TECHNICAL REPORT

PROTECTING THE VIRTUAL DATACENTER: DISASTER RECOVERY USING DELL EQUALLOGIC PS SERIES STORAGE AND VMWARE VCENTER SITE RECOVERY MANAGER

ABSTRACT

The virtual datacenter introduces new challenges and techniques for disaster recovery. This technical report details the installation and configuration of Dell™ EqualLogic™ PS Series storage and VMware® vCenter Site Recovery Manager to help make disaster recovery an automated and manageable part of your virtual environment.

TR1039

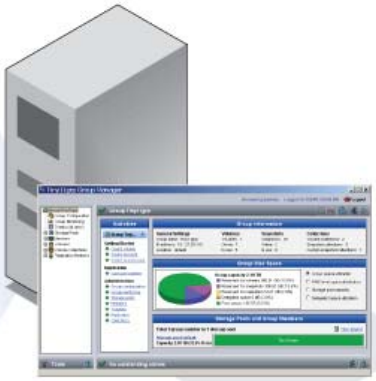
V2.1

[June 2010]

WWW.DELL.COM/PSseries

Array Software

PS Series Firmware
- Installation and Setup
- Group Administration
- CLI Reference
- Online Help
- Manual Transfer Utility User Guide
- Host Scripting Tools



Microsoft

Remote Setup Wizard
Multipath I/O DSM
- Host Installation Tools Installation and User Guide

Auto-Snapshot Manager (ASM/ME)
- User Guide
- Online Help

SAN HeadQuarters
- User Guide

VMware

Auto-Snapshot Manager (ASM/VE)
- User Guide
- Online Help

Storage Replication Adaptor for Site Recovery Manager
- Release Notes

Array Hardware

PS Series Arrays
- Setup Poster
- Installation & Setup
- Hardware Maintenance

PREFACE

Thank you for your interest in Dell™ EqualLogic™ PS Series storage products. We hope you will find the PS Series products intuitive and simple to configure and manage.

PS Series arrays optimize resources by automating volume and network load balancing. Additionally, PS Series arrays offer all-inclusive array management software, host software, and free firmware updates. The following value-add features and products integrate with PS Series arrays and are available at no additional cost:

Note: The highlighted text denotes the focus of this document.

- **PS Series Array Software**
  - **Firmware –** Installed on each array, this software allows you to manage your storage environment and provides capabilities such as volume snapshots, clones, and replicas to ensure data hosted on the arrays can be protected in the event of an error or disaster.
    - **Group Manager GUI:** Provides a graphical user interface for managing your array
    - **Group Manager CLI:** Provides a command line interface for managing your array.
  - **Manual Transfer Utility (MTU):** Runs on Windows and Linux host systems and **e**nables secure transfer of large amounts of data to a replication partner site when configuring disaster tolerance. You use portable media to eliminate network congestion, minimize downtime, and quick-start replication.
- **Host Software for Windows**
  - **Host Integration Tools**
    - **Remote Setup Wizard (RSW):** Initializes new PS Series arrays, configures host connections to PS Series SANs, and configures and manages multipathing.
    - **Multipath I/O Device Specific Module (MPIO DSM):** Includes a connection awareness-module that understands PS Series network load balancing and facilitates host connections to PS Series volumes.
    - **VSS and VDS Provider Services:** Allows 3rd party backup software vendors to perform off-host backups.
    - **Auto-Snapshot Manager/Microsoft Edition (ASM/ME):** Provides point-in-time SAN protection of critical application data using PS Series snapshots, clones, and replicas of supported applications such as SQL Server, Exchange Server, Hyper-V, and NTFS file shares.
  - **SAN HeadQuarters (SANHQ):** Provides centralized monitoring, historical performance trending, and event reporting for multiple PS Series groups.
- **Host Software for VMware**
  - **Storage Adapter for Site Recovery Manager (SRM):** Allows SRM to understand and recognize PS Series replication for full SRM integration.
  - **Auto-Snapshot Manager/VMware Edition (ASM/VE):** Integrates with VMware Virtual Center and PS Series snapshots to allow administrators to enable Smart Copy protection of Virtual Center folders, datastores, and virtual machines.
  - **MPIO Plug-In for VMware ESX:** Provides enhancements to existing VMware multipathing functionality.

Current Customers Please Note: You may not be running the latest versions of the tools and software listed above. If you are under valid warranty or support agreements for your PS Series array, you are entitled to obtain the latest updates and new releases as they become available.

To learn more about any of these products, contact your local sales representative or visit the Dell EqualLogic™ site at http://www.equallogic.com. To set up a Dell EqualLogic support account to download the latest available PS Series firmware and software kits visit: https://www.equallogic.com/secure/login.aspx?ReturnUrl=%2fsupport%2fDefault.aspx

TABLE OF CONTENTS

REVISION INFORMATION

The following table describes the release history of this Technical Report.

Report	Date	Document Revision
1.0	June 2008	Initial Release
2.0	January 2010	Updated Release for vSphere and vCenter Site Recovery Manager
2.1	June 2010	Updated Release for SRA 1.0.5 and Firmware 5.0

The following table shows the software and firmware used for the preparation of this Technical Report.

Vendor	Model	Software Revision
VMware®	vSphere	ESX 4.0
VMware®	vCenter Site Recovery Manager	vCenter Site Recovery Manager 4.0
VMware®	vCenter	vCenter Server 4.0
Dell™	Dell EqualLogic PS Series Storage	FW 4.2.x and 5.0
Dell™	Dell EqualLogic Storage Adapter	1.0.5

The following table lists the documents referred to in this Technical Report. All PS Series Technical Reports are available on the Customer Support site at: *support.dell.com*

Vendor	Document Title
VMware®	VMware vCenter Site Recovery Manager Administration
VMware®	VMware vCenter Site Recovery Product Documentation
VMware®	VMware vCenter Site Recovery Manager Performance and Best Practices
VMware®	VMware vSphere System Administrator Documentation
Dell™	Dell EqualLogic PS Series Installation and Setup
Dell™	Configuring VMware vSphere Software iSCSI with Dell EqualLogic PS Series Storage
Dell™	Dell EqualLogic PS Series Group Administration Guide

EXECUTIVE SUMMARY

Data Protection and Disaster Recovery (DP/DR) is foremost in the minds of datacenter administrators. Virtualization adds increased flexibility and techniques when looking at protection schemes for the environment. Because VMware® encapsulates systems into files, administrators can now take advantage of file based techniques such as clones, snapshots and replicas. Dell™ EqualLogic™ PS Series storage arrays offer built-in replication to transfer data, and thus the machines, from one location to another and integration software that combines with VMware vSphere™. VMware vCenter Site Recovery Manager is a suite of tools that help to automate and test a Disaster Recovery plan and depends on the PS Series replication to work. By combining these two platforms, administrators now have a manageable way to not only configure and test a disaster recovery plan, but the means to run it in the case of a disaster.

This Technical Report details the installation and configuration of VMware vCenter Site Recovery Manager (SRM) software. As part of this setup, Dell has a storage adapter plug-in that is needed to enable communication from the PS Series storage to VMware vCenter. In addition to SRM configuration and the storage adapter, this document will detail how to configure replication between sites and how to setup and test a recovery plan. The last section of this report shows administrators how to perform a full site failover and how to failback when the problems are resolved.

INTRODUCTION

Historically, disaster recovery (DR) solutions have been difficult and costly to implement. DR has been a pain point for many IT administrators, having to maintain consistency across duplicate hardware in various locations, documenting and maintaining detailed run books, reacting to changes in the environment, and scheduling testing that is classically disruptive to the production environment.

VMware's vCenter Site Recovery Manager, or Site Recovery Manager (SRM), works with the Dell EqualLogic PS Series built-in replication to make disaster recovery rapid, manageable, reliable and affordable. SRM is a plug-in for vCenter on both the primary and the recovery site. SRM and vCenter at the production site coordinate with vCenter and SRM residing at the recovery site to simplify and automate disaster recovery. SRM allows for automated testing of DR plans as well as managing recovery in the event of a real disaster. SRM facilitates the process of bringing an entire virtual environment from one location to another. SRM centralizes the process of configuring a DR plan run book and allows for the testing of the plan without causing any impact to the production environment.

This technical report will discuss the installation and configuration of SRM with the Dell EqualLogic PS Series storage arrays. It will cover setup, testing, failover, failback and troubleshooting. This document is designed to be used in conjunction with the *SRM Administration Guide* and assumes a prior knowledge of VMware vSphere and vCenter environments.

VMWARE VCENTER SITE RECOVERY MANAGER TERMINOLOGY

VMware's vCenter Site Recovery Manager introduces new terms when discussing DR planning and configuration. Because SRM and the PS Series storage supports bi-directional replication and configuration, it is sometimes confusing to use the terms "production site" and "DR site". There could be an example where there is a virtual environment in New York running Virtual Machines (VMs) in production that is replicating to Chicago as a DR site. Chicago also has its own virtual environment in production and its DR site is in New York. With SRM and bi-directional replication provided by the storage, both sites are protected from a disaster. If there is a problem in New York, all of those virtual machines can be recovered in Chicago and brought online and the reverse holds true if there is a problem in Chicago. There can also be a scenario where utilizing the many to one replication of the PS Series array, you can have multiple satellite offices each of which is configured to replicate back to a primary DR or centralized corporate datacenter.

VMware uses the terms **protected site** and **recovery site** to differentiate between the two sites for a VM. A protected site is the site in which production VMs are up and running. These Virtual Machines must be protected and are done so by configuring array-based replication for their datastores to another site.

A recovery site is the site that the protected VMs are replicated to. In the case of a disaster, SRM can bring these VMs online following a clear plan, minimizing the downtime and recovery time.

OVERVIEW AND PREREQUISITES

Site Recovery Manager requires VMware vCenter server to be installed at both the protected site and the recovery site. Both sites will have their own VMware vSphere environment and datacenters set up and configured. The configuration done in SRM is mirrored to the recovery site SRM server so that in the case the primary site is down, everything that the recovery site needs is local.

VMware vCenter Site Recovery Manager does not automate or configure storage replication between each site. This needs to be configured by the storage administrator as detailed in this document using storage array management tools.

Both PS Series replication and SRM require adequate network connectivity and bandwidth between the protected site and the recovery site.

SRM will protect the VMFS Datastores that the VMs reside on. All of the VMs must reside on shared storage and be configured for replication to qualify as protected.

CONFIGURING REPLICATION FOR VCENTER SITE RECOVERY MANAGER

VMware vCenter Site Recovery Manager is deployed with two separate PS Series groups that have replication enabled so that the Virtual Machines that reside on the datastores at the protected site are replicated to the recovery site. In order for a datastore to be protected with SRM the following conditions must be met:

- The PS Series groups must be configured for replication
- The volumes must have replication configured
- The volumes must be part of a replication schedule

Once these conditions are met the volume will show up as a protected datastore group inside SRM.

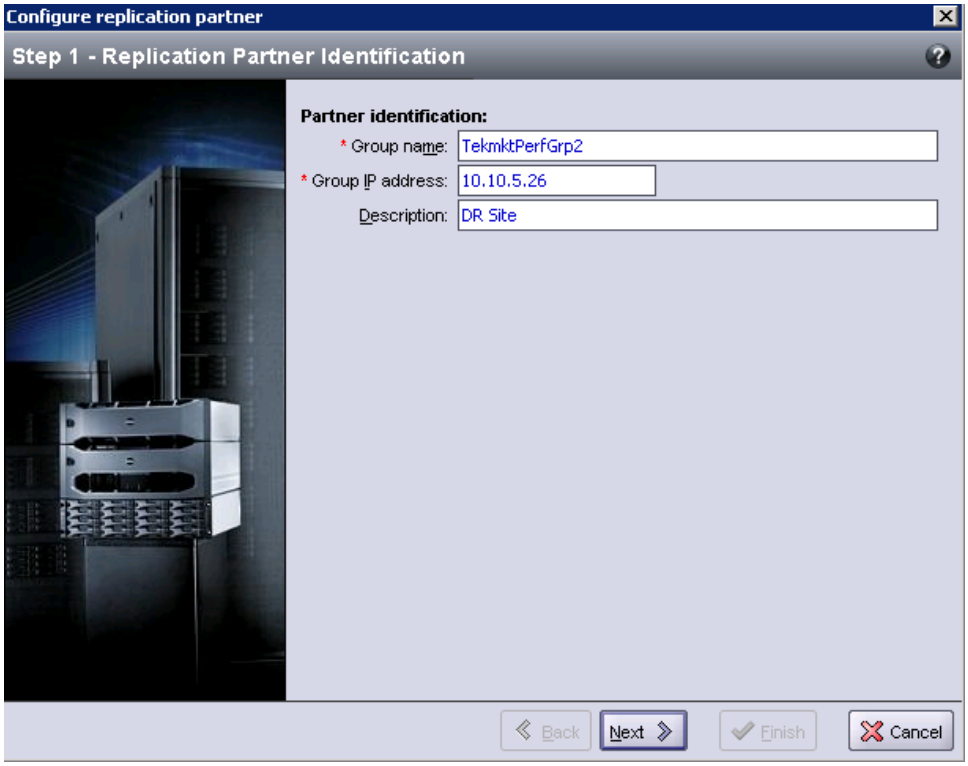
Replication capabilities are a standard feature in the PS Series SAN and are simple to configure. The steps for configuring replication and configuring the volume are detailed below. More detailed information can be found in the Group Manager under **Tools -> Online help -> Welcome To Group Manager GUI Help -> Managing Data Replication**. These operations are done using the PS Series array Group Manager GUI.

Step 1: Configure Replication Partnership between Protected Site Array and Recovery Site Array

1. From the protected site Group Manager GUI click the **Replication** management button.

2. Under Replication Partners in the **Activities** tab click on **Configure Partner**.

3. Enter in the **Group Name** of the recovery site (case sensitive), the **Group IP Address** and a **Description**. Click **Next**.

