



# Disaster Recovery Solutions with HP SVSP and VMware SRM

Maximizing the benefits of server and storage virtualization in a disaster recovery (DR) environment



## Table of contents

Introduction .....	2
How HP SVSP Virtualization enhances server virtualization .....	2
HP SVSP for disaster recovery .....	3
VMware SRM overview .....	4
Using HP SVSP and VMware SRM for disaster recovery .....	5
Prerequisites .....	6
Test configuration .....	6
SVSP configuration .....	7
Configure SVSP Domains .....	7
Configure asynchronous mirroring .....	7
Site configuration .....	8
Configure VMware Datastores .....	8
Installing Storage replication adapter (SRA) .....	9
Installing Site Recovery Manager .....	10
Installing the SRM plug-in .....	14
Configuring the SRM Plug-in .....	16
Pairing the Primary Site and the Secondary Site .....	16
Preparing for disaster recovery .....	19
Configuring storage array managers .....	19
Creating an Inventory Mapping .....	19
Creating a protection group .....	20
Creating a Recovery Plan .....	20
Testing the Disaster Recovery Plan .....	21
Performing the recovery failover .....	21
Performing a failback from the recovery site .....	22
Protected site was offline for a while and came back .....	22
Protected site was destroyed and completely rebuilt .....	22
Conclusion .....	22
For more information .....	23

## Introduction

A Cost-Effective Disaster Recovery solution is a critical need for business of all sizes: It is essential to protect mission-critical data from storage, site, or regional disasters. Furthermore, the rapid spread of server-based virtualization suggests that disaster recovery (DR) will increasingly take place in the context of virtualized environments. As a result, storage products must deliver cost-effective DR solutions that integrate with VMware. This paper describes the comprehensive and cost-effective DR solution that the HP StorageWorks SAN Virtualization Services Platform (SVSP) delivers for virtualized environments.

This paper begins with an overview of HP StorageWorks SVSP and the value it brings to virtualized server environments. Next, it provides an overview of VMware's Site Recovery Manager (SRM). Finally, it presents a Disaster Recovery solution using HP SVSP and VMware SRM to provide automatic failover of servers, virtual machines, and their underlying storage.

---

### Note

The SRM adapter technology described in this paper becomes available with SVSP 3.0, which is expected to release by early 2010.

---

## How HP SVSP Virtualization enhances server virtualization

Virtualization as a technology can offer tremendous benefits. It can also be deployed in several locations. For example, server virtualization can leverage the power behind a few large physical servers by creating hundreds of virtual machines. Storage virtualization can bring the original promise of SANs to reality, by creating large storage pools and then virtually allocating capacity as needed. By combining these two technologies, however, users realize even greater value than what they would by using them individually. To virtualize the data center, these two technologies are required.

HP StorageWorks SVSP provides the flexibility to allocate capacity rapidly and the ability to allocate large numbers of volumes—as needed. As it is very easy to add and remove virtual machines and applications in a virtual environment, the environment becomes very dynamic. In other words, virtual machines are created, used, and then reallocated or removed as needed. This provides tremendous application flexibility. However, in this highly dynamic environment, it is also important that the storage be provisioned and reallocated after use with the same mobility and simplicity as the virtual servers. Storage virtualization enables this flexibility.

Over-provisioning is another significant challenge for virtual environments. The typical practice is to over-provision storage for the physical servers, which drives down utilization rates and drives up capital expenses. The challenge increases significantly with the sprawl of virtual machines that follows the initial implementation of server virtualization. The SVSP provides a comprehensive set of data services that includes among others thin provisioning. With SVSP thin provisioning, virtual machines are allocated only the storage capacity needed in a just-in-time fashion (as opposed to the typical over-provisioning) significantly optimizing the deployment of storage and reducing near-term capital investments.

The HP SVSP also provides Point-in-Time (PiT) snapshots, which enable the creation of multiple snapshot copies that can be assigned to multiple host machines. With these capabilities, it is possible to create powerful application test environments by just making snapshot copies of production data (in seconds) and then allocating them to virtual machines that are used exclusively for testing. In addition, the HP SVSP snapshot function provides the capability to create snapshots of snapshots, so that, testers cannot only be assigned real "live" data within seconds, but can also take snapshots of the virtual disks throughout the testing process. All of these features reduce the time needed to setup and teardown testing and increase the efficiency of testing considerably.

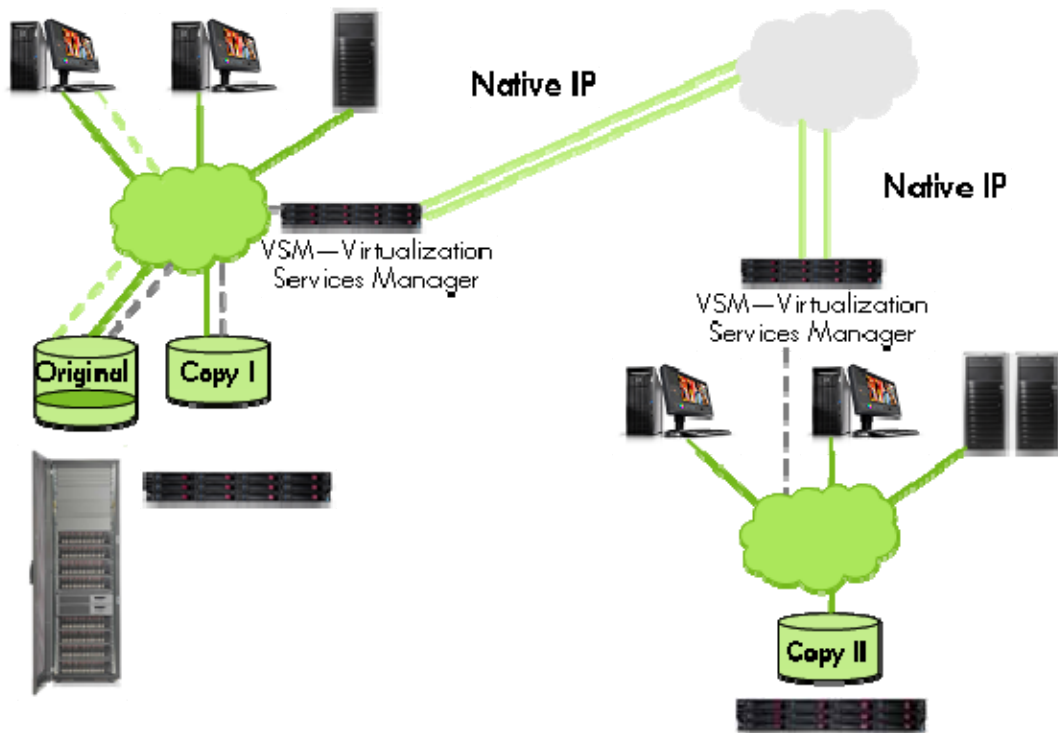
With the HP StorageWorks SVSP snapshot function, it is also possible to enhance and simplify backup operations, by avoiding the need to install backup agents on every virtual machine. The backup can be done by creating snapshot copies for every virtual server and then assigning the copies to a virtual machine with the dedicated role of backup server. In this manner, the backup server is the only physical or virtual machine that needs to have the backup software installed. When dealing with hundreds of virtual servers, this can reduce the cost of backup licenses considerably.

## HP SVSP for disaster recovery

The remote Asynchronous Mirroring capabilities in the SVSP Continuous Access option can facilitate service resumption after a storage, site, or regional disaster. The HP SVSP Business Copy feature keeps the system online and fully available during backup without any impact, allowing an entire application to restore in minutes. Together, these SVSP services help firms improve productivity through high up-time. Centralized management of recovery operations reduces administrative tasks and errors while lowering management costs.

In an SVSP Continuous Access deployment (see Figure 1), servers are present across two different SVSP domains at two different sites. Each site has its own application servers and storage, and each site is also a complete SVSP domain (that is, each site has its own pair of Virtualization Services Managers and Data Path Modules). The asynchronous mirroring capabilities of SVSP are used to replicate the changed data across the domains in a bandwidth-efficient way, across existing IP connections. (Note the contrast to alternative solutions that copy every write and often require dedicated and costly high-bandwidth links.)

