

# Disaster Recovery with Dell PS Series SANs and VMware vSphere Site Recovery Manager

VMware vSphere SRM version 6.5

Dell Storage Engineering  
June 2017

## Revisions

Date	Description
September 2011	Initial release
June 2017	Updated to reflect industry changes

## Acknowledgements

This paper was produced by David Glynn on the Dell EMC Storage Engineering team:

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

© 2011 - 2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

# Table of contents

Revisions.....	2
Acknowledgements.....	2
Executive summary.....	4
1 Introduction.....	5
2 VMware SRM terminology.....	6
3 Overview and prerequisites.....	7
4 Configuring array based replication.....	8
4.1 Step 1: Configure replication partnership between protected site array and recovery site array .....	8
4.2 Step 2: Configure replication on the datastore volumes .....	10
4.3 Step 3: Configure replication schedule.....	12
5 Installation and configuration of VMware SRM .....	14
5.1 Step 1: Install Dell EqualLogic Storage Replication Adapter .....	14
5.2 Step 2: Configure SRM connection .....	17
5.3 Step 3: Configure array managers .....	18
5.4 Step 4: Configure inventory mappings .....	20
5.5 Step 5: Configure placeholder datastore.....	21
6 SRM protection groups.....	22
6.1 Datastore cluster considerations in protection groups .....	24
7 Recovery plans.....	25
8 Testing.....	28
9 Recovery .....	31
10 Failback .....	33
10.1 Recovery scenario 1: Reprotect and failback.....	33
10.2 Recovery scenario 2: Re-establish SRM.....	34
11 Considerations for guest iSCSI connected volumes .....	38
12 Summary .....	39
A Technical support and resources .....	40
A.1 Related resources .....	40

## Executive summary

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

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 entire servers into a series of files that make up the virtual machine; administrators can now take advantage of block storage based techniques such as clones, snapshots and replicas to protect these servers. Dell PS Series arrays offer built-in replication to transfer data, and therefore the virtual machines, from one location to another. Integration software is also provided that combines with VMware vSphere®. VMware vCenter® Site Recovery Manager (SRM) is a suite of tools that help automate and test disaster recovery plans and depends on the PS Series replication to work. By combining these two platforms, administrators now have a manageable way to not only configure, automate, and test disaster recovery plans, but the means to easily run them in the case of a disaster.

This paper details the installation and configuration of VMware vCenter Site Recovery Manager software. As part of this setup, the Dell storage adapter plug-in, the Storage Replication Adapter (SRA), is needed to enable communication from VMware vCenter to the PS Series storage. In addition to SRM configuration and the storage adapter, this document details how to configure replication between sites and how to setup and test a recovery plan. The last section has instructions for performing a full site failover and how to failback when the problems are resolved.

# 1 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 SRM works with the Dell PS Series built-in replication to make disaster recovery rapid, manageable, reliable and affordable. SRM is an add-on feature to vCenter on both the primary and the recovery site. SRM and vCenter at Site A (the Production Site) coordinate with SRM and vCenter residing at Site B (the DR Site) to simplify and automate disaster recovery. SRM allows for automated testing of DR plans, in advance of a disaster, as well as managing the failover and 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 paper discusses the installation and configuration of SRM with the Dell PS Series arrays. It covers 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.

## 2 VMware SRM terminology

VMware SRM has unique terms when discussing DR planning and configuration. Because both SRM and the PS Series storage support bi-directional replication and configuration, it is not sufficient to use the terms *production site* and *DR site*. For example, consider a company with 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, each site is protected from a disaster. If there is a problem in New York, all of the virtual machines previously hosted there can be recovered in Chicago and brought online. The reverse holds true if there is a problem in Chicago. Another example would be an environment that leverages the many-to-one replication of the PS Series array, where multiple satellite offices are each configured to replicate back to a centralized corporate datacenter.

To avoid confusion, 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 VMs must be protected 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.