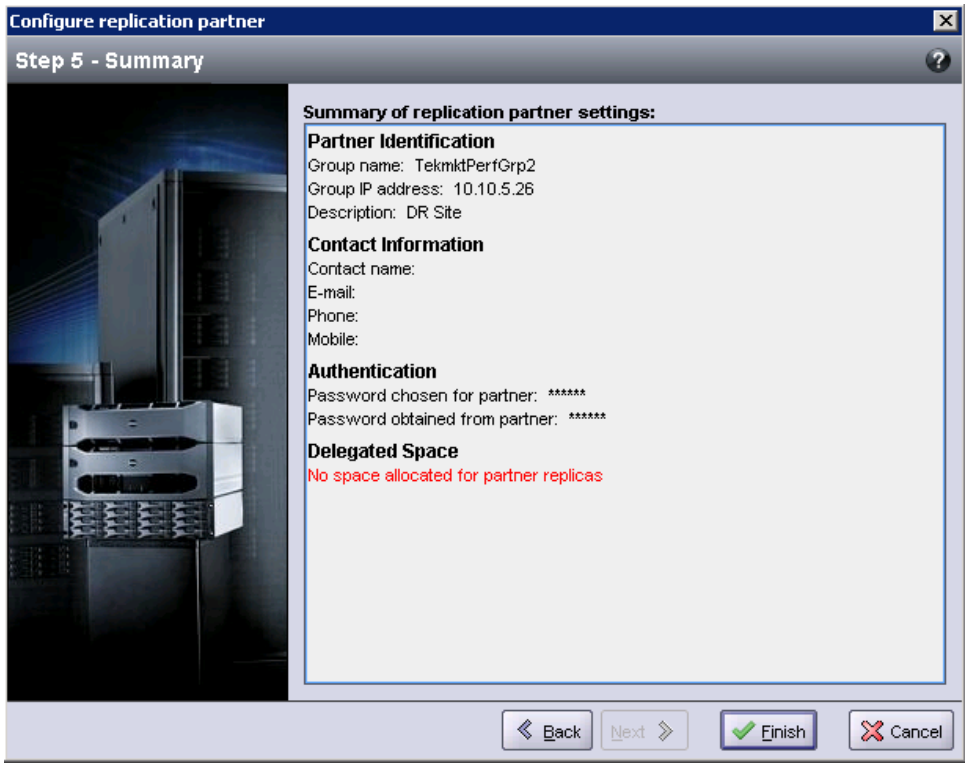


4. Enter in contact information in the next screen and click **Next**.

5. On the next screen there are two password fields. The first field is the **Password for partner**. This is the password that the protection group will give to the recovery group when establishing a connection for replication. The second field is the **Password obtained from partner**. This is the password that the recovery site expects to receive from the partner. Both of these can be the same or different depending on the environment. Enter in the passwords and click **Next**.

6. The 4th step in the configuration wizard is to configure **Delegated Space**. This is space that is created from local free space on the group to store replicas from the partner. The Dell EqualLogic PS Series SAN supports bi-directional replication as well as many to one replication. If there are going to be no replicas sent to this site then the value can be left at 0. Choose the amount of delegated space, the storage pool which the space will come from and click **Next**.

7. Verify all of the information is correct and click **Finish**.



8. This creates the partnership between the protected site and the recovery site. Now follow the same steps to configure the partnership between the recovery site and the protected site.

   When configuring the dedicated reserve space for replication, take into account the number of volumes being replicated and the total available space. For example, four 200GB volumes with data on them being replicated with 200% reserve space plus a little bigger will mean 1TB of delegated space on the recovery site. Choosing how much space to allocate will depend on things such as the number of replicas you wish to keep as well as how much data change is happening between each replica.

Step 2: Configure replication on the Datastore volumes

Once a partnership is established on both sides for replication, each volume needs to also be configured for replication.

1. From the protected site Group Manager GUI click the **Volumes** management button.

2. Click on a Datastore volume that you wish to protect with replication. In the **Activities** tab click on **Configure Replication**.

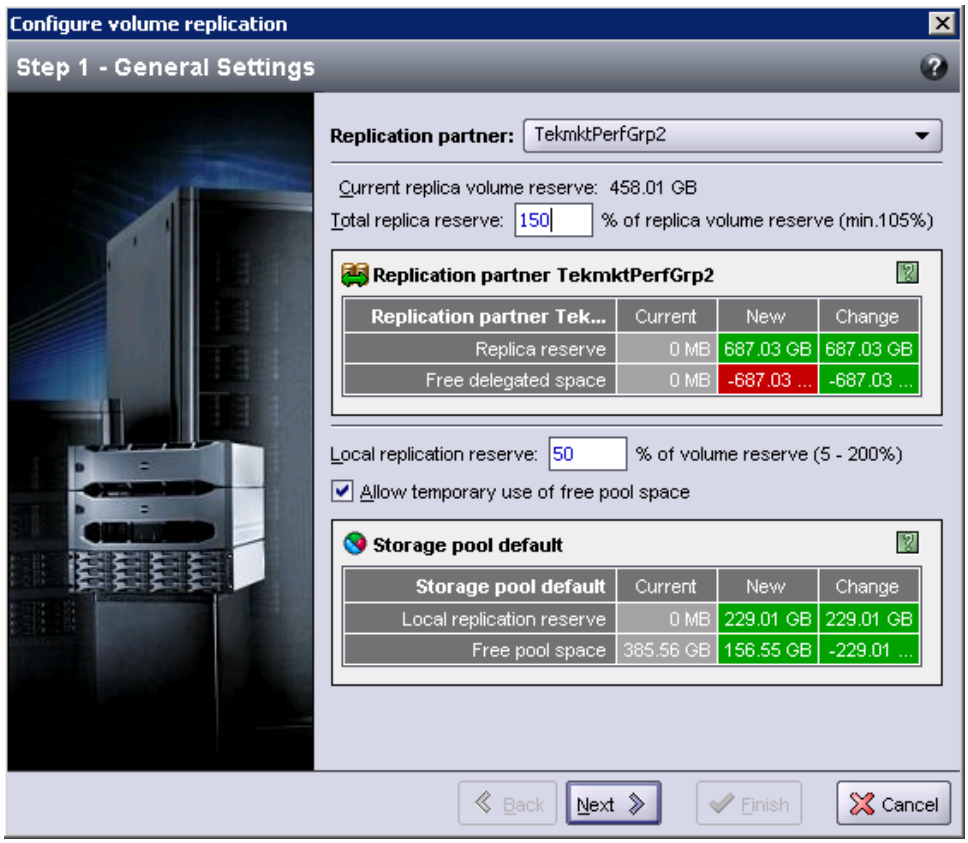
3. The next screen is divided into three sections.

   In the first section, choose the **Replication partner** that this volume will be replicated to.

   In the second section, select the Total replica reserve which is a percentage of this volume that is set aside from the delegated space on the partner. This percentage not only accounts for 100% of the initial replica volume but should be configured based on the amount of change and the number of replicas you wish to keep.

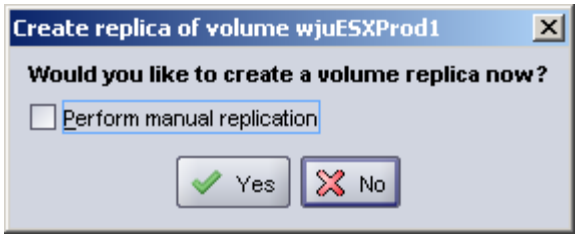
   The third section will set aside a percentage of this volume in the local replica reserve to keep track of changes made during the replica process. This is also where Fast Failback Snapshots are stored in the event you are failing back from a replica set. This can either come from local replica reserve or free space by selecting **Allow temporary use of free pool space**.

   Choose your options in each section and click **Next**. These can always be modified later.



4. In the Advanced Settings screen, you have the option to keep a failback snapshot. Fast Failback keeps a copy of the most recent replica on the protected array. In the event of fail back from the recovery site this will result in shorter recovery time as only the changes at the recovery site need to be replicated back to the protected site. In order to use Fast Failback this check box must be selected. Make your selection and click **Next**.

5. View the summary and click **Finish** to complete the replication configuration. When this is done you will be prompted to optionally start the volume replica process immediately. This will begin replicating the base volume and creating a replica set on the partner array, and can either be performed at this stage or by the replication schedule is created for the volume.



   Optionally you can utilize the Manual Transfer Utility (MTU) to perform the initial replica, which allows you to move data from one datacenter to another without using the built in replication. This is often done if the bandwidth between sites is large enough to accommodate change but not sufficient to create the initial replicas in a timely manner. In order to use the MTU click the checkbox in **Perform manual replication** See the *Manual Transfer Utility User Guide* for details.

6. Each volume has to be configured for replication. SRM will not recognize a Datastore as protected until it is configured for replication and has an active schedule configured which is detailed in the next step.

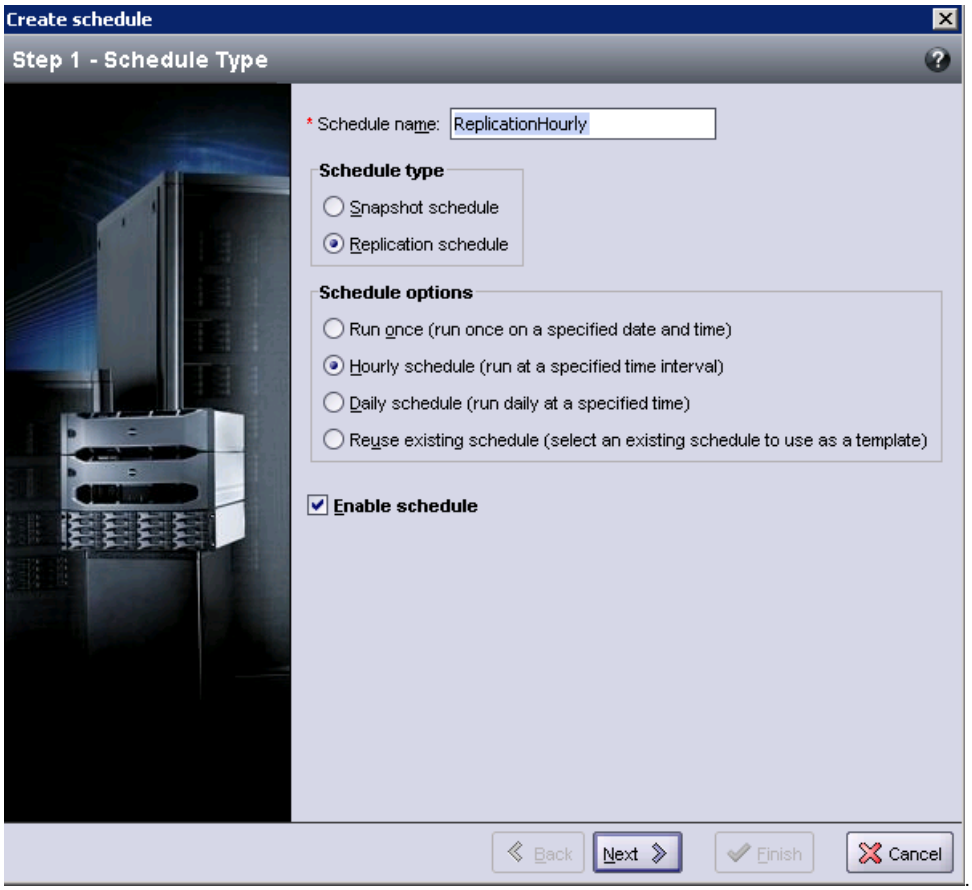
Step 3: Configure Replication Schedule

Each volume can be set up with different replication properties and schedules. This granular control allows for different volumes to have different protection schemes based upon the data that resides on the volume. For example, some volumes may be replicated hourly with keeping the last 10 replicas and others may only be replicated once or twice a day. By taking advantage of the per-volume schedules and schemes, administrators can develop a replication strategy that makes sense for the data contained.

1. From the protected site Group Manager GUI click the **Volumes** management button.

2. Click the volume that you need to configure a schedule for. In the **Activities** tab under **Schedules** click **Create Schedule**.

3. Give the schedule a name and choose **Replication Schedule**. Choose the schedule option and whether or not to enable the schedule and click **Next**.



4. Configure the replication schedule that meets the bandwidth and recovery needs for the VMs on that Datastore volume and click **Next**. For more information on Replication considerations, see the *PS Series Administration Guide*.

5. Verify the summary of the schedule and click **Finish**. Follow the same procedure on all the Datastore volumes that need to be protected in SRM.

NOTE: Dell has released a new version of the VMware Integration software titled Auto Snapshot Manager/VMware Edition (ASM/VE) with added support for replicas. This tool has built in integration with VMware vCenter and can also be used to create and run enhanced consistent replica smart copy schedules. For more information see Technical Report 1041 Protecting the Virtual Environment using Auto-Snapshot Manager/VMware® Edition.

Once the replication partnership is configured between the protected site and the recovery site, and every Datastore volume that needs to be protected has been configured for replication and has an active replication schedule, you can proceed with the configuration of SRM. These same steps can be done any time if new volumes are added to the virtual environment.

INSTALLATION AND CONFIGURATION OF VMWARE VCENTER SITE RECOVERY MANAGER

Before VMware vCenter Site Recovery Manager can be installed, both the protected site and recovery site must have their own copy of VMware vCenter Server installed and configured. Each of these vCenter servers must be able to communicate to each other as well as have connectivity to the SAN. For more information consult the VMware vSphere System Administrator Documentation.

NOTE: In some instances when using multiple networks for LAN/SAN connectivity, the iSCSI NICs may be bound first. This will cause SRM to show up looking on the SAN network instead of the LAN network. Double check NIC bindings so that public LAN bindings are first before SAN.

Once the vSphere virtual environment is configured on both the protected site and the recovery site, install VMware vCenter Site Recovery Manager on both sites. SRM requires a new database to be installed on both sites. The database may reside on the same database server with the vCenter database but it cannot use the same database. SRM is usually installed on the same server as the vCenter server but installations may differ. For more information consult the *SRM Administrator Guide* from VMware.