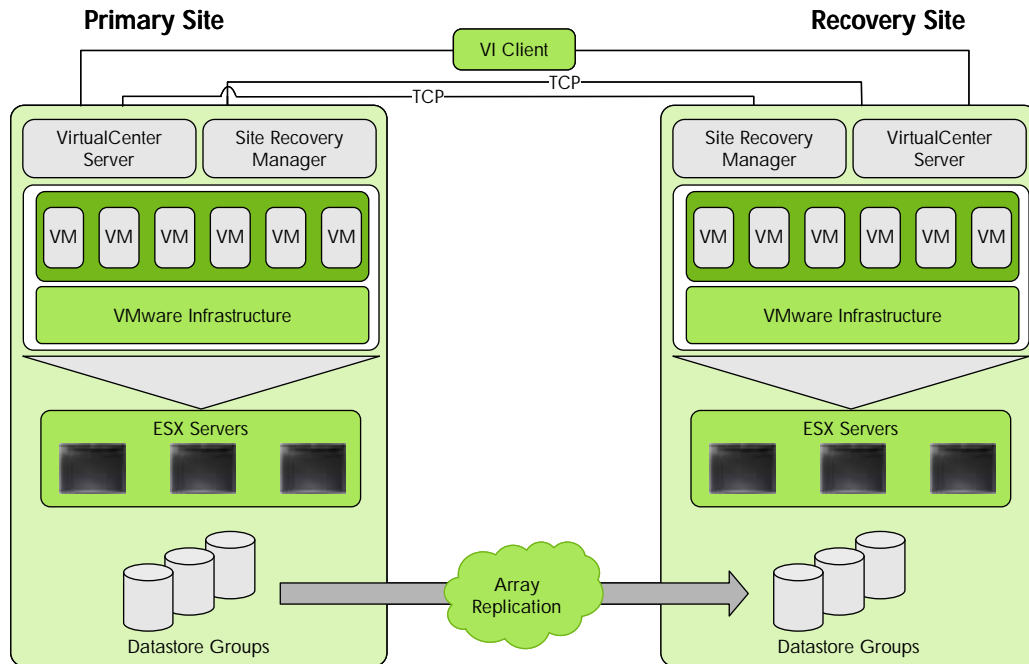
Figure 1: HP SVSP Asynchronous Mirroring



## VMware SRM overview

Site Recovery Manager (SRM) is a disaster recovery workflow product that automates setup, failover, and testing of disaster recovery plans. SRM relies on storage-array-based block replication, which is provided by the storage array vendor. SRM uses storage replication adapters (SRAs), which are small applications that are provided by the hardware storage array vendor in this case SVSP. SRAs control the replication of data from the primary site to the recovery site. The following Figure 2 shows the architecture of the VMware SRM product.

Figure 2: SRM Architecture

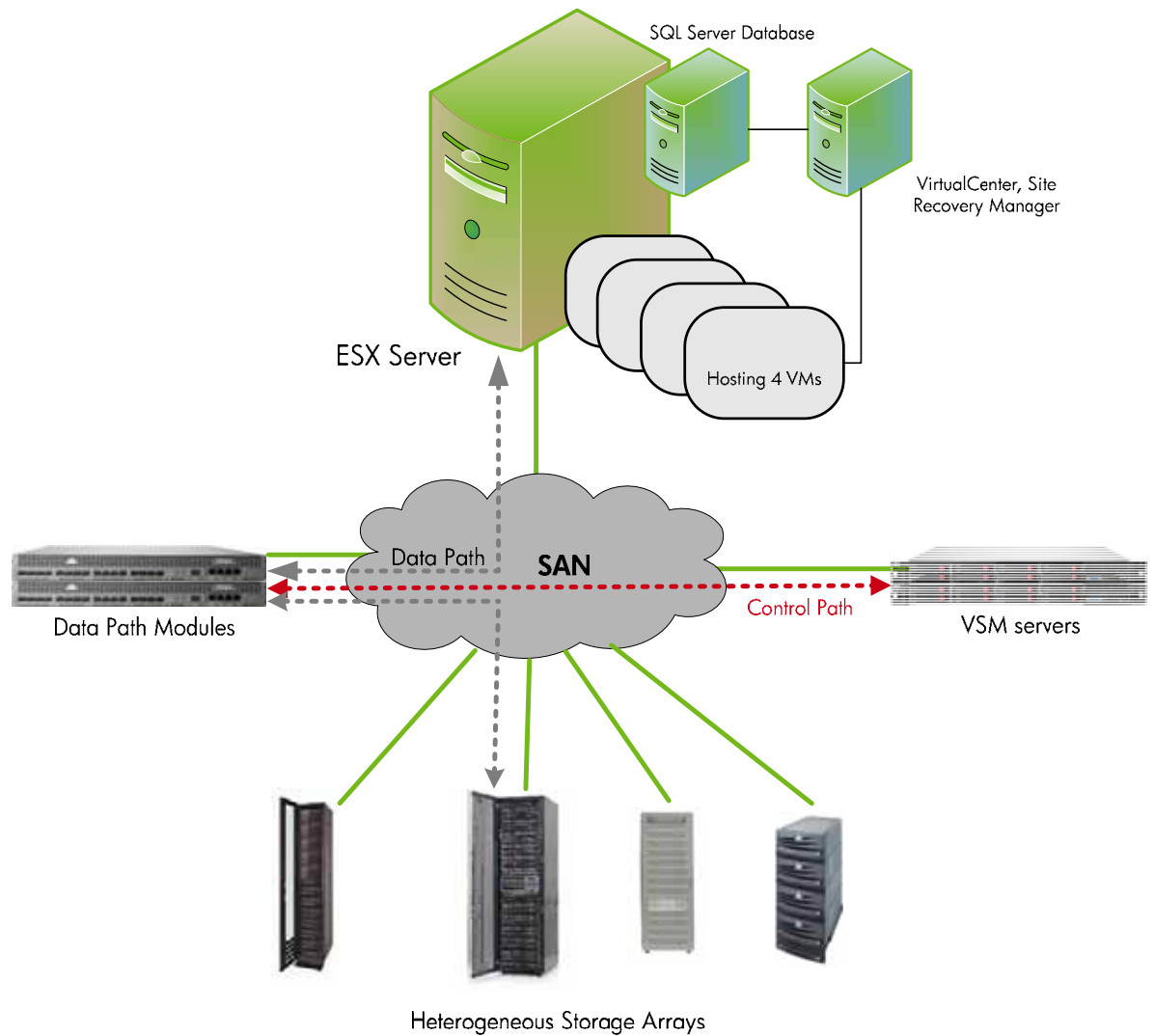


## Using HP SVSP and VMware SRM for disaster recovery

The asynchronous mirroring capabilities of the HP SVSP allow virtual disk replication over long distances in a bandwidth-efficient way, using existing IP connections.

VMware vCenter Site Recovery Manager controls and orchestrates failover and test operations on the array through a software component called the Storage Replication Adapter (SRA).

Figure 3: HP SVSP with VMware SRM



## Prerequisites

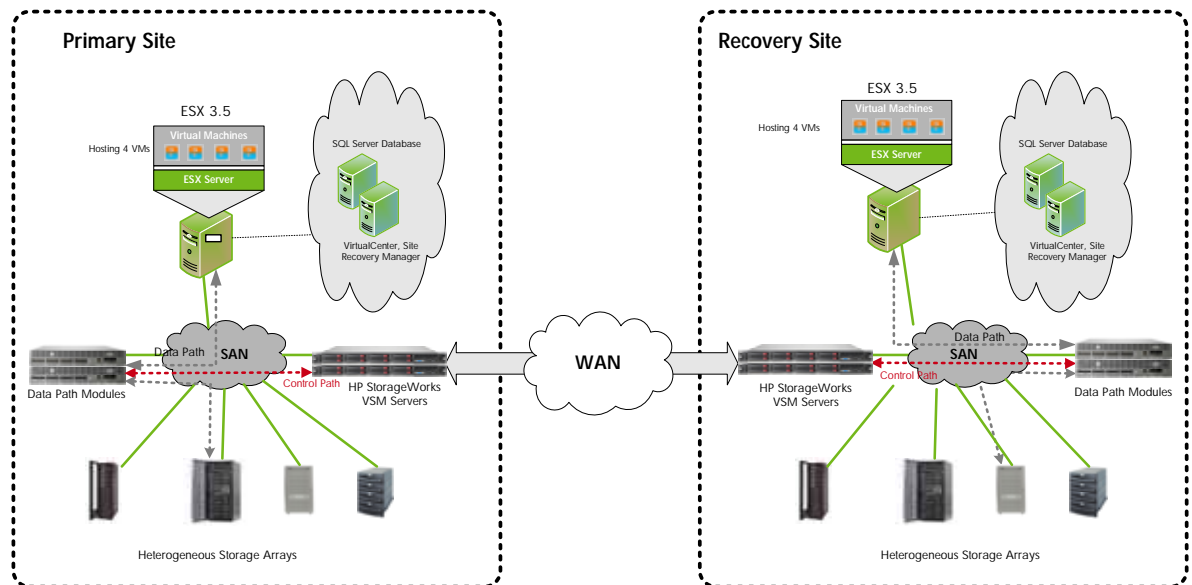
The following tasks must be completed before implementing the HP SVSP and SRM for disaster recovery:

- Install and configure two VirtualCenter servers and SRM servers (either physical machines or virtual machines), one on each site, as SRM requires two distinct virtual infrastructure sites.
- Configure the databases at each site to support VirtualCenter and SRM. Refer to VMware's guidelines on which databases are supported.
- Install the SRM server and plug-in at both sites. Refer to the VMware SRM Installation Guide.
- Install and configure two SVSP domains, one on each site, with appropriate licenses including for asynchronous mirroring. For more details, refer to the HP SVSP user guide. (See the [For more information section](#) of this paper to learn how to find the HP SVSP User Guide document.)
- Establish IP connectivity between the two SVSP domains (VSM to VSM). For more details, refer to the HP SVSP user guide. (Analysis of IP bandwidth requirements and the time required to copy data between the two sites are beyond the scope of this paper.)
- Set the asynchronous mirroring on primary and secondary sites using the Continuous Access feature of HP SVSP.
- Install the current VSM software and DPM image versions on each domain.

## Test configuration

The following diagram shows the test configuration used for this document:

Figure 4: Test Configuration



Make sure that you cluster the database servers to maintain and protect the data repository (VirtualCenter and SRM databases).

## SVSP configuration

To use HP SVSP and SRM for disaster recovery, make sure to configure the SVSP domain on each site and mirrored volumes in the recovery site SVSP domain (as described below).

---

### Note

In all subsequent sections, this paper presents summaries of SVSP operations. For detailed instructions and command sequences, please refer to the "For More Information" section of this paper to find the SVSP User Guide and SVSP Admin Guide documents.

---

### Configure SVSP Domains

Configuring the SVSP domain includes the following:

1. Install and configure the SVSP domains with two VSM servers and at least one DPM group on each site.
2. Create Storage Pools  
The SVSP GUI provides the user with the information about the LUNs presented by the different storage systems as back-end LUNs. Create Storage pools from the back-end LUNs exposed by storage systems. This step must be done on both SVSP domains, protected and recovery site.
3. Create Virtual disks  
Create required virtual disks from that storage pools on each site. Refer to the SVSP User guide for instructions on how to create the virtual disks from the storage pool.
4. Assign Virtual disks to VMware ESX servers  
Assign the created virtual disks with the same LUN number to all ESX servers that are a part of the VMware clusters or to standalone ESX servers that are not in the VMware cluster. This step can be done only on the source SVSP domain (also known the protected site). Virtual disks can also be created on the destination SVSP domain serving other hosts residing on the destination/remote site. Refer the HP SVSP User guide for instructions on how to assign the virtual disks to hosts.
5. Establish iSCSI connection between the VSM servers on both SVSP domains using the Microsoft iSCSI utility that was installed on the VSM servers as part of the VSM software install.

Refer to the SVSP User guide and SVSP Admin Guide for more details.

### Configure asynchronous mirroring

Asynchronous mirroring is useful for maintaining an offsite backup of virtual disks for disaster recovery. In asynchronous mirroring, the host application writes data to the original virtual disk, while the VSM servers copy the data in the background to mirrored virtual disks on a recovery site.

Configuration of the SVSP asynchronous mirroring includes the following:

- For every virtual disk that will participate in the VMware SRM protected group, an asynchronous mirror group must be created for the source virtual disk with one task for the destination.
- The number of PiTs and the replication interval must be configured the same for all replicated virtual disks that will be part of the VMware SRM protected group and the SVSP virtual disk group.

Refer to the HP CV SVSP User guide and the SVSP Admin guide for more details on how to create asynchronous mirror group and task.

## Site configuration

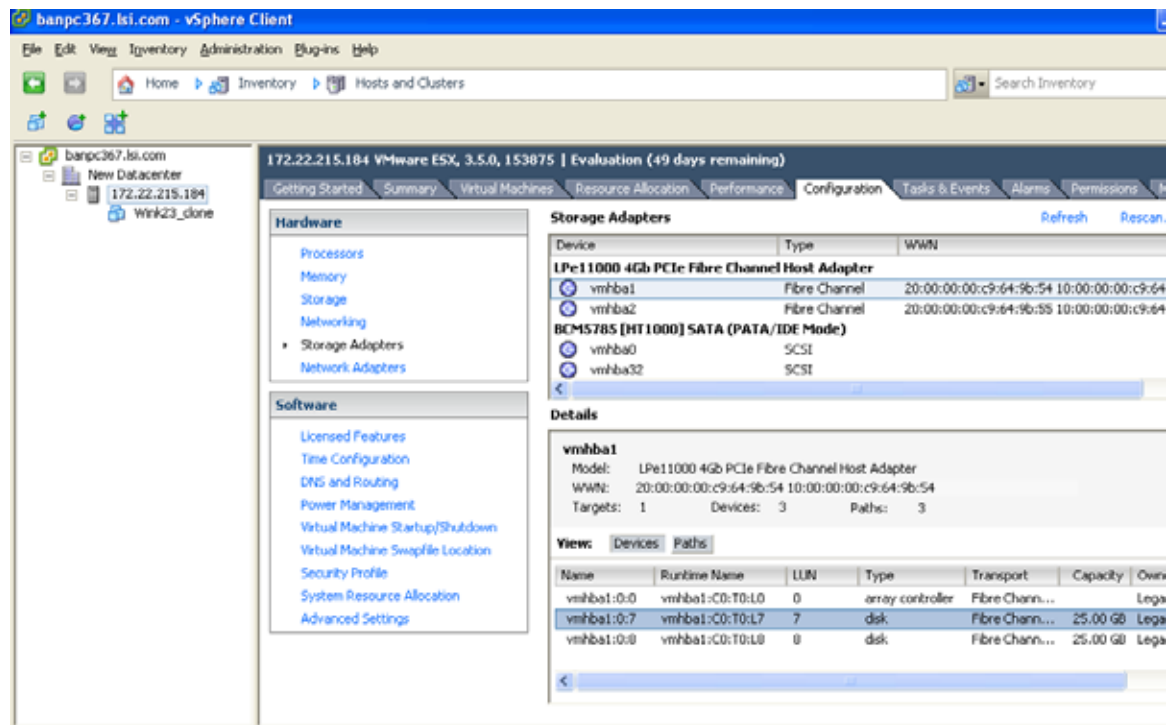
The following steps must be completed in the protected and recovery sites to perform Disaster Recovery Operation.

