost. Site A’s VM is now running on Site B’s ESXi 5 cluster (Figure 28).

**Figure 27: Failure – Site A Recovery Steps**

<table>
<thead>
<tr>
<th>Recovery Step</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Pre-synchronize Storage</td>
<td>Error: Failed to sync data on replica devices. The connection to the remote server is down.</td>
</tr>
<tr>
<td>2. Shutdown VMs at Protected Site</td>
<td>Error: The connection to the remote server is down.</td>
</tr>
<tr>
<td>3. Resume VMs Suspended by Previous Recovery</td>
<td></td>
</tr>
<tr>
<td>4. Restore hosts from standby</td>
<td>Success</td>
</tr>
<tr>
<td>5. Prepare Protected Site VMs for Migration</td>
<td>Error: The connection to the remote server is down. The connection to the remote server is down.</td>
</tr>
<tr>
<td>6. Synchronize Storage</td>
<td>Error: Failed to sync data on replica devices. The connection to the remote server is down.</td>
</tr>
<tr>
<td>7. Suspend non-critical VMs at Recovery Site</td>
<td></td>
</tr>
<tr>
<td>8. Change Recovery Site Storage to Writable</td>
<td>Success</td>
</tr>
<tr>
<td>9. Power On Priority 1 VMs</td>
<td></td>
</tr>
<tr>
<td>10. Power On Priority 2 VMs</td>
<td></td>
</tr>
<tr>
<td>11. Power On Priority 3 VMs</td>
<td>Success</td>
</tr>
<tr>
<td>12. Power On Priority 4 VMs</td>
<td></td>
</tr>
<tr>
<td>13. Power On Priority 5 VMs</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 28: Failure – Site A VM running on Site B’s ESXi cluster**

Upon reestablishment of site connectivity, VMware SRM alerts the user that the **Recovery** action needs to be re-run in order to complete the recovery action (Figure 29).

**Figure 29: Failure - Recovery required to complete failover**

Upon completion of the recovery, all the steps in the **Recovery Steps** will be marked as **Already Done** or **Success** and all the VMs at Site A are shut down and place holders are created for them. The option to **Reprotect** the VMs on Site B is now available and should immediately be run to protect the VMs and is needed before the VMs can be recovered back onto Site A.
Implementing a proof-of-concept

As a matter of best practice for all deployments, HP recommends implementing a proof-of-concept using a test environment that matches the planned production environment as closely as possible. In this way, appropriate configuration and solution deployment can be obtained. For help with a proof-of-concept, contact an HP Services representative or your HP partner (hp.com/large/contact/enterprise/index.html).

SPC-1 benchmark

SPC-1 benchmark is designed for business-critical applications that process large and multiple complex transactions and workloads such as VMware vSphere 5.

The HP 3PAR P10000 V800, T800 and F400 Storage systems have set individual performance records by achieving SPC-1 benchmark results of 450,212 IOPS for the V800; 224,989 IOPS for the T800; and 93,050 IOPS for the F400. The storage performance council website may be referred to for further details on these records and tests performed by SPC at storageperformance.org/results/benchmark_results_spc1.

HP 3PAR Storage offers unique mixed workload support so that transaction and throughput-intensive workloads run without contention on the same storage resources, alleviating performance concerns and dramatically cutting traditional array costs. HP 3PAR Storage is massively parallel and autonomically load balanced, making simplified storage administration, high performance and consolidation easily achievable by any organization. HP 3PAR Storage is suitable for a mission-critical virtualized environments like VMware that relies on top storage array performance.

Table 1. HP 3PAR SPC-1 performance

<table>
<thead>
<tr>
<th>Tested storage configuration</th>
<th>HP 3PAR P10000 V800</th>
<th>HP 3PAR T800</th>
<th>HP 3PAR F400</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPC-1 IOPS</td>
<td>450,212.66</td>
<td>224,989.65</td>
<td>93,050.06</td>
</tr>
<tr>
<td>Total ASU* capacity (GBs)</td>
<td>230,400GB</td>
<td>77,824GB</td>
<td>27,046GB</td>
</tr>
<tr>
<td>SPC-1 Price/performance $/SPC-1 IOPS</td>
<td>$6.59</td>
<td>$9.30</td>
<td>$5.89</td>
</tr>
<tr>
<td>Data protection level</td>
<td>Mirroring</td>
<td>Mirroring</td>
<td>Mirroring</td>
</tr>
<tr>
<td>Identifier</td>
<td>A00109</td>
<td>A00069</td>
<td>A00079</td>
</tr>
<tr>
<td>Version</td>
<td>1.12</td>
<td>1.10.1</td>
<td>1.10.1</td>
</tr>
</tbody>
</table>

Summary

Coupling the simplicity and efficiency of HP 3PAR Remote Copy with HP 3PAR Replication Adapter for VMware vCenter Site Recovery Manager enables HP 3PAR customers to easily implement VMware vCenter Site Recovery Manager for end-to-end management of array-based replication and failover of virtual machines. The combination of HP 3PAR Remote Copy and VMware vCenter Site Recovery Manager lets customers build resilient utility computing infrastructures, protect applications at a lower cost, and recover data more quickly and efficiently compared to traditional disaster recovery offerings.

Not only does leveraging HP 3PAR Storage enable seamless integration with VMware SRM for simplified disaster recovery, but is also enables organizations using VMware vSphere with HP 3PAR several other key benefits. Using HP 3PAR Storage with VMware vSphere storage enables its users to double virtual machine density on physical servers, placing twice as many VMs on physical servers as with traditional storage platforms. Also the tight integration of VMware vCenter Server and the HP 3PAR Management Software Plug-In for VMware vCenter allows administrators to monitor and manage HP 3PAR Storage volumes to create point-in-time, VM-and application-aware, disk-based snapshots from within the vSphere console. Lastly with HP 3PAR Thin Persistence, as the ESXi host writes zeros to the VMDK file, the zeros are detected in-line by the ASIC, and no space is allocated for the VMDK in the thin provisioned...
volume. Also, with Thin Persistence, when a VM is deleted or moved to another data store, that now unallocated storage is released back to the array rather than keeping it assigned to the LUN.

For more detailed information on the HP 3PAR Management Software Plug-In for VMware vCenter or HP 3PAR Recovery Manager Software for VMware vSphere, see hp.com/go/3PAR.

For more information
HP 3PAR Storage Family, hp.com/go/3PAR
HP 3PAR P10000 Storage Systems, hp.com/go/P10000
HP 3PAR T-Class Storage Systems, hp.com/storage/3PAR-tclass
HP 3PAR F-Class Storage Systems, hp.com/storage/3PAR-fclass
HP Storage, hp.com/go/storage
VMware vCenter Site Recovery Manager Documentation, vmware.com/products/site-recovery-manager/resource.html

To help us improve our documents, please provide feedback at hp.com/solutions/feedback.