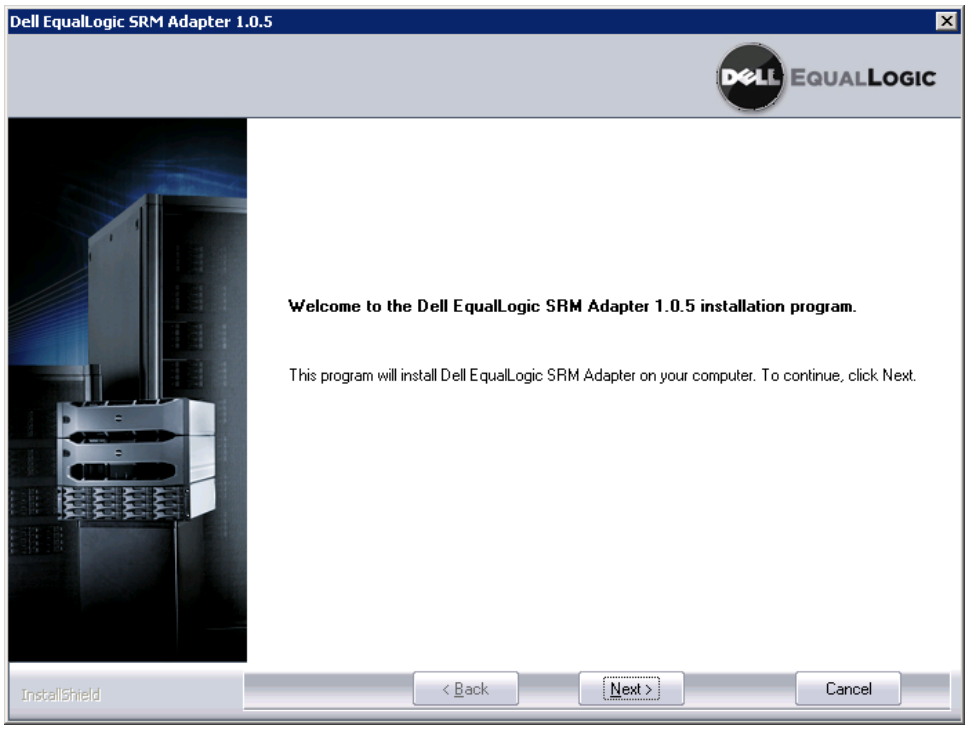
Step 1: Install Dell EqualLogic Array Manager Adapter

Once SRM is installed on both sites the Dell EqualLogic Array Manager adapter (sometimes referred to as array scripts) can be installed on each site. This adapter is necessary to allow vCenter to communicate with the PS Series SANs and to coordinate the entire process of testing, cloning and failing over storage resources as part of disaster protection and testing. SRM does not automate the SAN replication configuration and management process, so this is done using PS Series management tools as described in the previous steps.

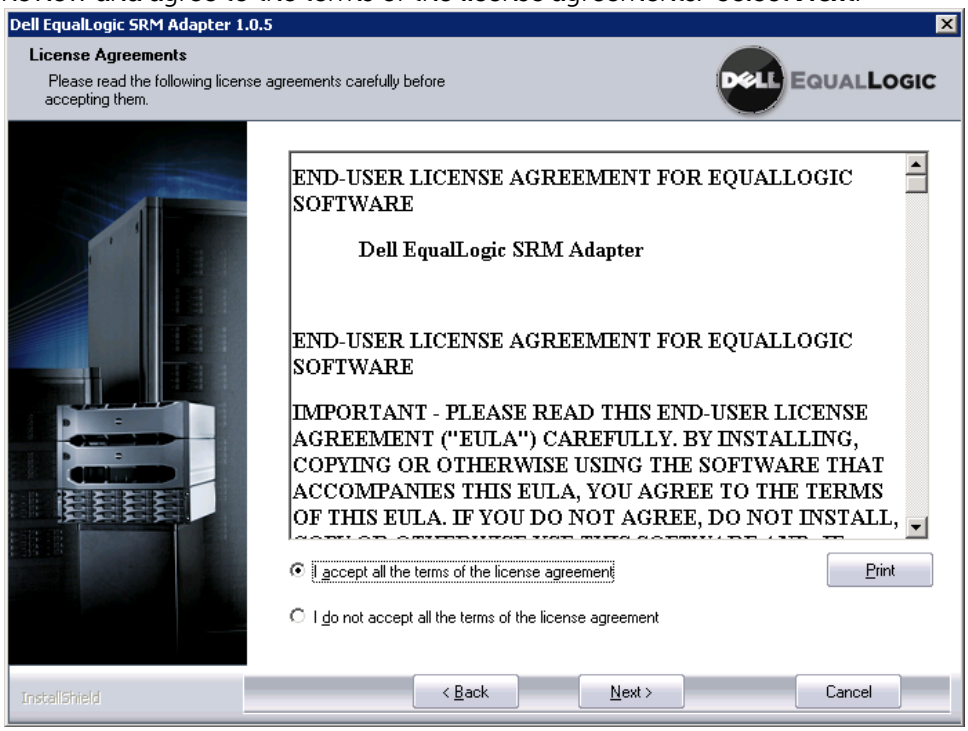
1. You can find the PS Series Array Manager storage replication adapter for SRM download page on the Dell EqualLogic support site, http://www.equallogic.com/support . Download the installer and install on both servers that are running SRM.

2. On both sites the installation procedure is the same. Run the executable for each site.

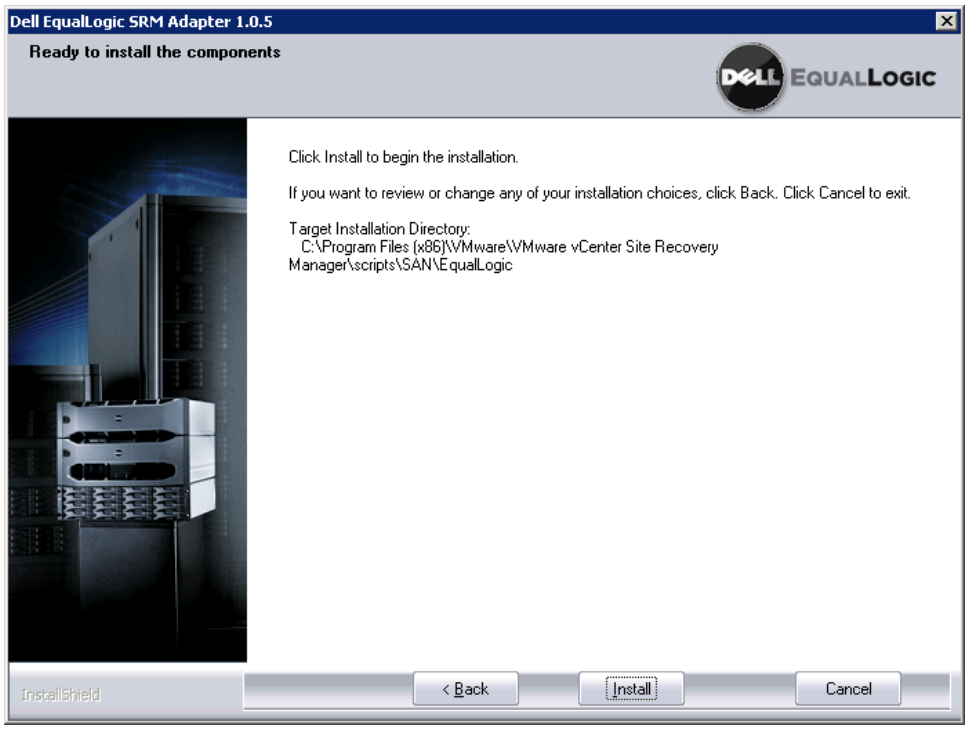
3. Click **Next**.



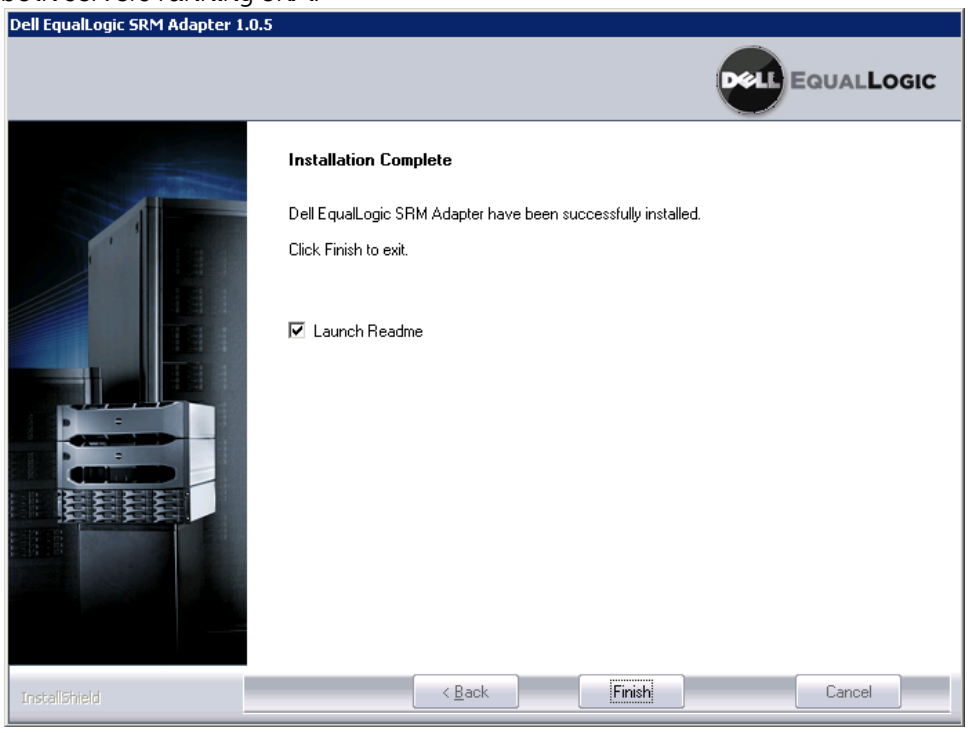
4. Review and agree to the terms of the license agreements. Select **Next**.



5. Verify the target installation directory. If the system is a 32bit server, the installation path should be `C:\Program Files`. In a 64bit installation environment, the path will be `C:\Program Files (x86)`. This is fine as SRM is a 32 bit application and will install where it is supposed to go by default.



6. When the install is complete select **Finish**. The storage adapter needs to be installed on both servers running SRM.

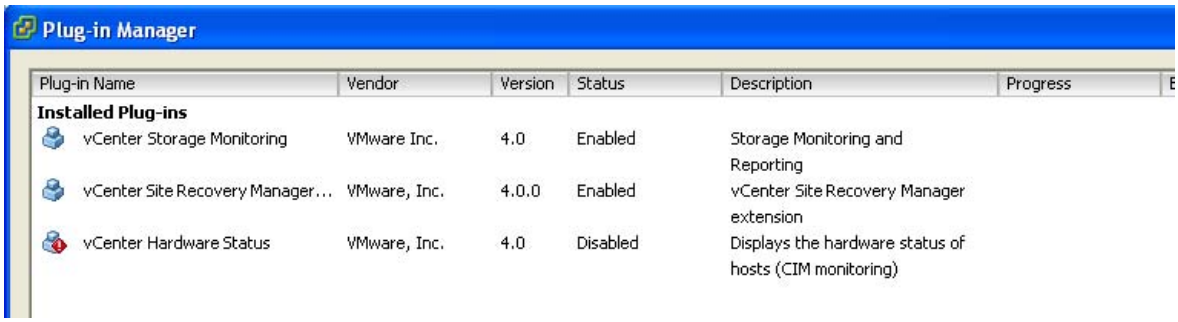


7. Once the adapter is installed the services for VMware vCenter Site Recovery Manager need to be restarted so that SRM can see the new adapter. This can be done by either restarting the **VMware vCenter Site Recovery Manager Server** service or rebooting the SRM server.

Step 2: Connect Using VMware vSphere Client

1. Now that SRM and the Array storage adapters are installed, connect to the environment using VMware vSphere Client. Install and configure the SRM Plug-in for each client being used to manage SRM.

2. From the file menu click on **Plug-ins** and then **Manage Plug-ins**. Choose the vCenter Site Recovery Manager Plug-in to install. This will need to be done on any vSphere Client that is used to connect to the environment in which management of SRM is also needed.



3. For more information consult the *SRM Administrator Guide* from VMware.

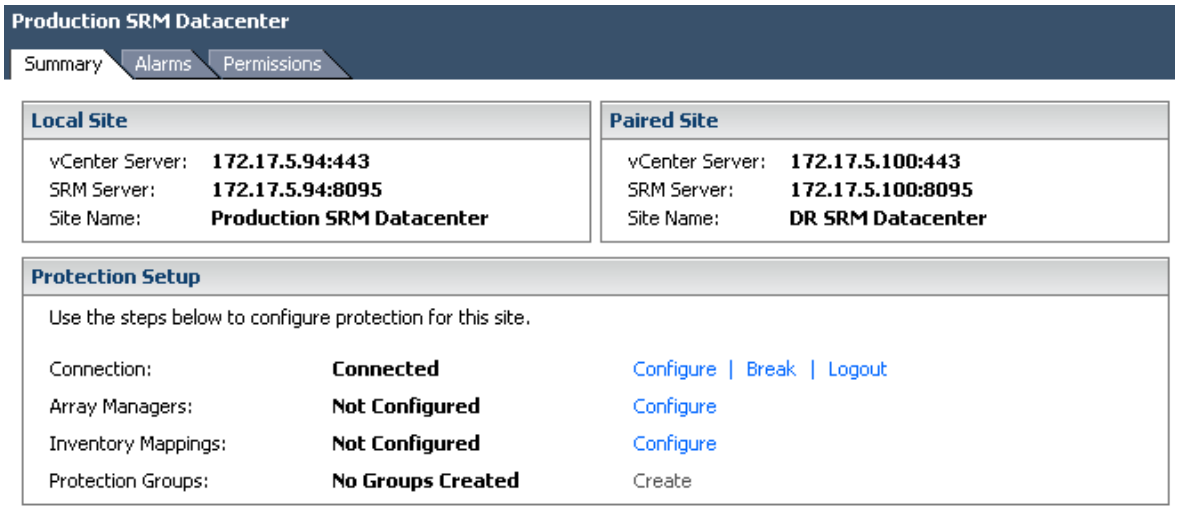
Step 3: Configure Site Recovery Manager Connection

1. Just as the PS Series SAN needs to have a partnership established for replication, vCenter Site Recovery Manager needs to have a partnership established between the protected site and the recovery site.

2. To get to the SRM configuration screen select **Home**. Then under Solutions and Applications click **Site Recovery**.

3. From the Protection Setup section of the SRM Plug-in screen in the GUI click **Configure** next to Connection. Put in the hostname or IP address of the SRM server at the recovery site and it will go through and establish the partnership.

4. This is covered in more detail in the *SRM Administrator Guide*, but when it is configured it will look similar to the following example. This partnership is only established once and SRM will take care of configuring both partners to see each other.



5. From the example screenshot, it can be seen that the protected vCenter server and protected SRM server are on the same system, 172.17.5.94, this was given the site name of Production SRM Datacenter. On the recovery site the vCenter server and SRM server reside on 172.17.5.100, and the site name is DR SRM Datacenter.