### Configure VMware Datastores

Configuring the VMware Datastores using vCenter GUI includes the following:

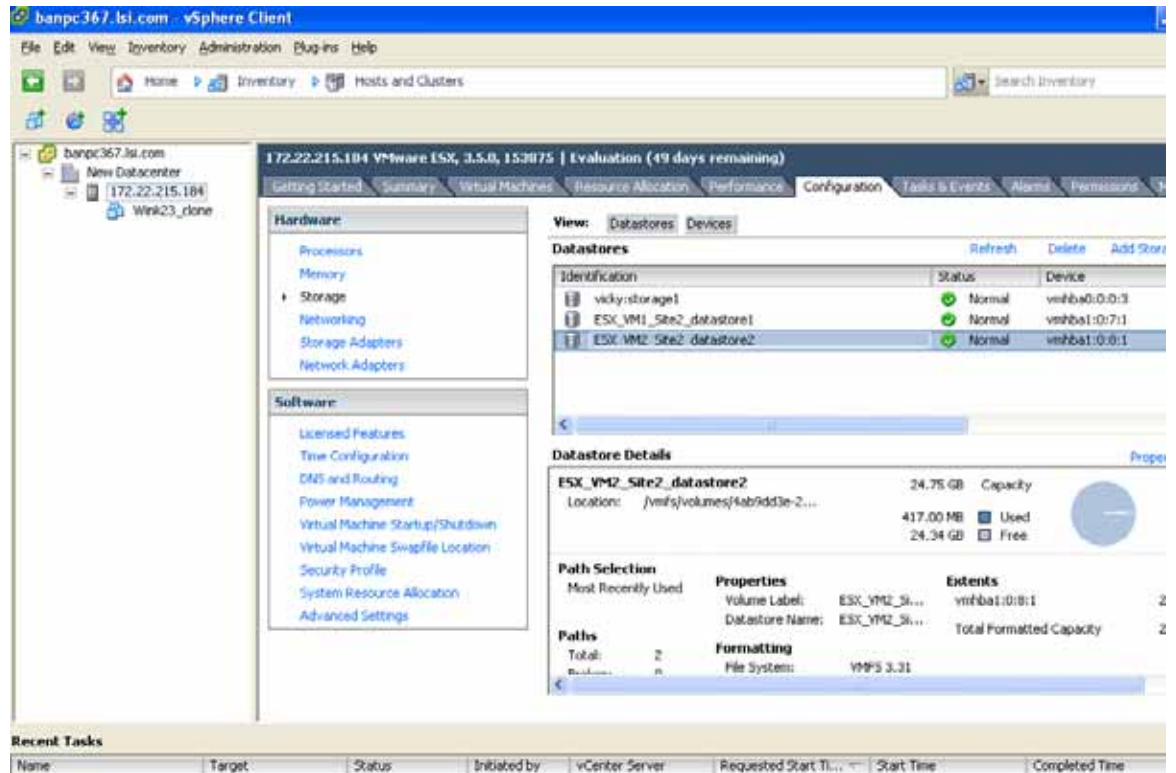
1. After assigning the virtual disks to ESX server in the protected site, rescan the storage to discover the virtual disks exposed by SVSP.

Figure 5: vCenter GUI showing discovered LUNs



2. Use Add Storage to create the datastores in the discovered disks.

Figure 6: Created DATASTORES on top of virtual disks



3. Create virtual machines and save them on the DATASTORE residing on SVSP virtual disks.

For more details on how to create DATASTORE, please refer to the VMware SAN user guide.

### Installing Storage replication adapter (SRA)

SRA is an interface between storage and SRM. The HP SVSP SRA enables SRM communication with SVSP features, specifically replication and snapshots. SVSP SRA lets SRM support many different storage arrays without embedding specific storage array knowledge into the SRM binary file. The SVSP SRA contains scripts and a command line interface (CLI).

To install SVSP SRA, perform the following steps.

1. Download the SRM main binary file and the SRA for SVSP.
2. Install the SRM server plug-in and then install the SRA. SRA installation does not require a lot of configuration. Detailed SVSP instructions for installing SRAs are included in a README file that comes with the SVSP SRA.

## Installing Site Recovery Manager

This section documents the installation wizard for Site Recovery Manager (SRM). SRM must be installed at both the protected site and the recovery site.

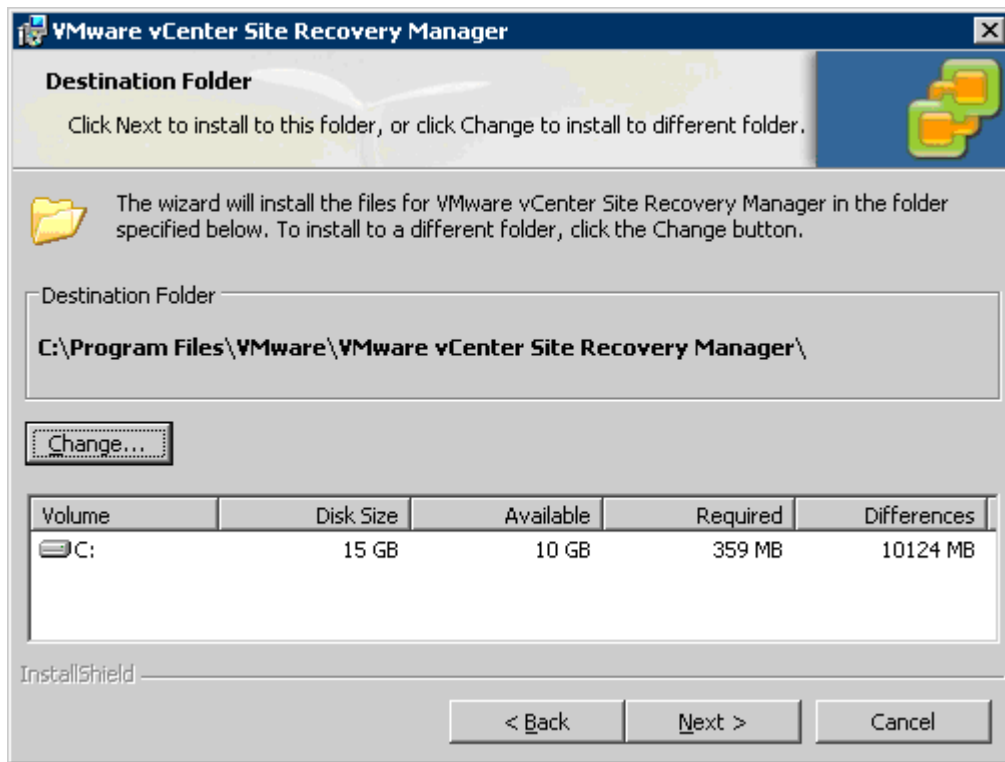
Before installing SRM, you must complete all the requirements listed below:

- **An installed vCenter Server:** SRM and vCenter reside on the same host. You need the vCenter address (IP address), username, and password for both the protected and recovery site.
- **A SQL Server database:** You will need a client database DSN, database username, password, connection count, and maximum connections.

To install SRM, perform the following steps.

1. Click the `srminstall.exe` icon to begin the installation.
2. Click Next on the "Welcome to the installation" wizard screen.
3. At the **License Agreement** screen, click **I accept the terms in the license agreement** and then click **Next**. To print the License Agreement, click **Print**. At the **Destination Folder** screen, accept the default folder, and click **Next** to continue.

Figure 7: vCenter SRM Destination Folder



4. At the VMware VirtualCenter Server screen, enter:
    - **VirtualCenter Address:** Enter the IP address of the VirtualCenter Server.
    - **VirtualCenter Port:** You can accept the default or enter another port.
    - **VirtualCenter Username:** Enter your user ID for VirtualCenter Server.
    - **VirtualCenter Password:** Enter the password for the Username.
- 

Figure 8: vCenter Server information

VMware vCenter Site Recovery Manager

**VMware vCenter Server**

Enter vCenter Server information for VMware vCenter Site Recovery Manager registration.

vCenter Server Credentials

Registration requires administrator credentials in order to access vCenter Server.