### 3 Overview and prerequisites

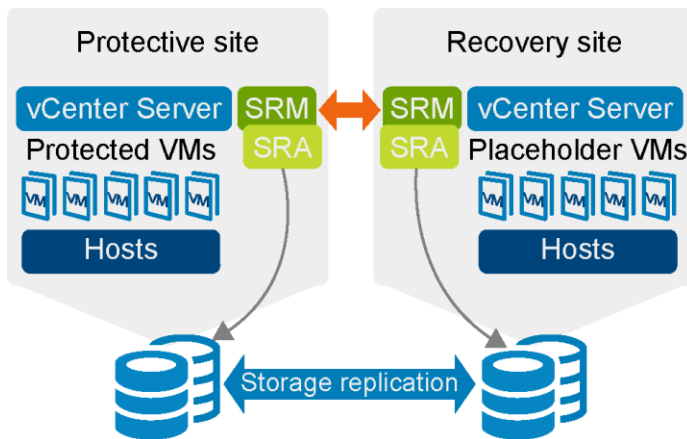
Site Recovery Manager requires VMware vCenter server to be installed at both the protected site and the recovery site. Each site will have its own VMware vSphere environment and datacenters. The SRM configuration is mirrored to the recovery site SRM server so that if the primary site goes down, everything that the recovery site needs to resume operations at the primary site is local.

VMware SRM does not automate or configure SAN storage replication between sites. This needs to be configured by the storage administrator using the storage array management tools (see section 4 Configuring array based replication).

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.

PS Series replication is always configured between two PS Series groups, even if all the SAN members are in the same physical location.



## 4 Configuring array based replication

VMware Site Recovery Manager is deployed with two separate PS Series groups that have asynchronous 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 straight forward to configure. The steps for configuring replication and configuring the volume are detailed below. These operations are done using the PS Series array Group Manager GUI.

**Note:** PS Series Synchronous Replication (SyncRep) and Dell Storage cross-platform replication are not supported with SRM.

### 4.1 Step 1: Configure replication partnership between protected site array and recovery site array

1. From the protected site Group Manager GUI click **Replication management**.
2. Under Replication Partners in the **Activities** tab, click **Configure Partner**.
3. Enter the **Group name** of the recovery site (case sensitive), the iSCSI **Group IP address** and a **Description**. Enter the contact information, and click **Next**.



Configure replication partner

1 - Replication Partner Identification

> 1 - General

2

3

4

Partner identification

\* Group name:

\* Group IP address:

Description:

Contact information

Name:

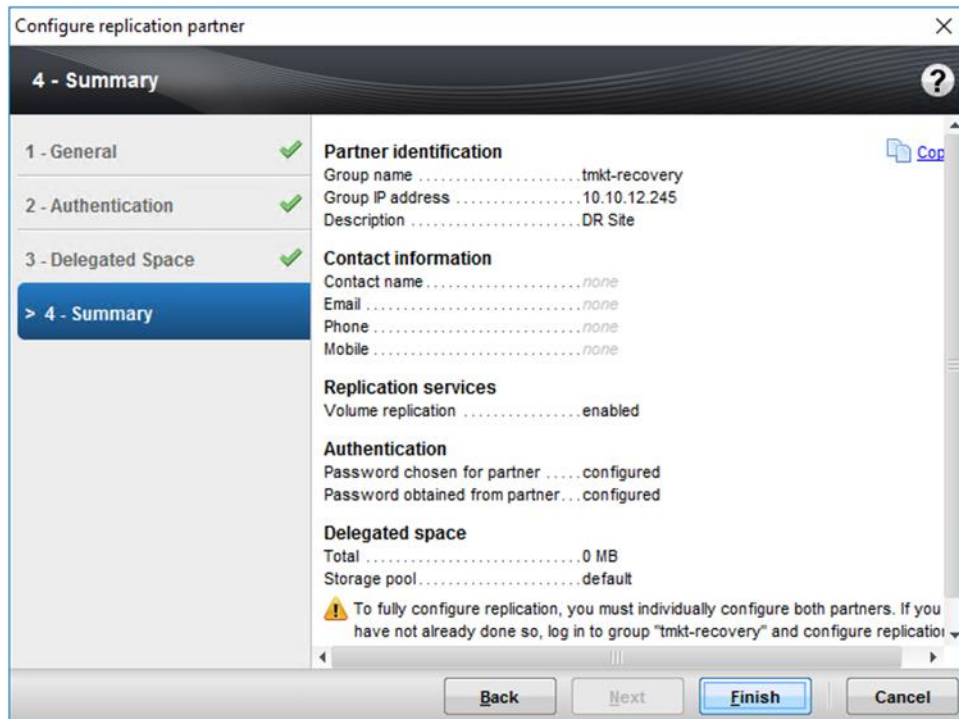
Email:

Phone:

Mobile:

Back Next Finish Cancel

4. On the next screen there are two password fields. The first field is the inbound password. This is the password that the protected group will give to the recovery group when establishing a connection for replication. The second field is the outbound password. This is the password that the recovery group expects to receive from the partner. These passwords do not need to be the same, and are set by individual group administrators. Enter in both passwords and click **Next**.
5. The next step in the replication configuration wizard is to specify delegated Space. This is space that is reserved from local free space on the protected group to store inbound replicas from the partner group. The Dell PS Series SAN supports bi-directional replication as well as many to one replication. If replicas are not going to be sent to this site from this partner then the value can be left at 0. Choose the amount of delegated space (the originating storage pool) and click **Next**.
6. Verify all of the information is correct and click **Finish**.