Step 4: Configure Array Managers

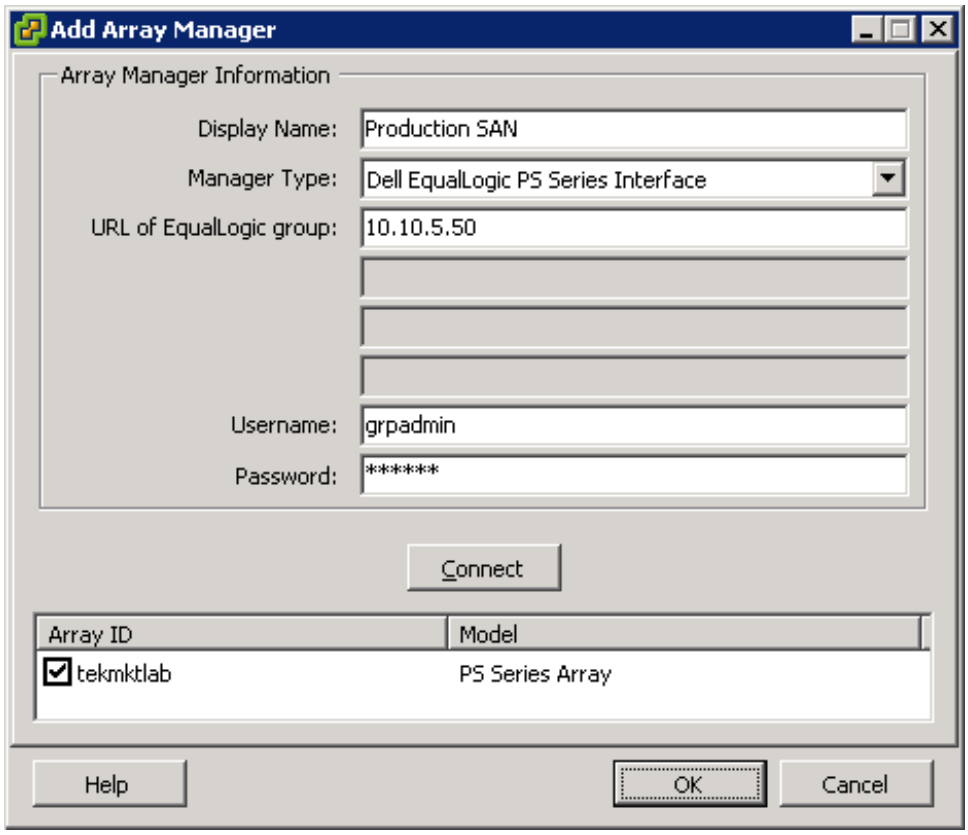
Once the SRM partnership between the two sites is established the Array Manager needs to be configured. This is only done on the protected site unless there is bi-directional replication. If so, the steps are the same with the roles being reversed.

NOTE: Even if there is only one way replication, the storage replication adapter must be installed on both the protected site and recovery site. When configuring the array manager on the protected site it needs to communicate to vCenter at the recovery site which needs to be able to see the recovery site array.

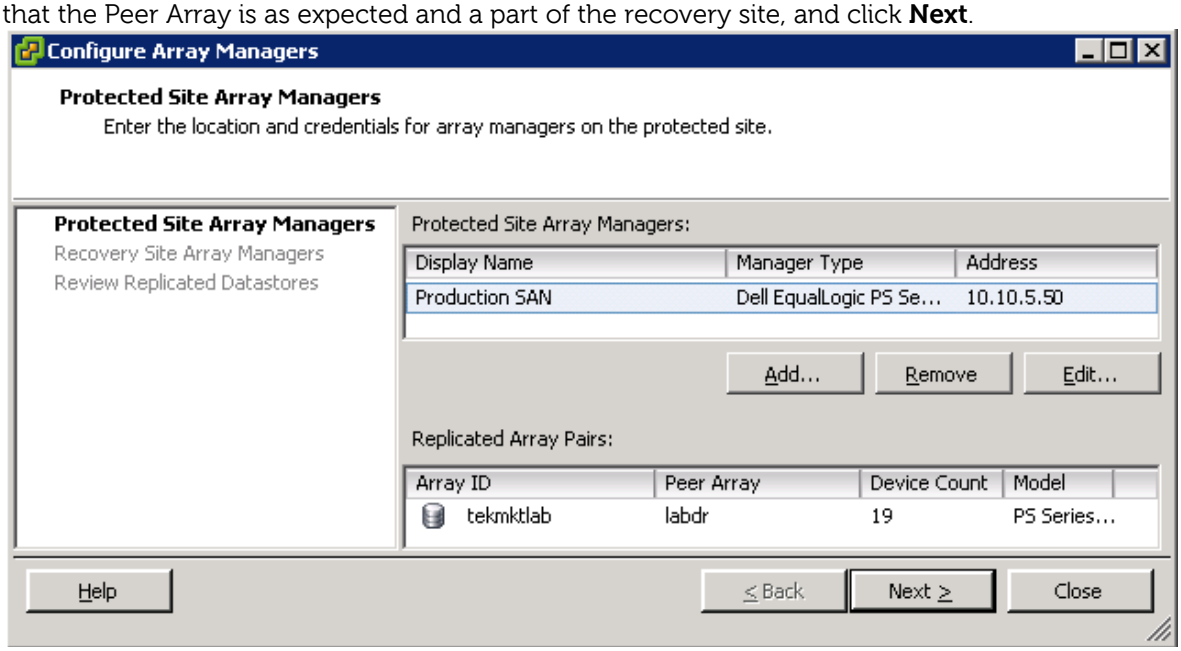
1. Next to Array Managers click **Configure**.

2. Under Protection Side Array Managers click **Add**.

3. Enter in a Display Name and the IP Address of the PS Series group. Enter in the group administrator username and password and click **Connect**. This will go out and scan the array to gather information about it. This will populate array ID with the group name. Click **Ok** to continue.

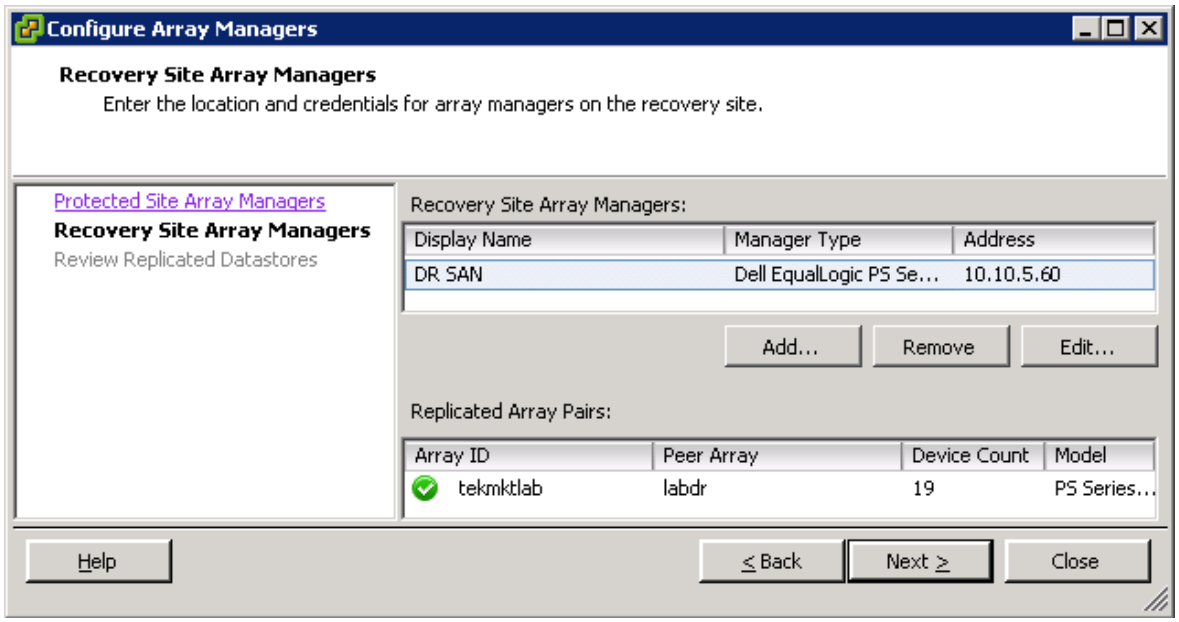


4. This will show the protection site array, its peer array at the recovery site, as well as the number of replicated volumes on the array. The replicated volumes do not necessarily match with just VMware datastores but all replicated volumes in this PS Series group. VMware will scan these volumes later to see which ones are valid datastores. Verify that the Peer Array is as expected and a part of the recovery site, and click **Next**.

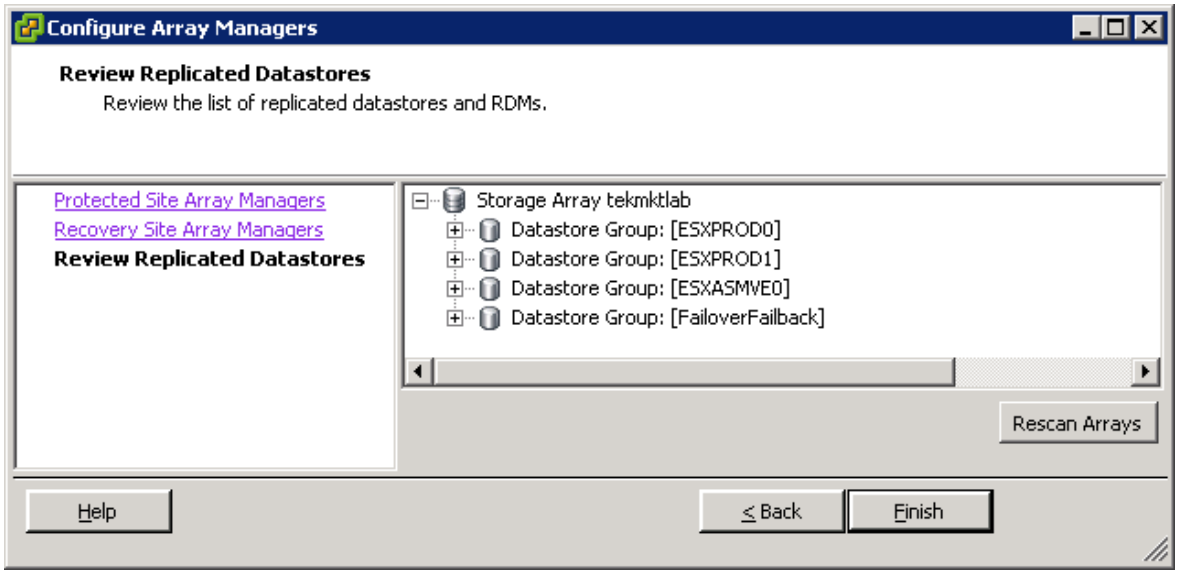


5. The next screen is configuring the Recovery Site Arrays. Select **Add** and enter the information for the recovery site group. When this is done click **Ok**.

6. Site Recovery Manager will scan the arrays and make sure they meet the necessary requirements of having replication configured, having the volumes configured for replication, and having replication schedules. There will be a green check mark when this is done. Click **Next** to continue.

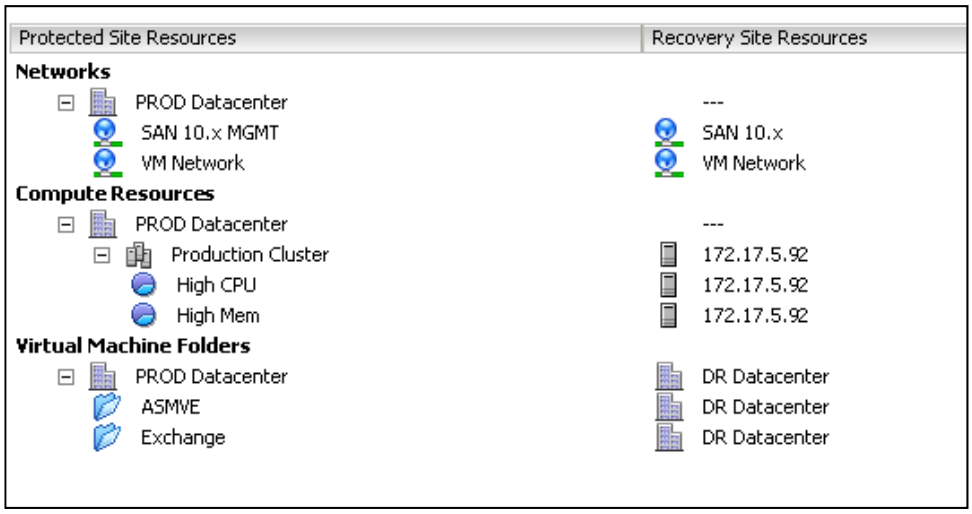


7. SRM will then scan the SAN and match up the VMware datastores with the matching SAN volumes. If the volumes can be protected it will list them in the Replicated Datastores screen. SRM will also group datastores together if they contain VMs that span multiple volumes. Review the list of replicated datastores and click **Finish**. This completes the configuration of the Array Managers. Anytime there are changes to the number of replicated and protected volumes, you should re-run the Configure Array Managers and click **Rescan Arrays** button on the third screen.



Step 5: Configure Inventory Mappings

Inventory mappings are global settings that match the protected site resources with the recovery site resources. This can be used to match data centers, resource pools and networks on the protected site with data centers, resource pools and networks on the recovery site. This enables administrators to guarantee that broad configuration choices that are made in the protected site match up on the recovery site when a failover occurs. These global settings can be overwritten at the individual VM level during the creation of the protection group. Consult the *SRM Administration Guide* on how to configure the inventory mappings for SRM. This can then be used to match networks, hosts, resource pools, and folders from the protected site to the recovery site for testing and failover. Below is an example of Inventory Mapping.