vCenter Server Address: 172.28.9.47

vCenter Server Port: 80

vCenter Server Username: administrator

vCenter Server Password: \*\*\*\*\*

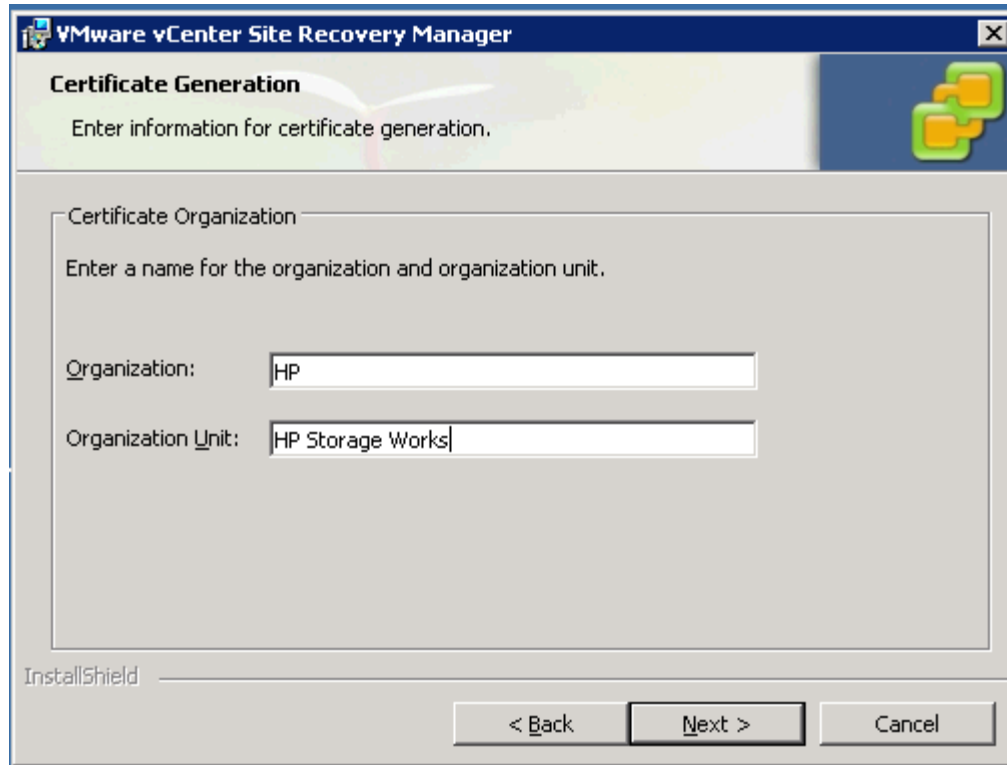
InstallShield

< Back   Next >   Cancel

---

5. Click **Next**.
6. At the **Certificate Type Selection** screen, select **Automatically generate certificate** and then click **Next**.
7. At the **Certificate Generation** screen, enter your organization and organization unit. This is typically your company and your group within the company.

Figure 9: Organization Information for certificate generation



8. At the VMware Site Recovery Manager Extension screen, enter the following:
  - **Local Site Name:** Enter a unique name for this installation of SRM. Each installation of SRM at one site must have a unique identifier.
  - **Administrator email:** Enter the email ID of the person or group who will monitor SRM and respond to any alerts or notifications.
  - **Additional email:** Enter the email ID of the person or group who should also receive any alerts or notifications.
  - **Local Host:** Enter the name of the local host or the IP address.
  - **Listener Ports:** Enter the ports on which you want to listen for SOAP and SNMP messages over the network.
  - **API Listener Ports:** Enter the ports on which you want to listen for SOAP and SNMP messages from the SRM API. For more information, see [\(link to API section\)](#).

Figure 10: Registering the VMware vCenter Site Recovery Manager extension

**VMware vCenter Site Recovery Manager Extension**

Enter info to register the VMware vCenter Site Recovery Manager extension.

Enter a name for this site's installation. It must be unique across all VMware vCenter Site Recovery Manager installations. You must also enter at least one e-mail address for administrators to receive notifications. Additionally, select the address for the local host and port numbers to use for server network traffic.

Local Site Name:

Administrator E-mail:

Additional E-mail:

Local Host:

Listener Ports: SOAP Port:  HTTP Port:

API Listener Port: SOAP Port:

InstallShield

< Back    Next >    Cancel

Click **Next** to continue.

9. At the **Database Configuration** screen, enter:

- a. **Database Client:** Click the arrow on the right of the field and select the database client for your site.
- b. **Data Source Name:** Enter the data source name (DSN) you will use for this installation of SRM. Click ODBC DSN Setup to create a DSN for this installation. Use a centralized database for the SRM protected (point to the protected database srmP...) and recovery (point to the recovery database srmS...) sites.
- c. **Username:** Enter your user ID for the database.
- d. **Password:** Enter the password for the Username.
- e. **Connection Count:** Enter the initial connection pool size you want opened to the database.
- f. **Max Connections:** Enter the maximum number of connections you want to open to the database at one time.

10. Click **Next** to continue.

11. At the **Ready to Install the Program** screen, click **Install** to install SRM.

12. After installation completes, you are prompted with a warning about installing the security certificate. Click **Yes** to install the certificate. Now, SRM is installed.

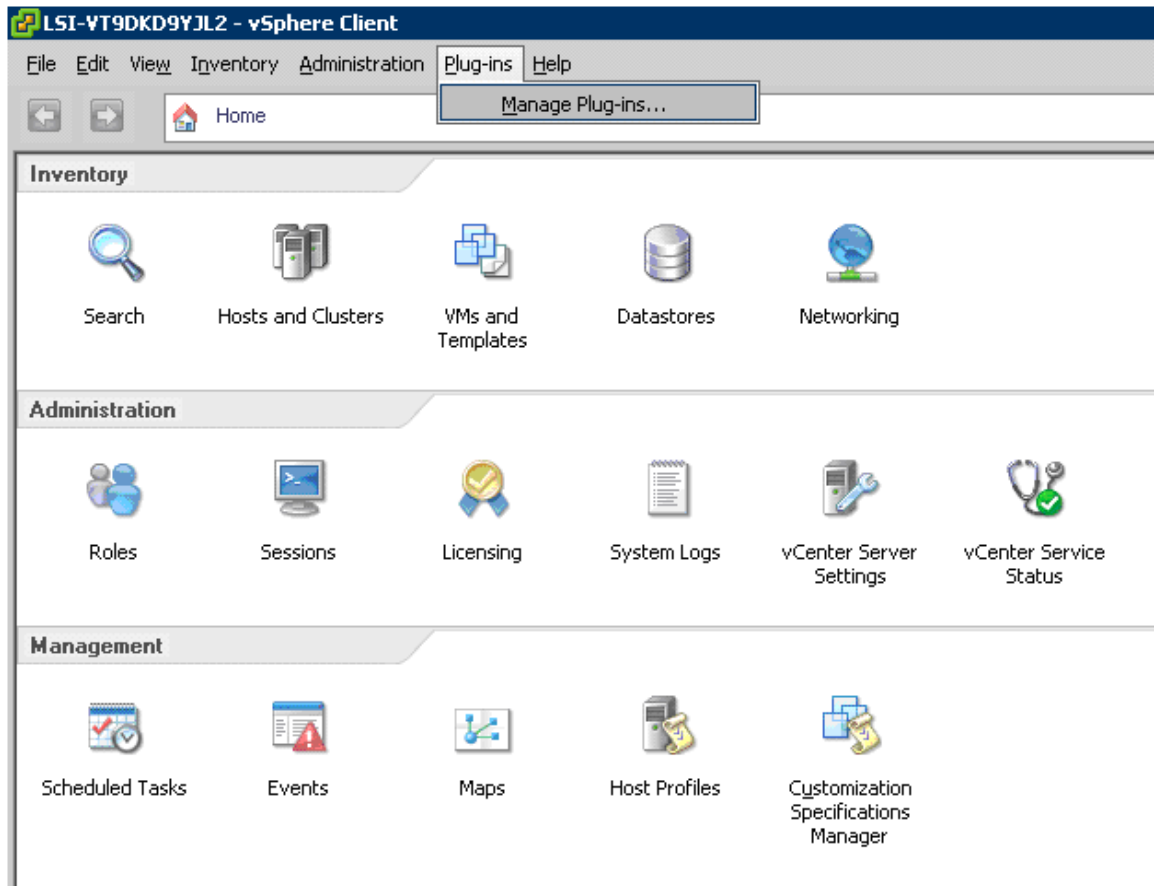
## Installing the SRM plug-in

The SRM plug-in lets the VI Client Manager and configure the Site Recovery options for SRM. You must connect the VI Client to a VC Server that has SRM installed before you can download the SRM plug-in application.

If not already installed, install VMware's VI Client. For this, perform the following steps.

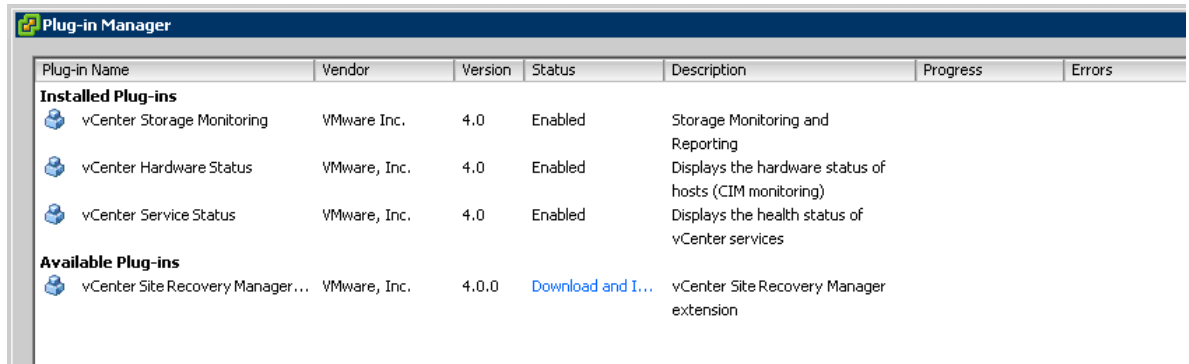
1. Select the **Plug-ins** menu option, and then select **Manage Plug-ins**.