This creates the partnership between the protected site and the recovery site.

7. Follow the same steps to configure the partnership between the recovery site and the protected site.

**Note:** 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 various factors such as the number of replicas you wish to keep as well as how much data change is happening between each replica.

## 4.2 Step 2: Configure replication on the datastore volumes

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

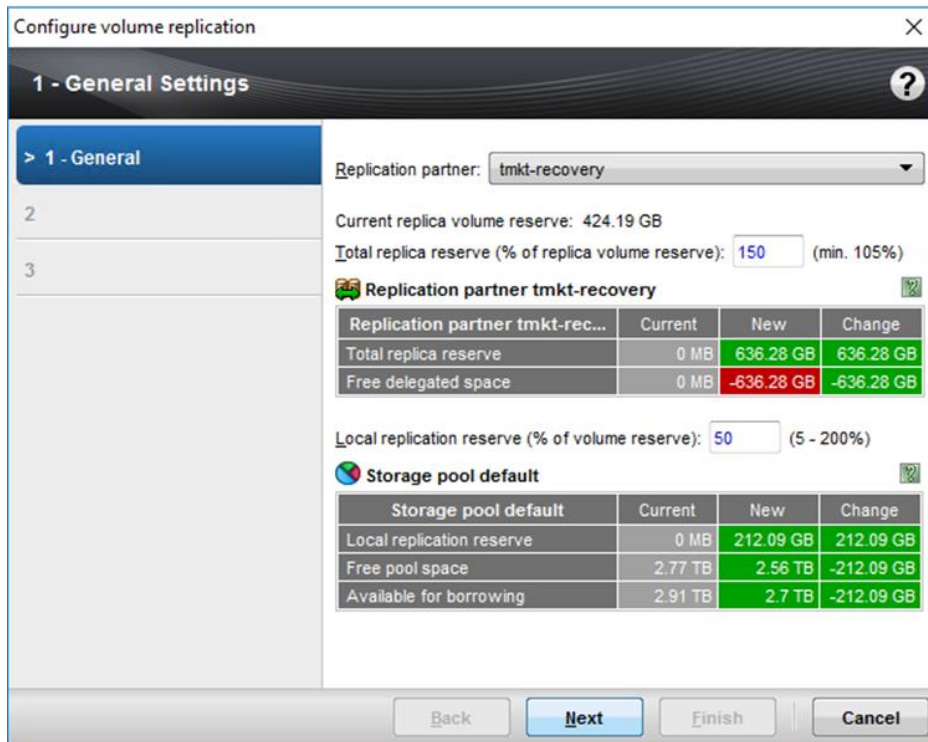
1. From the protected site Group Manager GUI, click **Volumes management**.
2. Click the datastore volume that needs to be protected with replication. In the **Activities** tab, click **Configure Replication**.
3. The next screen is divided into three sections. In the first section, choose the replication partner for the volume.  
In the second section, select the total replica reserve; a percentage of the 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 expected amount of change and the number of replicas you wish to keep.

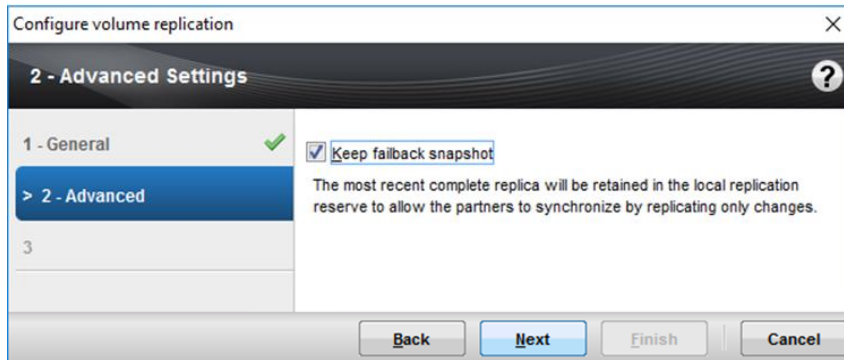
The third section will set aside a percentage of this volume in the local replica reserve to keep track of changes made during the replica process. This is also where Fast Failback Snapshots are stored in the event you are failing back from a replica set. This can either come from local replica reserve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

**Note:** These settings can easily be changed later by selecting **Modify replication settings** in the volume's activities pane.