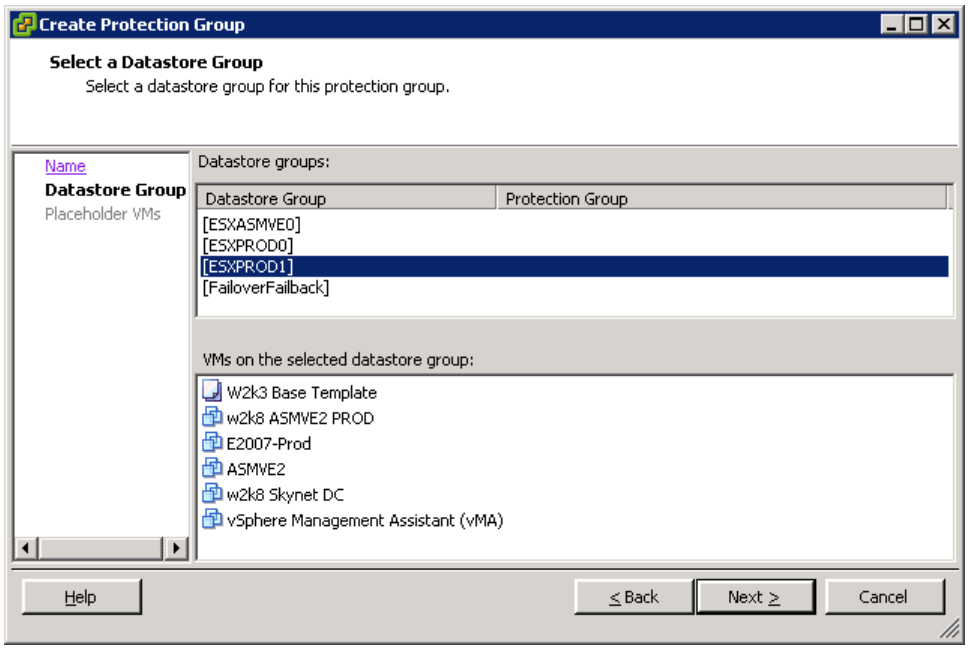
SRM PROTECTION GROUPS

A protection group is a datastore volume or group of datastore volumes that contain virtual machines that need to be protected. A protection group is configured on the protected site through the VMware vCenter GUI. More detailed information can be found in the *SRM Administration Guide*, but the following is an example of the steps taken:

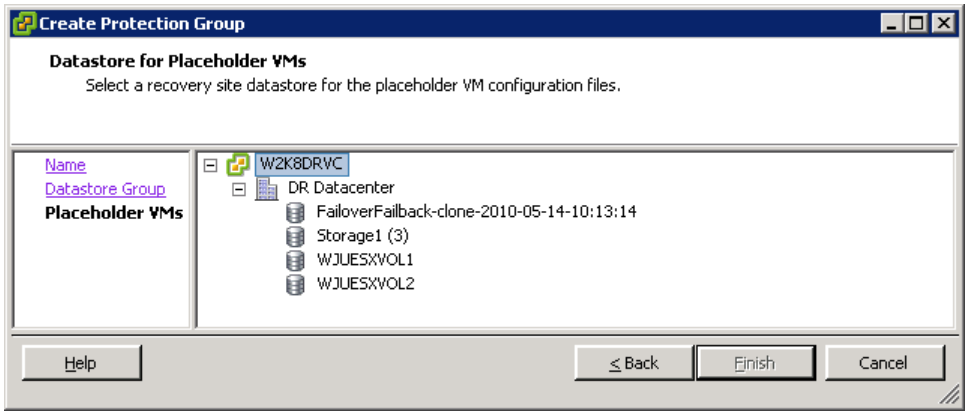
1. From the vCenter Client logged into the protected site click on **Home-> Solutions and Applications->Site Recovery**. Select **Protection Groups** and click **Create Protection Group**.

2. Give the new protection group a name and click **Next**.

3. The next image shows a list of replicated datastores from earlier in the configuration. Selecting a datastore will list the VMs that reside on that datastore. SRM will group datastores together if a VM spans multiple volumes to protect them. If a Datastore Group is already involved in a Protection Group, it will be listed to its right. Select a datastore group and click **Next**.



4. Choose a location to store the recovery placeholder VM configuration files. This is a datastore on the recovery site. There does not need to be much space allocated here as it is just a temporary space to hold the small .vmx and other configuration files. It is suggested to use a volume that is shared among all of the recovery ESX servers. Click **Finish**. SRM will communicate with the recovery site and add the VMs from the protection group to the recovery site inventory.



5. Follow this same procedure for every datastore group that needs to be protected. Each datastore, or datastore group if a VM spans multiple volumes, is configured individually.

6. More detailed explanation of modifying the protection group can be found in the *SRM Administration Guide*. There are many options including recovery priority, customization of individual machines, pre- and post-power on scripts and many other options. The power of SRM lies in the ability to modify each VM for recovery and testing, and then testing these changes without impacting the production environment.

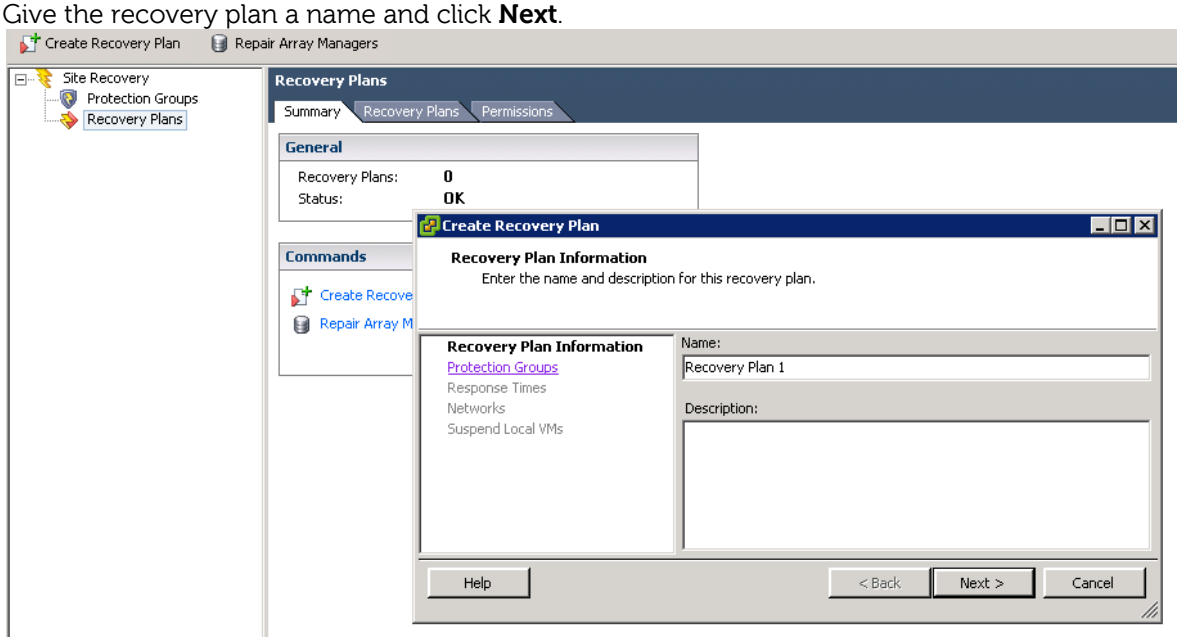

Site Recovery
Protection Groups
Protection Group 1
Recovery Plans
Protection Group 1
Summary
Virtual Machines
Permissions
Configure All
Configure Protection
Remove Protection
Repair All
Name
Status
Folder
Compute Resource
Network
W2k3 Base Template
OK
DR Datacenter
SAN 10.x, VM Network
w2k8 ASMVE2 PROD
OK
DR Datacenter
172.17.5.92
SAN 10.x, VM Network
E2007-Prod
DR Datacenter
172.17.5.92
SAN 10.x, VM Network
ASMVE2
DR Datacenter
172.17.5.92
VM Network
w2k8 Skynet DC
DR Datacenter
172.17.5.92
SAN 10.x, VM Network
DR Datacenter
172.17.5.92
VM Network
Configure All
Configure Protection
Remove Protection
Repair All
Refresh

RECOVERY PLANS

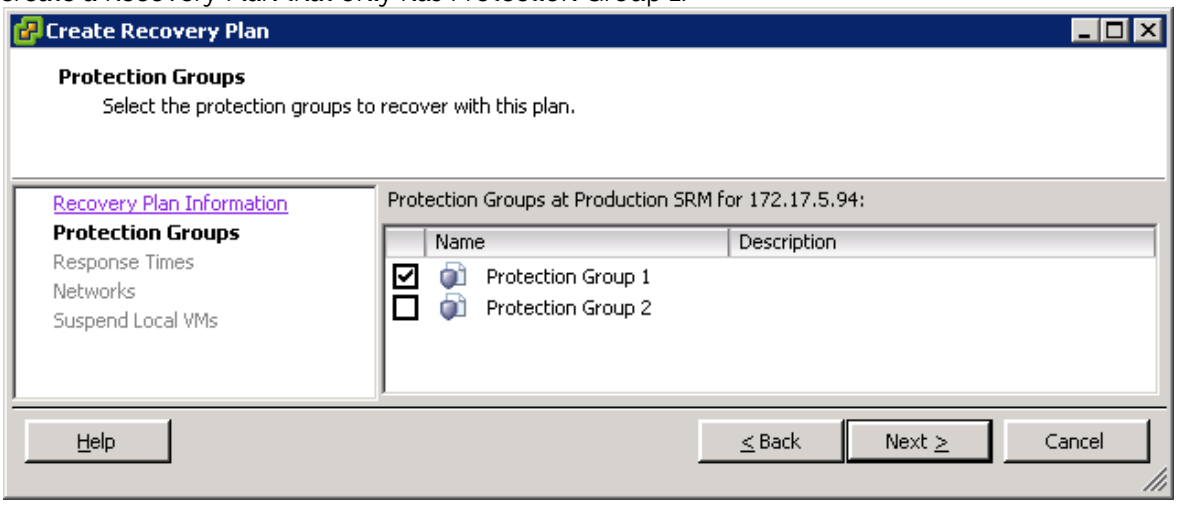
A recovery plan is a run book plan to facilitate and automate the process of testing and failing over virtual machines. The recovery plan is created on the recovery site and can encompass one or all of the protection groups that were created on the protected site. This allows administrators to configure various test scenarios and to run these tests. It also allows for more comprehensive full site failover situations to be run. More detailed information can be found in the *SRM Administration Guide*, but the following is an example of the steps taken.

1. From the vCenter Client logged into the recovery site vCenter GUI click on **Home-> Solutions and Applications->Site Recovery**. Select **Recovery Plans** and click **Create Recovery Plan**.

2. Give the recovery plan a name and click **Next**.

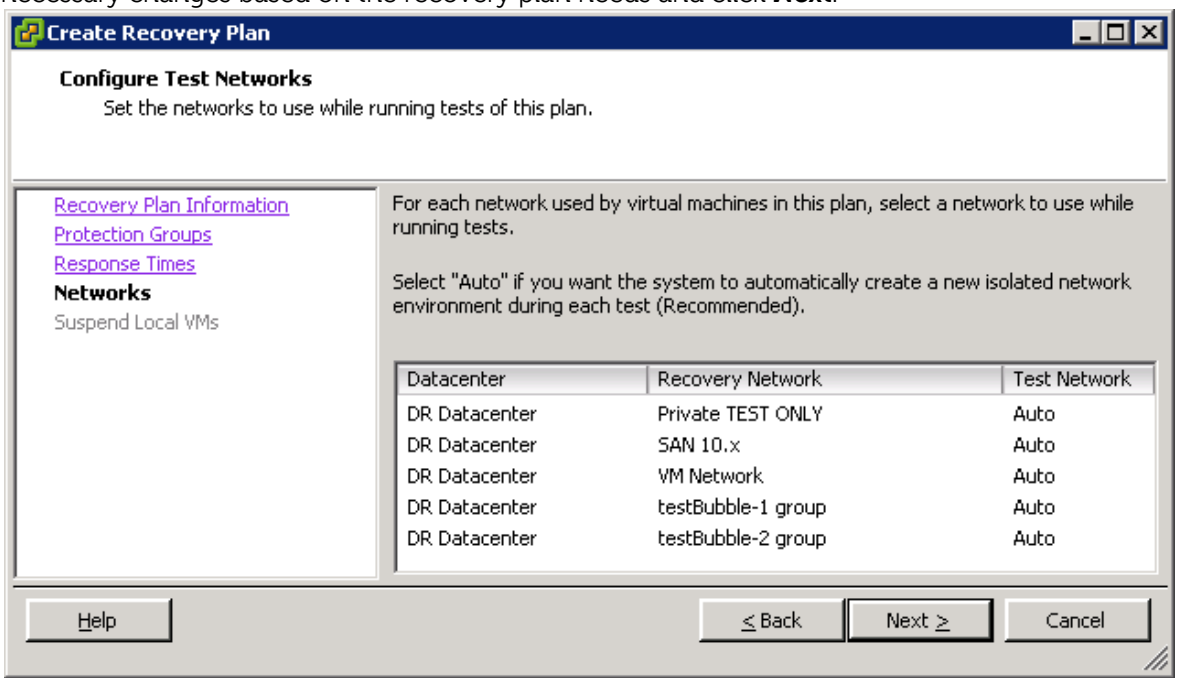


3. Select the protection groups that are to be a part of this recovery plan and click **Next**. The benefit of Recovery Plans is that multiple plans and protection groups can be configured to account for various testing and failover procedures. For example, you can create a Recovery Plan that incorporates Protection Groups 1, 2 and 3 and then also create a Recovery Plan that only has Protection Group 1.



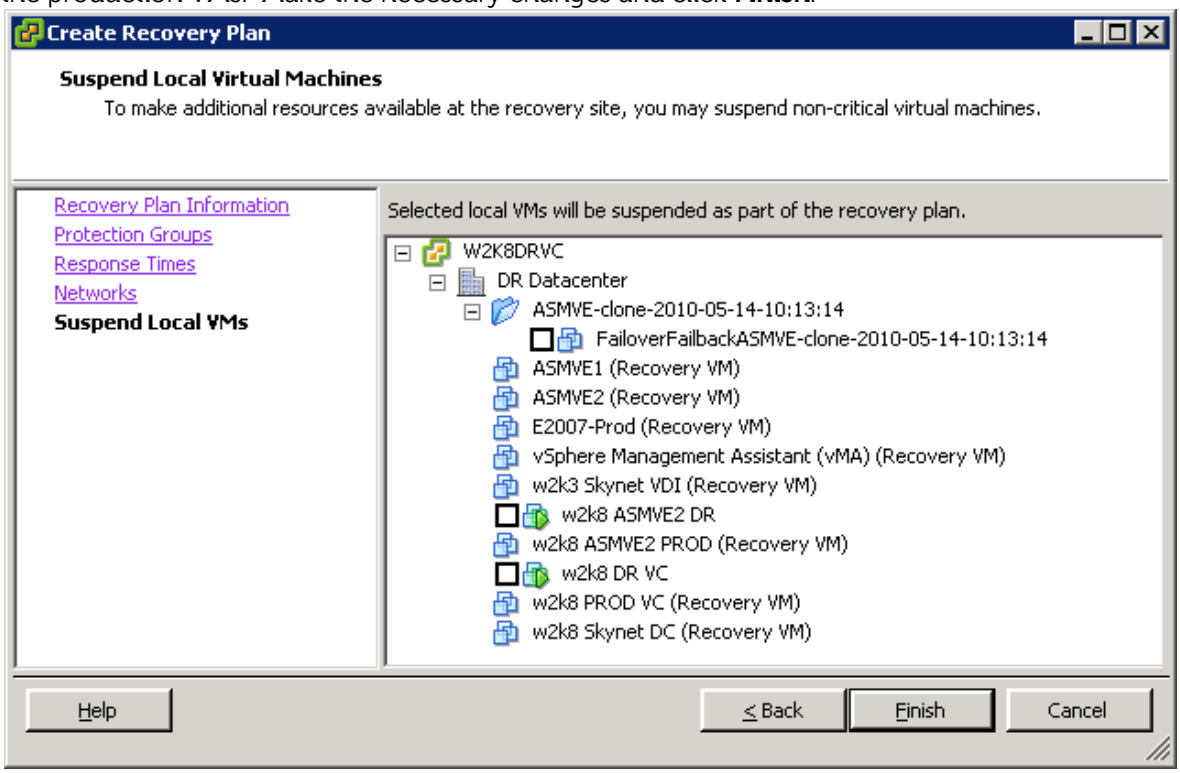
4. The next screen prompts for timeout values for when the VM powers on and VMware Tools gives the heartbeat. This can be modified based on the environment, keeping in mind that the default is 10 minutes per VM that does not have the tools installed. SRM will power up each VM sequentially based on priority level on each separate host and wait for this timeout value to pass.