Figure 11: VI Client Manage Plug-ins



2. From the **Available** tab, download and install the plug-in for VI, if the SRM server is detected.

Figure 12: Available SRM Plug-in



The screenshot shows the 'Plug-in Manager' window with a table of installed and available plug-ins. The 'Available Plug-ins' section is highlighted, showing the 'vCenter Site Recovery Manager' plug-in with a 'Download and Install' button.

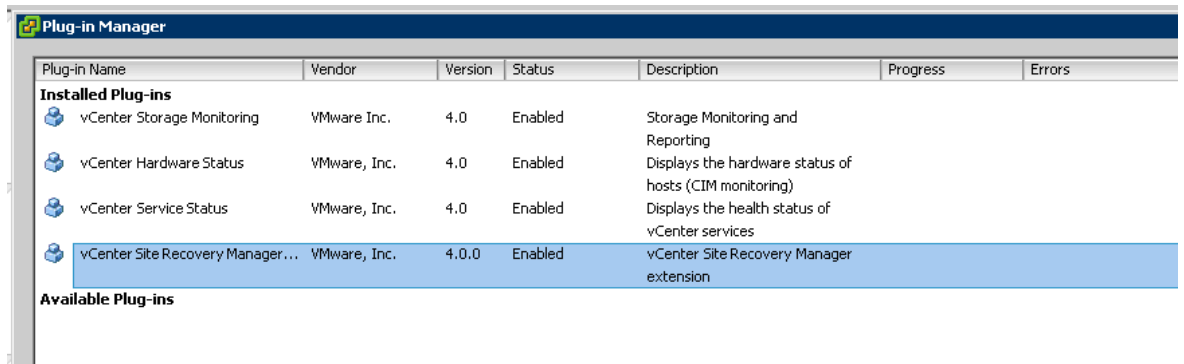
Plug-in Name	Vendor	Version	Status	Description	Progress	Errors
<b>Installed Plug-ins</b>						
vCenter Storage Monitoring	VMware Inc.	4.0	Enabled	Storage Monitoring and Reporting		
vCenter Hardware Status	VMware, Inc.	4.0	Enabled	Displays the hardware status of hosts (CIM monitoring)		
vCenter Service Status	VMware, Inc.	4.0	Enabled	Displays the health status of vCenter services		
<b>Available Plug-ins</b>						
vCenter Site Recovery Manager...	VMware, Inc.	4.0.0	Download and I...	vCenter Site Recovery Manager extension		

#### Note

Best Practice: Select one VI Client instance on which to install the SRM plug-in. If possible, use VI Client on the same server that was used in the VC server installation and the SRM server installation.

3. After the plug-in is installed, close the window.
4. Open the **Manage Plug-ins** dialog again.
5. In the **Installed** tab, select SRM plug-in to set up the SRM plug-in.

Figure 13: Installed SRM Plug-in



The screenshot shows the 'Plug-in Manager' window with the 'vCenter Site Recovery Manager' plug-in now listed under the 'Installed Plug-ins' section. The 'Status' column for this plug-in is 'Enabled'.

Plug-in Name	Vendor	Version	Status	Description	Progress	Errors
<b>Installed Plug-ins</b>						
vCenter Storage Monitoring	VMware Inc.	4.0	Enabled	Storage Monitoring and Reporting		
vCenter Hardware Status	VMware, Inc.	4.0	Enabled	Displays the hardware status of hosts (CIM monitoring)		
vCenter Service Status	VMware, Inc.	4.0	Enabled	Displays the health status of vCenter services		
vCenter Site Recovery Manager...	VMware, Inc.	4.0.0	Enabled	vCenter Site Recovery Manager extension		
<b>Available Plug-ins</b>						

A new **Site Recovery** icon appears in the VI Client.

## Configuring the SRM Plug-in

In the VI Client, click the Site Recovery icon to start the Site Recovery window.

Click Configure next to the option you want to configure to start the setup wizards. The options available include:

- Connection
- Array Managers
- Inventory Mappings

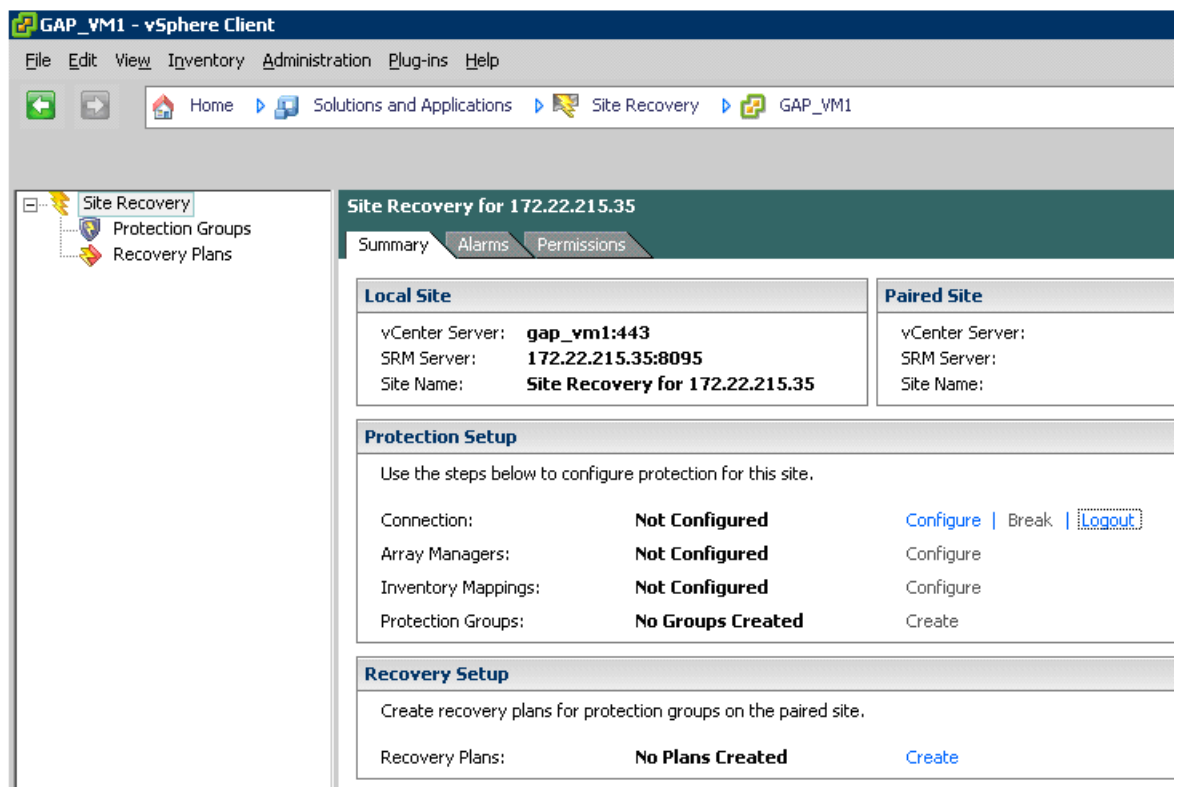
To create a recovery plan, click Create next to Recovery Plan to start the setup wizard.

## Pairing the Primary Site and the Secondary Site

The first task after installing SRA that must be completed is pairing of the primary site to the secondary site. You can accomplish this task by selecting the **Configure** link next to the Connection header under the Protection Setup section from the **Site Recovery** window.