5. The next screen allows for the configuration of the network settings based on the test run. The default is auto. SRM will create an isolated test bubble network and assign all of the VMs in the recovery plan to this bubble. This is to insure that the test environment does not impact or conflict with the production VM environment. There will be some instances when it makes sense to change the Test Network to something other than Auto. For example you may have an isolated test network with client machine VMs or an existing test that needs to communicate with a new test. Make the necessary changes based on the recovery plan needs and click **Next**.



6. The last screen shows a list of currently running VMs. VMs can be suspended during the recovery plan to free up memory and CPU resources on the hosts. Many environments use their DR infrastructure as a test or development environment and these VMs may need to be suspended during a test or failover to free up resources for

the production VMs. Make the necessary changes and click **Finish**.



7. There can be multiple recovery plans configured with multiple scenarios. The benefit of SRM is the ability to not only configure multiple recovery plans but to also test them to assure they meet the organization's needs. Once there is at least one recovery plan, testing can begin.

TESTING

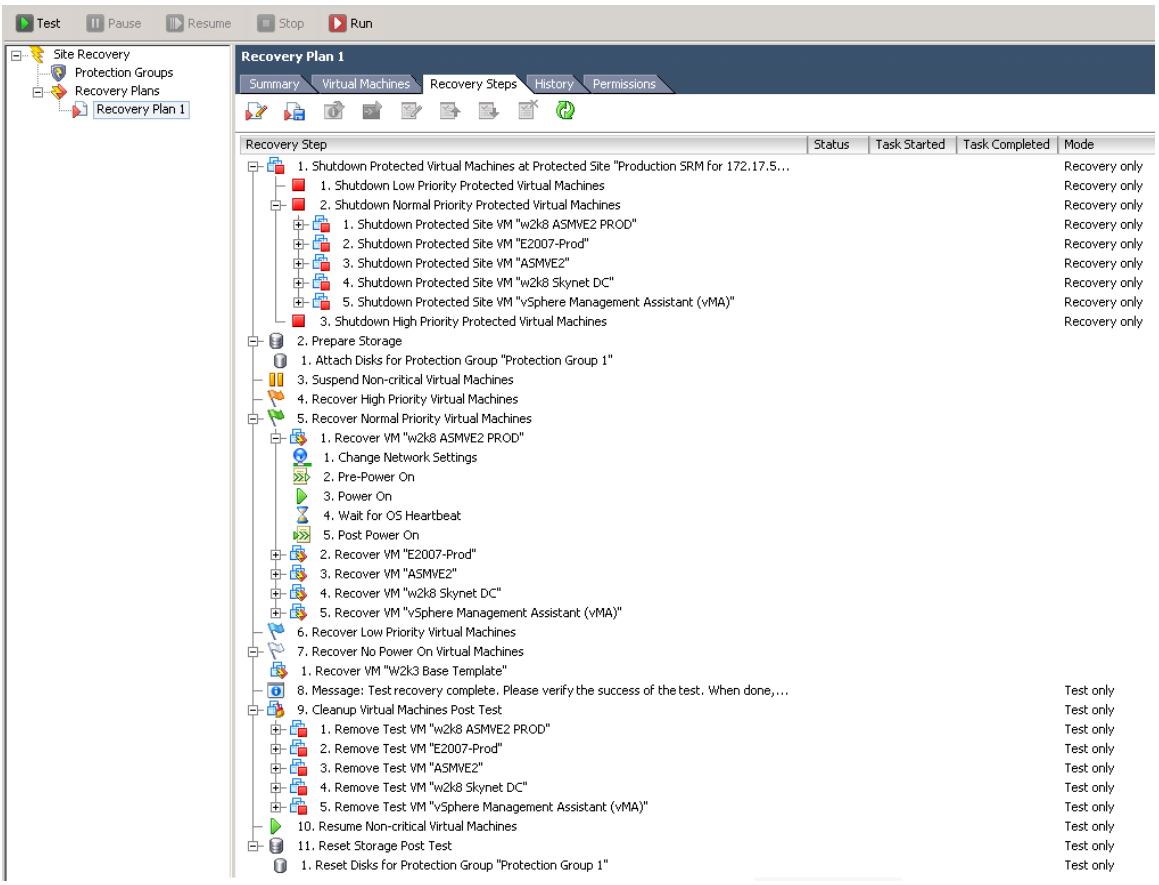
One of Site Recovery Manager's greatest attributes is the ability to test the recovery plan before there is a failure. This allows administrators the ability to tune their recovery process and make sure that the plan is sound in the case of an actual failover. It also allows for comprehensive auditing of the recovery plans without impacting actual running virtual machines.

A test failover scenario is designed to completely limit impact onto the production VMs and Datastore volumes. When a test is run on the recovery site the recovery group is told to create a clone of the replica volumes and bring the clones online. SRM will send the iqn information from the ESX hosts to the SAN group to add to the access control list. Since it creates a clone of the replica, at no time is the production replication impacted. However, there needs to be extra free space in the group in order to create a clone and bring it online. If there is not enough free space the clone operation will fail and the test will fail with an error of not being able to see the Datastore volumes.

Once the clone is created and brought online, SRM will rescan the storage at the ESX host level. It will resignature the volume as needed to be able to bring that clone online as a new Datastore.

SRM will then re-register the Recovery VMs to point to the new clone volume and start powering them up in the order specified during the creation of the Protection group and Recovery plan. During the testing phase SRM will isolate the VMs based on the testing network setting that was configured earlier. By default it will create a Test-Bubble virtual switch with no external NIC connections. Again, this is done along with everything else to protect the production environment.

1. To start the test, log into the recovery site with the vCenter Client. Click on **Home-> Solutions and Applications->Site Recovery** and expand out the **Recovery Plans**. Click the Recovery Steps tab to see the run book of the particular plan.



2. There are two buttons, Test and Run. Click **Test** to start.

3. The progress of the test will fill up the Recovery Steps screen. It will go through and prepare the storage by creating the clones, bringing the clones online and rescanning the storage subsystem, re-registering the VMs, and bringing them online according to the plan.

4. Once the entire Recovery plan has been run it will pause with a message. At this point you can see if the test was successful by logging into the console of various VMs. Because of the isolated network there may be some limitations to the things that can be done inside the VM, such as mapped drives or connections to iSCSI volumes. These are all processes to be tested and documented in the case of a true failover. If there was an error you can troubleshoot the issue and correct the error and re-run the test.

5. Click **Continue** to finish the test and clean up the environment. SRM will unregister the VMs, re-register them to point towards the temporary Datastore, and remove the isolated test network. It will then unregister the storage from ESX and delete the clone volume, freeing up that space and refreshing the ESX storage subsystem. Within a few minutes the recovery site environment will be back to the way it was before the test was run.

   This process allows for not only the fine tuning of the DR recovery plan, but also testing any time without having to bring the production environment down.

FAILOVER

In the case of a full site failure or simply wanting to fail over individual protection groups, running the recovery plan follows a different process flow. The first thing SRM will do is see if it can communicate with the protected site vCenter Server. If it can, SRM will shut down any VMs on the protected site to make sure they are not online on both sites. When running the recovery plan, instead of making a clone of the volumes, replication is paused on the SAN and the replicas are promoted with the ability to be demoted. SRM will send the same IQN information so that the access control list can be populated with the ESX server information.

Once all the replicas are promoted, ESX will rescan all of the storage adapters and bring the promoted volumes online as storage.

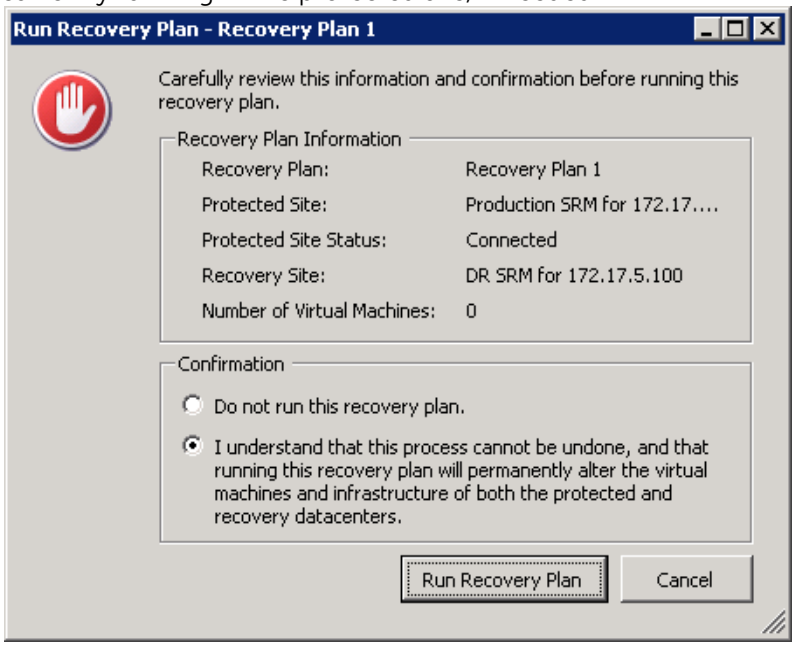
SRM will then re-register the recovery VMs to point to the newly promoted volumes. Unlike a test though, the network configuration will be changed to match the recovery settings so the Test-Bubble virtual switch will not be used. Each of the VMs will power on based on their priority level and the rest of the recovery plan will run.

Once the entire recovery plan is complete, the virtual environment will now be up in production on the recovery site.

The volumes that were promoted are not fully promoted volumes. They retain the ability to be demoted to utilize the fast failback procedure on the group. Because the promotion is not permanent there are a few features that cannot be done on the volume, such as renaming it or resizing it. At any point you can make the promotion of the volume permanent.

The failover process will also pause the inbound replication of any volumes on the recovery site. If the array is a replication partner from another site, be sure to re-enable the replication as needed.

1. To start the full recovery click the **Run** button. This will pop up a warning. This action will invoke the entire failover for that recovery plan including powering off VMs that are currently running in the protected site, if needed.



2. If you are certain, click **Run Recovery Plan**. This will start the process and after some time the entire production environment detailed in the recovery plan will be online at the recovery site.

Planned Failover

For a planned failover, in the event of an expected outage at the protected site, there are two additional steps that should be completed prior to running the SRM recovery plan to ensure that all of the data is in a clean and consistent state on the DR site.

1. From the vCenter Client logged into the protected site, shut down the virtual machines that are in the protection group to be failed over.
2. From the array group manager select the volume or volumes that make up the protection group and click **Replicate to partner** to perform a final replication. Do this for each protection group that is part of a Recovery Plan to insure the latest clean shutdown state of the virtual machines is replicated.
3. Run the SRM recovery plan, as detailed in this document.
4. Repeat these steps for each Recovery Plan and any Protection Groups associated with it.

FAILBACK

Failback is the process to bring all of the VMs that are running on the recovery site back to the original protected site after a full recovery plan has been run. There can be multiple reasons for enacting the full recovery plan and moving production VMs from the protected site to the recovery site; anything from power outage, equipment outage, planned migration, to a true disaster. In each of these cases, careful consideration must be given to bringing the existing environment back onto the original protected site.

Site Recovery Manager does not automate the failback process. With careful planning, bringing the recovery site virtual environment back into production on the protected site can happen with very little downtime, of which that downtime is planned.

Regardless of the reason that the recovery site is now servicing production VMs, there are two basic scenarios for utilizing failback: the SAN on the protected site is still in production and has some subset of data from the production environment before the failover; or the SAN is completely new, either because it is new hardware or has been re-initialized. There may even be an instance where each of these techniques is used, depending on the reason for failover.

During the discussion, the role of protected site and recovery site will change; so to keep things straight, this section will discuss Site A as the original protected site with data in production and Site B as the original recovery site that was failed over to.

Utilizing PS Series Array Fast Failback: Used to update the original site with changes since failover occurred

The first example of configuring failback assumes that the original virtual environment is still in place and the SAN still contains a subset of production data. There may have been a building power outage or something similar which caused the production environment to be brought up on the recovery side. In this case, the PS Series Fast Failback option can be used to replicate only the new changes back to the production SAN.

Array based Fast Failback is supported with PS Series Firmware 3.x and above. See appendix A for instructions on fast failback with firmware 4.x. The following contains instructions on using fast failback on array firmware 5.x. Since SRM leaves the replicated volume in a promoted but not permanent state, administrators can take advantage of the fast failback feature to send changes from the DR site back to the production site.

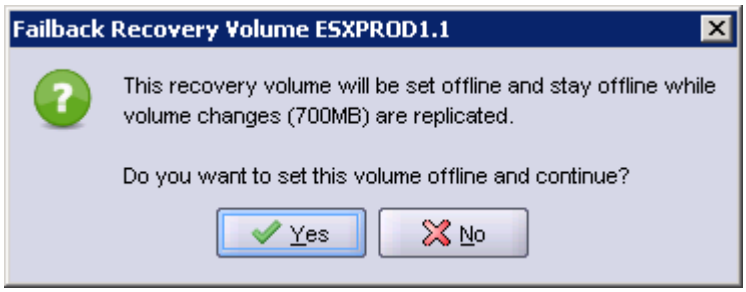
Controlled Failback

A controlled failback is when the administrator has the time and ability to schedule downtime and prepare for failing back from Site B to Site A. Administrators can take their time devising a strategy in which to migrate back to Site A with all of the current data that was written since the failover occurred. Because failback is done at the volume and datastore layer, administrators need to ensure that all of the VMs that reside on the volume are shut down to insure data consistency. Also, if there are VMs that span multiple volumes, all of these volumes need to be failed back at the same time to guarantee the VMs operation back at Site A.

1. In order for PS Series Group Fast Failback to work, the Site A production volume cannot have any active connections. If there are ESX servers attached to the production Site A volume, you need to either set the volume offline in the Site A Group Manager UI, or shut down the attached ESX servers.

2. Using the vCenter client at Site B, shutdown the failback VMs.

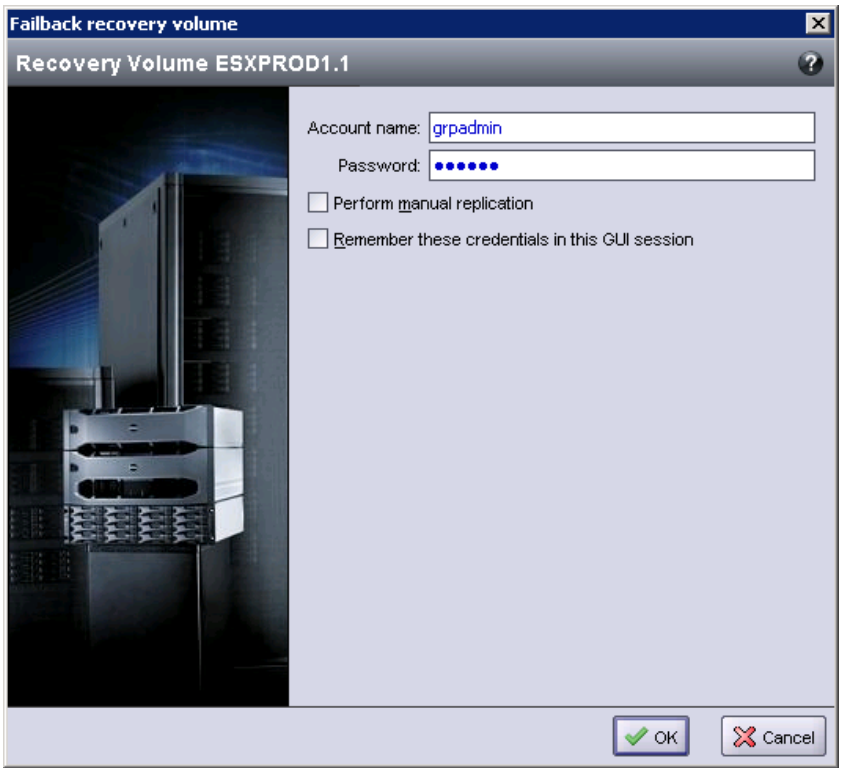
3. Then from the Site B Group Manager UI select the volume or volumes to be fast failed back and in the **activities** tab select **Failback to Primary**. Since data has changed it will warn and ask:



Click **Yes** to proceed. This will take the volume offline, and ESX servers at Site B that were accessing it will no longer be able to see the VMs on the volume. The VMs will need to be removed from vCenter inventory as part of the post failback cleanup.

4. Enter in account credentials for managing volumes on the Site A group. In addition, administrators have the option to perform a manual replication using the Manual Transfer Utility. This can be done if the data change is quite large and exceeds the bandwidth between sites. For more information on using the MTU refer to the *PS Series Group Manager Administrator Guide*.

5. Enter in all the information and click **OK**.



6. To monitor the replicate to partner operation and make sure all tasks complete, open the Alarms panel at the bottom of the Site B group manager GUI window and click the **Failback Operations** tab. This replication process will replicate all of the changes back to the original volume and set the volume online.

7. Once the volume is back online, depending on the state of the vCenter environment you may need to rescan the datastores, possibly re-register the VMs and then bring them back online. Since the VMs were cleanly shut down prior to the controlled failback, they will be able to be brought online as if they were just shut down locally.

SRM in Reverse: Used when all the data needs to be recovered at the original site

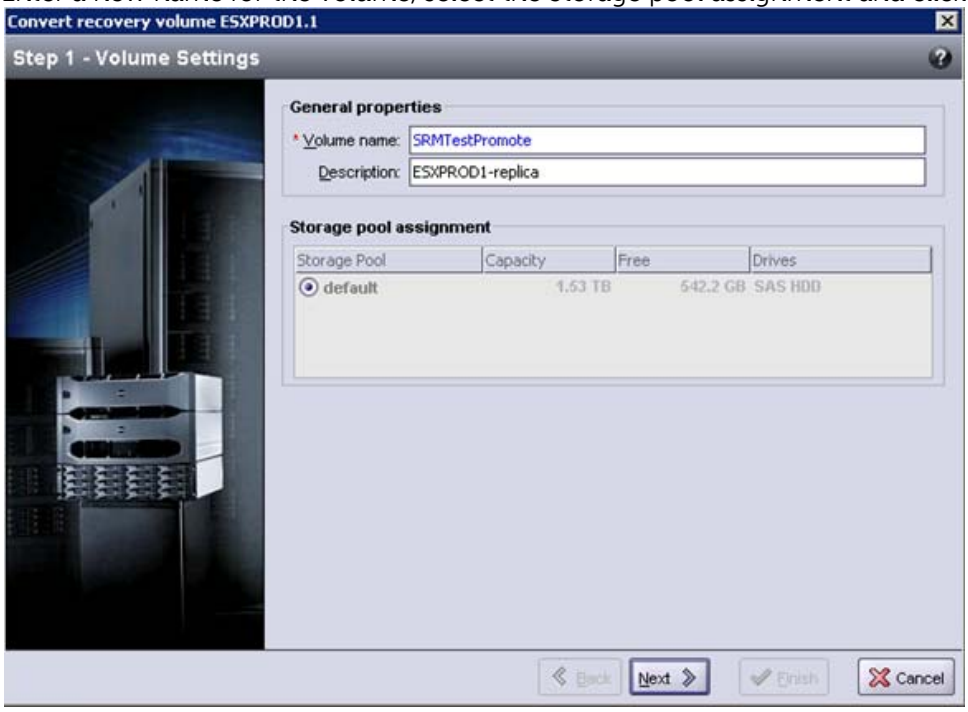
If the SAN on the original protected site (Site A) is considered a new production environment with no prior data residing on it, the failback process will be much like configuring SRM in the beginning with the recovery site (Site B) now taking on the role of the protected site and the old protected site (Site A) temporarily becoming a recovery site.

In this scenario there are a few steps that must be performed on the SAN before starting the process to failback.

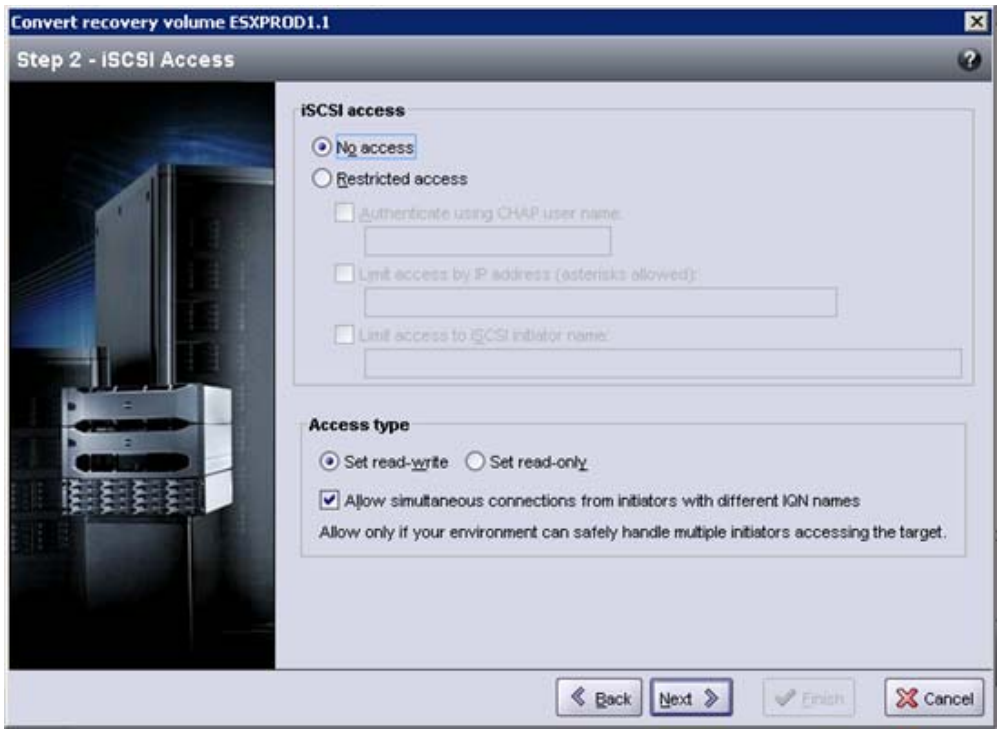
Make Promotions Permanent

1. During the full recovery the replicas on the recovery site (Site B) were promoted with the ability to fail back. Since there is nothing to fail back to, these volumes need to be promoted permanently to reverse the replication process. Select each volume that was promoted during the recovery process. In the **Activities** tab click **Make Promote Permanent**.

2. Enter a new name for the volume, select the Storage pool assignment and click **Next**.



3. In Step 2 you can add an additional iSCSI access. The volume was already given the access control list from SRM when the volume was promoted. *Note that if you select No Access it does not remove the existing access list.* Choose No Access or add another access control and click **Next**.



4. Verify the settings are correct and click **Finish** to make the promotion permanent. Once this is done the volume cannot utilize the Fast Failback option and any failback must include the reconfiguration of replication to the other partner group.

5. Do this step for all volumes that were promoted during the SRM failover.

6. Now that the volumes have been promoted, treat this as a new configuration for SRM with the failover site becoming the new protected site and the original protected site becoming a temporary recovery site.

Configure Replication Partnership

Since this example assumes that there is no partnership established between the current protected site (Site B) and the new recovery site (Site A), re-create the replication partnership as detailed earlier. If the new group will have different group information, delete the current partnership that exists on the currently running site (Site B) and re-create it with the new information.

Configure Volume Replication

Configure replication for each of the volumes that were promoted that contain data for the virtual environment. Once the volumes are configured, create a replication schedule for each volume as well.

Create new vSphere Environment

If there is no vSphere environment configured on the new recovery site (Site A), configure vCenter and SRM as detailed earlier.

Configure Site Recovery Manager

Now that this site (Site B) will be used as the new protected site, SRM must be configured. This may have been done if the environment was configured for bi-directional protection. If not, follow the same steps for the protection site (Site A) earlier.

- Install Site Recovery Manager
- Install the Dell EqualLogic SRM Array scripts
- Configure the SRM connections
- Configure the SRM Array Managers
- Configure the SRM Inventory mappings
- Delete any old Recovery Plans

Configure Protection Groups

Once SRM is installed and configured, treat this site (Site B) as a new protected site and configure all of the protection groups and settings to prepare the environment to return to the original protected site (Site A).

Configure Recovery Plans

On the new recovery site (Site A), configure the recovery plans that will be enacted to return the environment back to its original state. Careful planning and consideration need to be done because this will be a controlled failback. Many factors need to be considered depending on the needs of the organization, the bandwidth requirements and downtime requirements. Because this is a controlled failback you will have be able to dictate when machines return to the original protected site (Site A) as well as guarantee their consistency.

Verify the recovery plans by utilizing the test feature of SRM. Make sure everything is configured correctly before beginning the controlled failback.

Controlled Failback

Because this is a controlled failback, you can guarantee consistency in each Virtual Machine by shutting them down and running one more replication. This will replicate the VM in a powered down state so that no new changes will come in. Because replication takes place at the volume level on the PS Series Group, you can dictate how the controlled failback occurs.

- Shut down each guest VM on a volume that is part of a protection group. Make note if the VM is part of a Datastore group for replication.
- In Group Manager select the volume or volumes that are part of the protection group. In the **Activities** tab click **Create replica now**. This will start the last replication. When this is done you have consistent VMs on the new recovery site (Site A).
- Run the Recovery Plan on the recovery site (Site A) and bring those VMs back into production.

Reconfigure Environment

Now that everything is back onto the original protected site (Site A), the same process as before must be used to clean up the environment and make it ready for SRM again.

- Make the promotion of the volumes permanent
- Reconfigure SRM as a protected site including cleaning up old recovery plans
- Reconfigure Protection Groups
- Reconfigure Recovery Plans on the original recovery site (Site B)

- Test Recovery Plans to verify everything is back and the virtual environment is once again protected

INTEGRATION WITH ISCSI CONNECTED VOLUMES

There are many benefits to utilizing the native iSCSI initiator from inside the VM to connect to the storage array. These can include, but are not limited to, MPIO, VSS integration, physical to virtual clustering and snapshots.

One of the difficulties of combining this with SRM is that during a test the VMs that are brought up on the DR site are isolated in a test network bubble. This is for the safety of the production VM and production data. Because VMware encapsulates the VM into a file, there is no difference between booting up a VM on the protected site and bringing it up on the recovery site. This could lead to potential issues not only with duplicate name and IP addresses, but the server will try to connect to the same volumes on the SAN that the production VM has access to. Because of this, advanced techniques and additional steps need to be taken when utilizing guest attached volumes. The same process can be used but in a manual fashion. When bringing up a VM that has guest attached volumes, a clone can be created of the replica just like SRM does. Bringing this clone online and attaching it to a separate test server can validate the data on the replica while SRM validates the VM is configured properly. During a failover there is no isolated network, so promoting the replicas of the guest attached volumes and then attaching them to the VM will work.

TROUBLESHOOTING

Q: I cannot see the PS Series group in the Array Manager list of devices to configure.

A: Verify that the Dell EqualLogic SRM Adapter has been installed and that Java 1.5 or higher is running on each SRM server. Restart the SRM service or reboot the SRM server once these are installed. If running SRM 4 and w2k8 the local instance of SRM java will be used.

Q: I cannot see the recovery site group when I try to configure the Array Manager.

A: Verify that you can access the recovery site Group Manager from both SRM servers. Some DR sites are configured only for replication traffic to be sent.

Q: I cannot see any datastore groups when I try to configure the Array Manager.

A: Verify that the datastores that have VMs on them have been configured for replication in the Dell EqualLogic Group Manager. Verify that they also have a schedule configured and active.

Q: During a test I get a storage error and no VMs come online.

A: During the test process, a clone of the replica is created. This requires additional free space on the recovery site SAN. If there is not enough free space to clone the replica, the clone will not be created and the test will fail.

Q: Unable to see test clones or failover volumes at DR site.