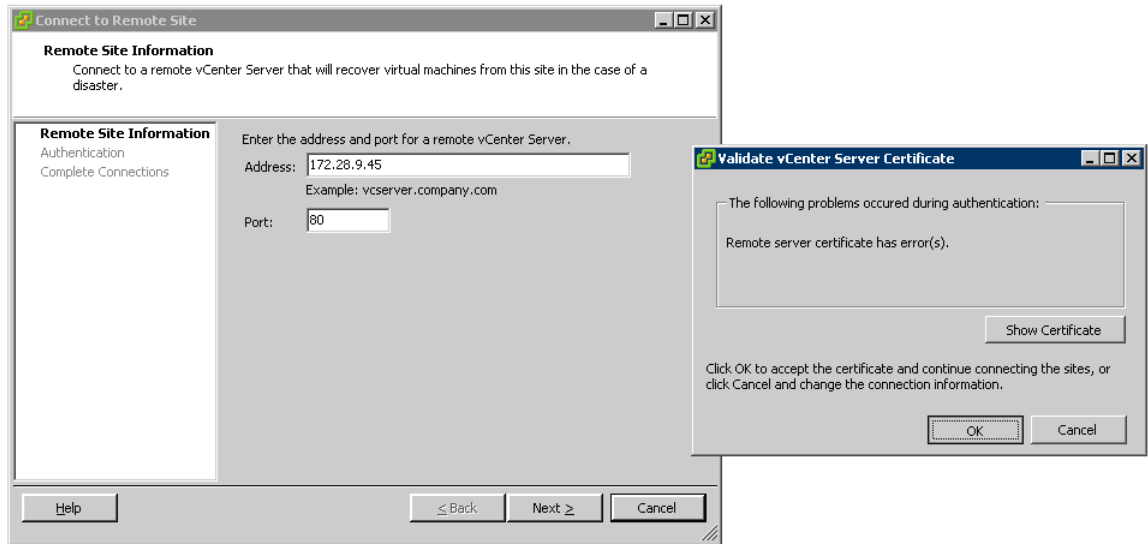
1. In the Site Recovery window, click **Configure**.

Figure 14: Site Recovery Manager Initial window



2. The "Connect to Remote Site" dialog appears.

Figure 15: Remote Site vCenter information



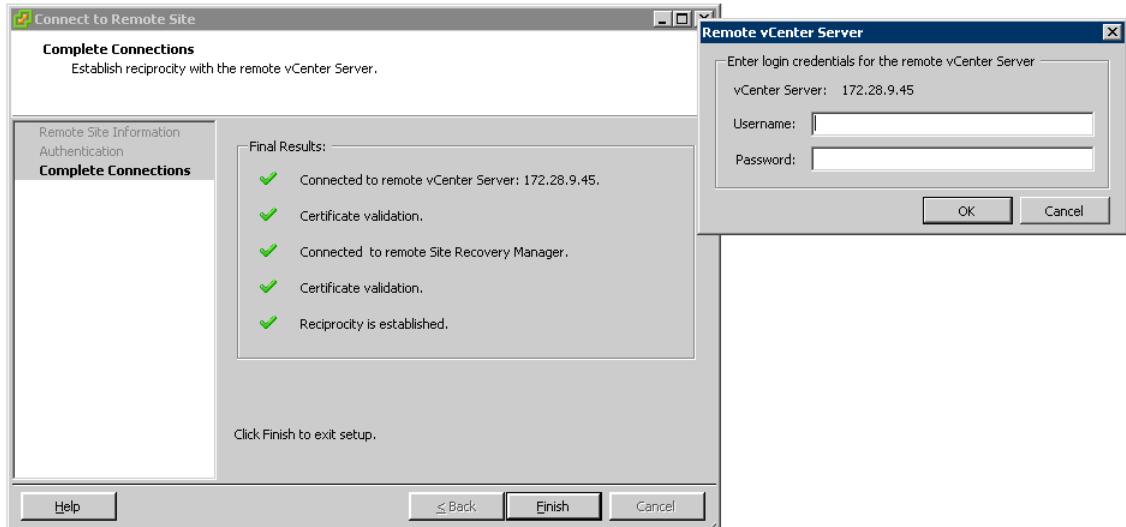
To establish the site roles (protected and recovery), perform the following steps.

3. Select **Remote Site Information**.
  - a. Enter the address and the port of the recovery site VirtualCenter server. If the certificate error screen appears, either click **OK** or fix the certification problems.

**Note:**  
Certificate configuration is beyond the scope of this document.

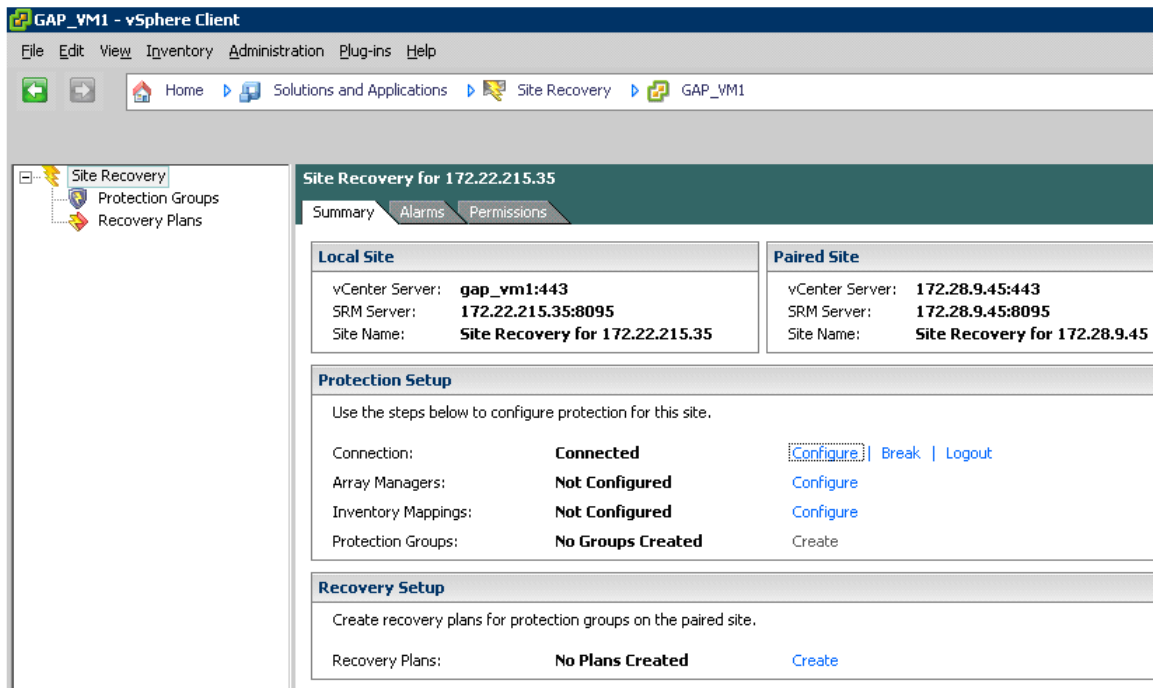
4. Select **Authentication**.
  - a. Enter the administrator username and password for the recovery site VirtualCenter.
  - b. If the certificate error screen appears, either click **OK** or fix the certification problems. Certificate configuration is beyond the scope of this document.

Figure 16: Remote vCenter Server login credential



5. Click **Finish** to complete the connections.
  - a. The dialog boxes requesting the username and the password might appear at both the sites.
  - b. To complete the pairing, enter username and password.

Figure 17: Established connection



Now the pairing is established between two sites.

## Preparing for disaster recovery

Declaring a disaster and running the appropriate recovery plan requires manual intervention. SRM can be set up to notify administrators when communication with the remote site is lost. Using these alerts and the other alerts, the administrator must decide when a disaster has occurred and whether or not to carry out a recovery plan. Running a recovery plan is also called a failover.

### Configuring storage array managers

Storage array management defines the storage arrays to SRM. It also lets SRM, through the SRA, interface to the enhanced remote mirroring feature to control the replication of data between the primary site and the secondary site.

- Launch the SVSP SRA window to configure the storage array.

Array managers have to be created successfully before protection groups can be configured.

Sometimes, existing array managers do not refresh correctly. If this problem occurs, click the **Rescan** option on the final page to find the array managers again.

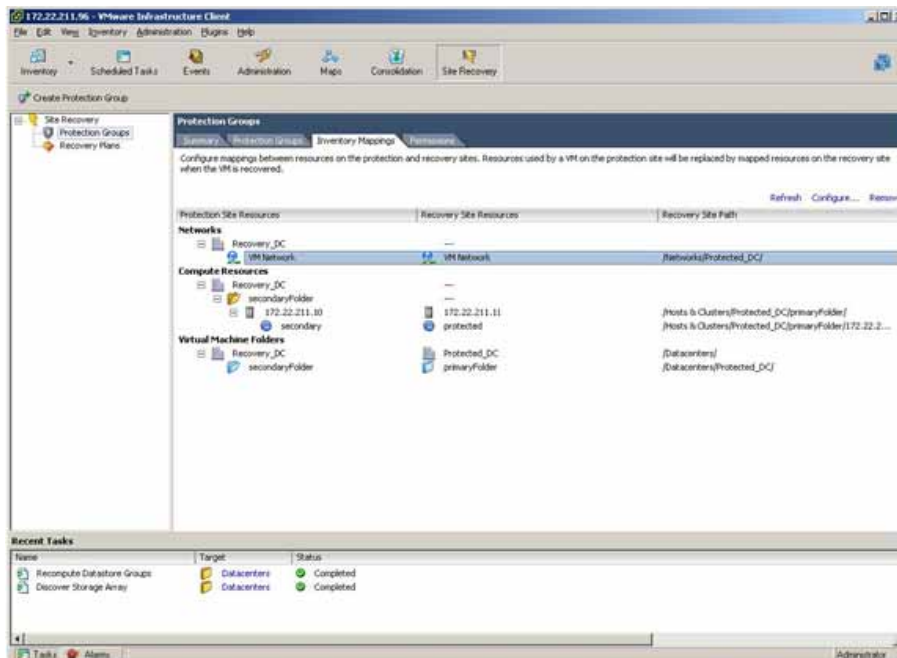
If you view the **Site Recovery** window for the secondary site, you might find that the Array Managers show as not configured. Only the primary site shows the datastores on that site. The recovery site has read-only access to the mirrored volumes.

### Creating an Inventory Mapping

Inventory mappings specify the corresponding device or service on the recovery site to which the protected site device or service will failover. Configuring the inventory mappings is optional. However, if these mappings are not specified at the time, you must configure inventory mappings for each protected virtual machine (VM) individually.

1. Click **Configure** in the Inventory Mappings tab.

Figure 18: Inventory Mapping



This screen shows how the resources that are in use on the primary site map to the recovery site resources.

2. Double-click each line that states none selected in the **Recovery Site Resources** field to select the appropriate recovery site resource.

### Creating a protection group

**Protection groups** are groups of virtual machines that are failed over together. Grouping such virtual machines together on a single virtual machine file system (VMFS) LUN is convenient. This procedure is also preferred because a one-to-one relationship between a protection group and a datastore exists. No special SVSP Configuration is needed to create a Protection Group.

1. From the **Site Recovery Summary** window, select **Create** next to the Protection Groups field.

The Protection Groups dialog appears.

- a. In the **Protection Group** field, enter the name of the new protection group.
  - b. Select the datastore group that contains the virtual machines to be grouped together.
  - c. Enter a location to hold the temporary inventory files on a local datastore that is not replicated at the recovery site.
2. Click **Next** to review or change the list of protected VMs to be assigned to the new Protection Group.
  3. Click **Finish** to create the new group.

### Creating a Recovery Plan

A **recovery plan** is a sequence of steps that are performed by SRM at the secondary site when a true DR scenario occurs or when a DR plan is being tested. A recovery plan contains protection groups from the primary site. Recall that the protection group contains all virtual machines in the plan. All of these virtual machines will be recovered by the recovery plan.

4. Log on to the recovery site VirtualCenter server.
5. In the main **Site Recovery** window, click **Create** in the **Recovery Setup** field.

The **Create Recovery Plan** dialog box appears.

- a. Specify a Recovery Plan name and description, and click **Next**.
- b. Specify one or more protection groups to include in the plan.
- c. Modify or accept the defaults for response times of VMs.
- d. Specify the network to use for testing the DR plan.

Suspend any local VMs to free up resources for testing recovery plan.

After you complete the recovery plan, you can simulate a failover of the protected resources at the recovery site in an isolated environment that includes network and storage. To facilitate this test procedure, you must specify a separate network to use during the test.

## Testing the Disaster Recovery Plan

SRM lets you test disaster recovery plans at anytime without affecting production services significantly. SRM performs this task using SVSP redirect-on-write snapshots of the mirrored volumes that are created by SVSP SRA at the recovery site. During the recovery plan configuration, you can suspend non-critical VMs on the recovery site to make sure that you have enough resources to run the DR test.

You can test the DR plan by clicking on the **Test** button on the menu bar.

On the recovery site SVSP domain, SVSP SRA will create snapshots of the protected datastore volumes on the recovery site array and map them to the Recovery Site ESX host as read/write volume. Once these temporary volumes are mapped to the ESX host, SRM will start each of the VMs that are contained on the replicated datastore. Once all the VMs have been brought online, the recovery plan will pause to allow verification of the VMs. During this process, the IP address would have been removed, so you will not be able to access the VMs remotely, but can launch the console window to verify the status of the VMs. After verification, click the **Continue** link to remove the VMs and snapshots from the Recovery Site ESX host.

## Performing the recovery failover

To run a Disaster Recovery plan, select the **Run** button from the menu under the SRM Recovery Plan window.

In case of a failure at the primary site where it is deemed necessary to failover to the Recovery Site, the process is similar to the Test plan with key exceptions. Failing over to the Recovery Site is a one-way process in that, to failback, you will need to configure the Recovery Site (now acting as Primary Site) and the Primary Site (now acting as Recovery Site) relationships before you can failback from the Recovery Site. Configuring the relationships includes creating inventory maps, protection groups, and recovery plans. You would then need to run the new recovery plan to failback to the original Primary Site. Also, when running the recovery plan, SRM will attempt to shut down any protected VMs that are still running and shutting down any designated VMs on the Recovery Site that were listed in the recovery plan

On the recovery site that uses the remote SVSP domain, SVSP for each asynchronous mirror group:

1. Breaks/splits the asynchronous mirror group
2. Assigns the destination virtual disk to the ESX servers on the recovery site

After you run a failover, the failover is irreversible except by following the steps outlined in the next section.

## Performing a failback from the recovery site

Failback is the process of setting the replication environment back to its original state. The failback is a manual process that includes three steps:

1. Synchronize the data changes from the recovery site back to the protected site
2. Reinstall the replication back to its original state from protected site to recovery site
3. Reinstall the VMware SRM original state

Steps 1 and 2 are done on the SVSP side and step 3 is done on the VMware side.

There are two possible scenarios for failback:

### Protected site was offline for a while and came back

Failback steps will include the following:

1. On the SVSP, use the async mirror merge feature which sync only the data changes back from the recovery site to the protected site
2. On the SVSP, use the async mirror split feature which will reinstall the async mirror back to its original state
3. On the VMware site, perform the steps to reinstall the SRM to its original state

### Protected site was destroyed and completely rebuilt

Failback steps will include the following:

1. On the SVSP, create a new async mirror group and tasks which will first sync all data from the recovery site to the new protected site
2. On the SVSP, use the async mirror split feature which will revert the async mirror direction back to its original state
3. On the VMware site, perform the steps to reinstall the SRM to its original state

## Conclusion

HP StorageWorks SAN Virtualization Services Platform (SVSP) and VMware can be combined to create new opportunities. Both server and storage virtualization offer unique benefits, but it is not until the two technologies are combined that users truly recognize the full benefits of a solution. The integration of HP SVSP with VMware's SRM provides a comprehensive and cost-effective disaster recovery solution.

## For more information

For more information see: <http://www.hp.com/go/svsp>

To find all manuals and technical documents related to SVSP, please follow the link above, click on "Support & Documents" (on the right of the page) and then click "Manuals" (under "Resources for HP StorageWorks SAN Virtualization Services Platform.")

The "HP SVSP User Guide" referred to in this document is the "HP StorageWorks SAN Virtualization Services Platform Manager User Guide." In 2010, its name will change to the "HP Command View SVSP User Guide."

When it ships, the SVSP SRA plug-in will be available at this website:

<http://h20000.www2.hp.com/bizsupport/TechSupport/ProductList.jsp?lang=en&cc=us&taskId=135&prodTypeId=18964&prodSeriesId=499896>



## Technology for better business outcomes

© Copyright 2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA2-9855ENW Rev. 1, December 2009