A: SRM/SRA will populate the volume ACL with the iqn of the ESX servers. If using CHAP authentication on the DR site the ESX iSCSI initiator should be set to "Do not use CHAP unless required by target".

Q: Replications are significantly larger then data rate change.

A: A common cause of this is over commitment of the physical memory that the VMs reside on, this causes ESX to page memory to disk, and as it is a protected volume this data is then replicated to DR. This can be resolved by; reducing the amount of memory allocated to the VMs, increasing the amount of memory in the physical hosts, or changing the default location for the VM's swap file to a non-replicated volume.

SUMMARY

In today's virtual datacenter, Customers are currently utilizing the Dell EqualLogic auto replication feature to provide a cost effective disaster recovery solution using manual processes and lengthy and detailed run books. VMware vCenter Site Recovery Manager helps to automate that process and more importantly allows for the testing of these plans to provide a complete DR solution for the virtual environment.

FOR MORE INFORMATION

For detailed information about PS Series arrays, groups, and volumes see the following documentation:

- *Release Notes*. Provides the latest information about PS Series storage arrays and groups.
- *QuickStart*. Describes how to set up the hardware and start using a PS Series storage array.
- *Group Administration*. Describes how to use the Group Manager GUI to manage a PS Series group. This manual provides comprehensive information about product concepts and procedures.
- *CLI Reference*. Describes how to use the Group Manager command line interface to manage a group and individual arrays.
- *Hardware Maintenance*. Provides information on maintaining the PS Series storage array hardware.

The *QuickStart* and *Hardware Maintenance* manuals are printed and shipped with the PS Series array.
They are also located on the documentation CD-ROM that is shipped with the array, along with the
Group Administration and *CLI Reference* manuals and the Group Manager online help.

The Host Integration Tools kit and documentation will be available on the support website (`support.dell.com/EqualLogic`) and on a CD-ROM that is shipped with the PS Series array.

TECHNICAL SUPPORT AND CUSTOMER SERVICE

Dell's support service is available to answer your questions about PS Series SAN arrays. If you have an Express Service Code, have it ready when you call. The code helps Dell's automated-support telephone system direct your call more efficiently.

Contacting Dell

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services might not be available in your area.

For customers in the United States, call 800-945-3355.

Note: If you do not have access to an Internet connection, contact information is printed on your invoice, packing slip, bill, or Dell product catalog.

Use the following procedure to contact Dell for sales, technical support, or customer service issues:

1. Visit support.dell.com or the Dell support URL specified in information provided with the Dell product.

2. Select your locale. Use the locale menu or click on the link that specifies your country or region.

3. Select the required service. Click the "Contact Us" link, or select the Dell support service from the list of services provided.

4. Choose your preferred method of contacting Dell support, such as e-mail or telephone.

Online Services

You can learn about Dell products and services using the following procedure:

1. Visit www.dell.com (or the URL specified in any Dell product information).

2. Use the locale menu or click on the link that specifies your country or region.

APPENDIX A

Configuring Replication for vCenter Site Recovery Manager with Firmware 4.x

VMware vCenter Site Recovery Manager is deployed with two separate PS Series groups that have replication enabled so that the Virtual Machines that reside on the datastores at the protected site are replicated to the recovery site. In order for a datastore to be protected with SRM the following conditions must be met:

- The PS Series groups must be configured for replication
- The volumes must have replication configured
- The volumes must be part of a replication schedule

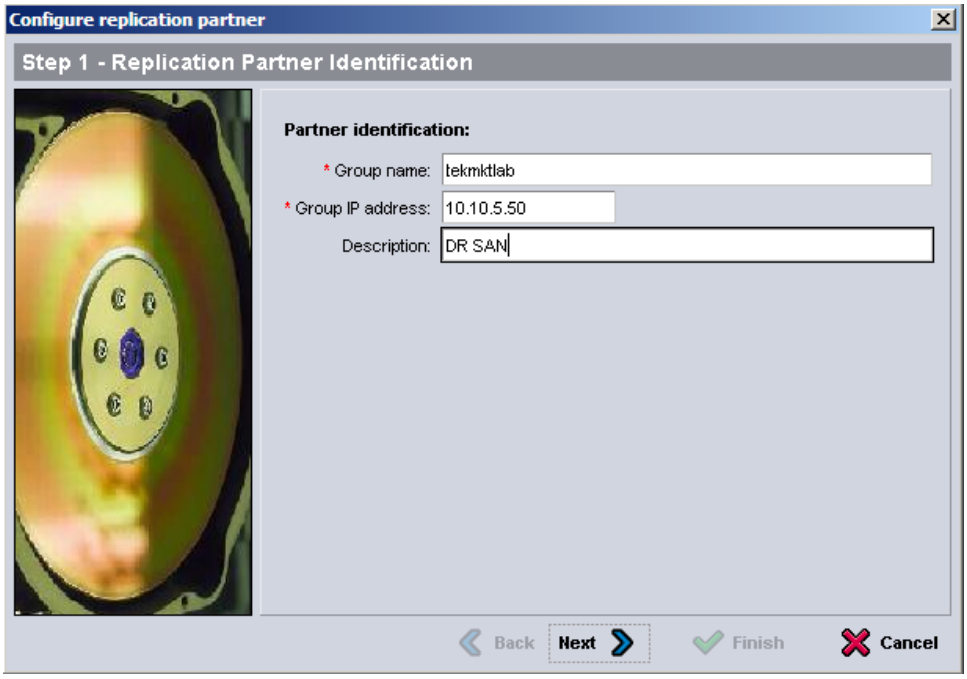
Once these conditions are met the volume will show up as a protected datastore group inside SRM.

Replication capabilities are a standard feature in the PS Series Arrays and are simple to configure. The steps for configuring the replication and configuring the volume are detailed below. More detailed information can be found in the Group Manager under **Tools -> Online Help -> PS Series Group Administration->Managing Data Replication**. These operations are done using the PS Series arrays Group Manager GUI.

Step 1: Configure Replication Partnership between Protected Site Array and Recovery Site Array

1. From the protected site Group Manager click on **Replication Partners** and then under the **Activities** tab click on **Configure partner**.

2. Enter in the **Group Name** of the recovery site (case sensitive), the **Group IP address** and a **description**. Click **Next**.

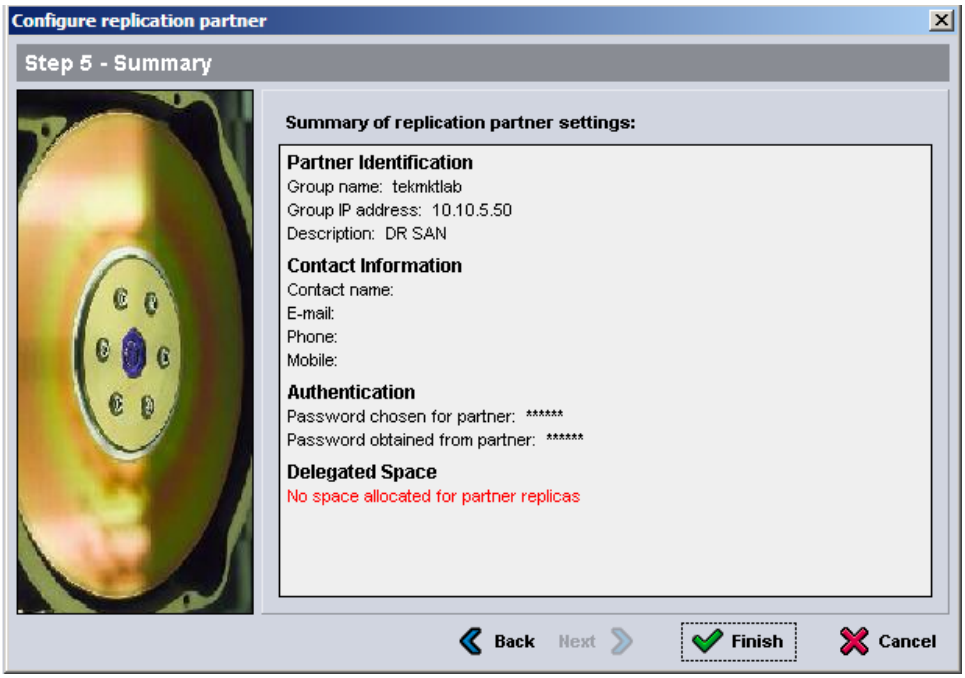


3. Enter in contact information in the next screen and click **Next**.

4. On the next screen there are two password fields. The first field is the **Password for partner**. This is the password that the protection group will give to the recovery group when establishing a connection for replication. The second field is the **Password obtained from partner**. This is the password that the recovery site expects to receive from the partner. Both of these can be the same or different depending on the environment. Enter in the information and click **Next**.

5. The 4th step in the configuration wizard is to configure **Delegated space**. This is space that is created from local free space on the protected site to store replicas from the partner. If there are going to be no replicas sent to the protection site this value can be left at 0. Choose the amount of delegated space, the storage pool which the space will come from and click **Next**.

6. Verify all of the information is correct and click **Finish**.



7. This creates the partnership between the protected site and the recovery site. Now follow the same steps to configure the partnership between the recovery site and the protected site.

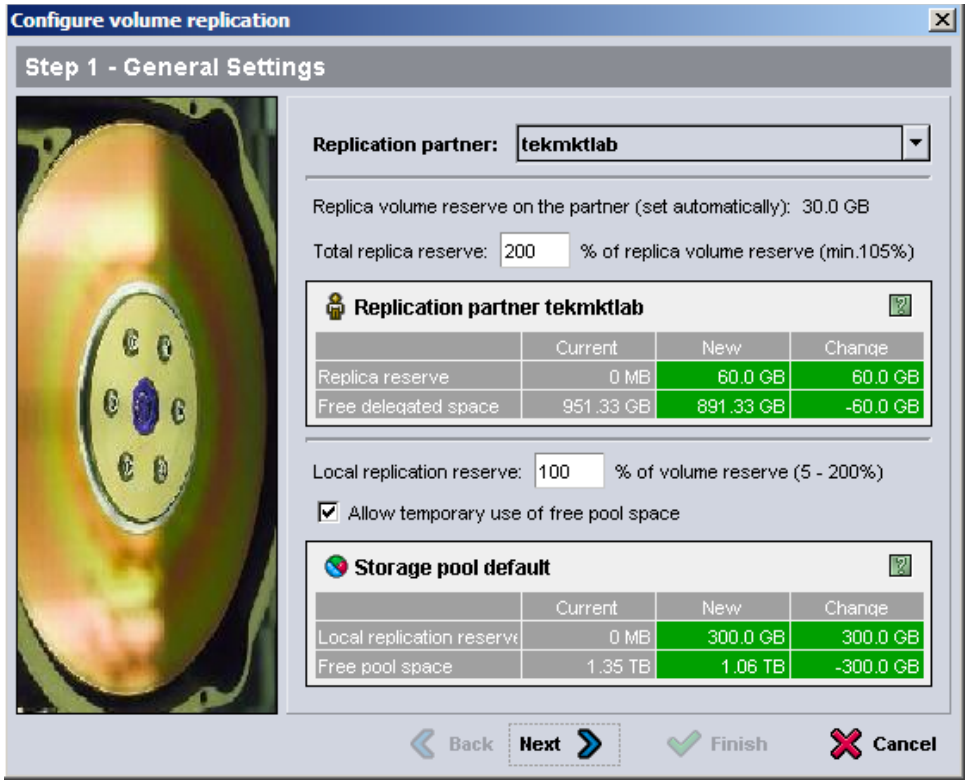
   When configuring the recovery site take into account the number of volumes that are being replicated and the total space. For example, four 200GB volumes with VMs on them being replicated with 200% reserve space plus a little buffer will mean 1TB of delegated space on the recovery site. Choosing how much space to allocate will depend on things such as the number of replicas you wish to keep as well as how much data change is happening between each replica.

Step 2: Configure replication on the Datastore volumes

1. From the protected site Group Manager click on a Datastore volume that you wish to protect. In the **Activities** tab click on **Configure replication**.

2. In the next screen choose the Replication partner that this volume will be replicated to.

VMware vCenter Site Recovery Manager 4 supports only one recovery site, so all Datastore volumes should be replicated to the recovery site that was configured in step 1. Select the percentage of **Replica reserve on the partner**. This is the amount of space on the recovery site that is reserved for this volume to replicate. The default and recommended amount is 200%. The next field is the **Local replication reserve**. This is space reserved on the local group to track replication changes and keeping fast failback snapshots. The default is 100%. There is also a check box to **Allow temporary use of free pool space**. If this is checked then it will use free space to track changes if the local replication reserve is not enough. Choose your options and click **Next**.



3. In the next screen there is a check box to **Keep failback snapshot**. This is not selected by default, but for SRM Failback scenarios this should be checked. This will save time in case of a failover and the protected site is still available to failback to. See the section on Failback for more information. Make your selection and click **Next**.
4. View the summary and click **Finish** to complete the replication configuration. When this is done you will be prompted if you want to create a volume replica now. This is optional, as a schedule will be created in the next part. During this initial replica stage you can use the Manual Transfer Utility (MTU) to configure a manual replica which allows you to move data from one datacenter to another without creating the initial replica over the wire.
5. Configure all Datastore volumes that need to be protected for replication. SRM will not recognize a Datastore as protected until it is configured for replication and has an active schedule configured.

Step 3: Configure Replication Schedule

1. The last thing that needs to be configured in order for SRM to see a Datastore volume as protected is a replication schedule.

2. From the protected site Group Manager click on a Datastore volume that you need to configure a schedule for. This can be done with Volume Collections as well. In the **Activities** tab click on **Create Schedule**.
3. Give the schedule a name and select **Replication schedule**. Make sure it is enabled and click **Next**.
4. Configure the replication schedule that meets the bandwidth and recovery needs for the VMs on that Datastore volume and click **Next**. For more information on Replication considerations, see the *PS Series Administration Guide*.
5. Verify the summary of the schedule and click **Finish**. Follow the same procedure on all the Datastore volumes that need to be protected in SRM.

NOTE: Dell has released a new version of the VMware Integration software titled Auto Snapshot Manager/VMware Edition (ASM/VE) with added support for replicas. This tool has built in integration with VMware vCenter and can also be used to create and run replica smart copy schedules. For more information see Technical Report 1041 Protecting the Virtual Environment using Auto-Snapshot Manager/VMware® Edition.

Once the replication partnership is configured between the protected site and the recovery site, and every Datastore volume that needs to be protected has been configured for replication and has an active replication schedule, you can proceed with the configuration of SRM. These same steps can be done any time if new volumes are added to the virtual environment.