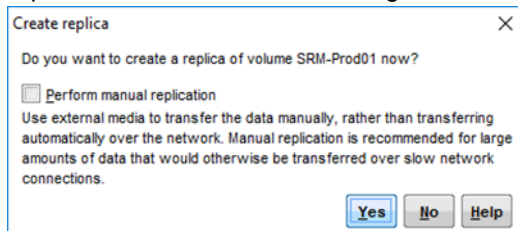
4. Choose your options in each section and click Next.



5. In the Advanced Settings screen, you can keep failback snapshot. Fast failback keeps a copy of the most recent replica on the protected array. SRM allows administrators to “reprotect”, or automate failback, to the original protected site after the cause of the failover has passed. Leveraging fast failback, results in shorter recovery time as only the changes at the recovery site need to be replicated back to the protected site. Make your selection and click **Next**.



6. View the summary and click **Finish** to complete the replication configuration. Upon completion, you can start the volume replica process immediately. This will begin replicating the base volume and creating a replica set on the partner array. It can either be performed at this stage or by the volume replication schedule that is configured in the next step.



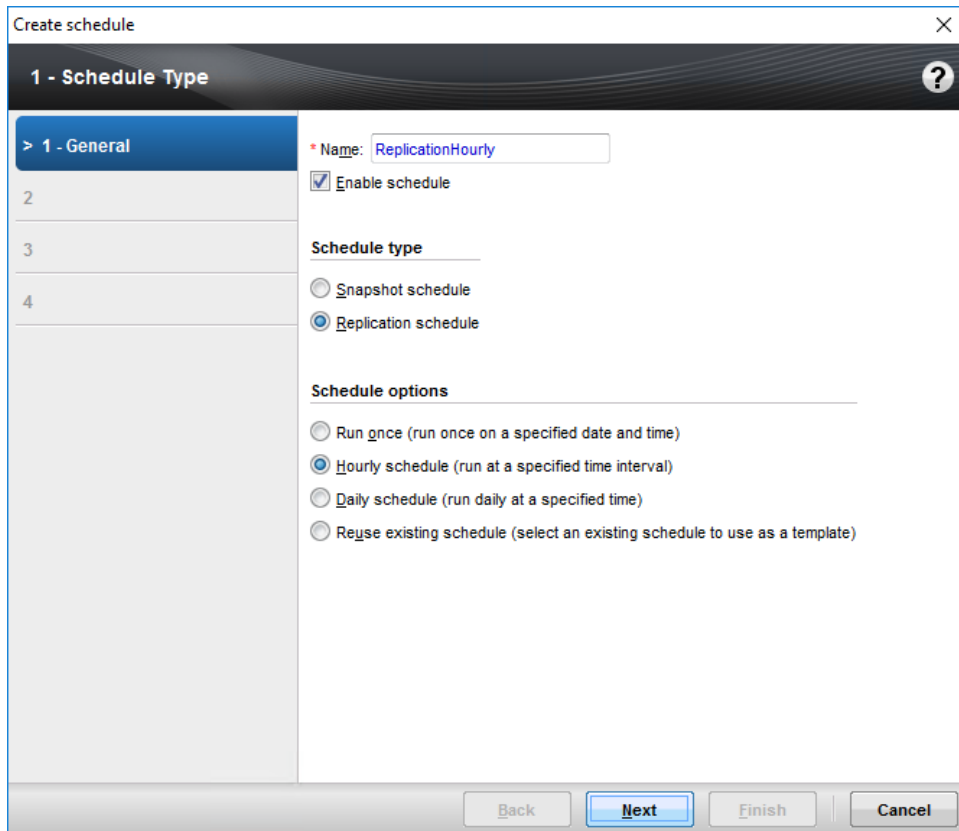
Optionally, you can utilize the Manual Transfer Utility (MTU) to perform the initial replica. This allows data to move from one datacenter to another without using built-in replication. This is often done if the bandwidth between sites is sufficient to accommodate the rate of data change of the volume, but not enough to create the large initial replica in a timely manner. In order to use the MTU, check **Perform manual replication**. See the [Manual Transfer Utility User Guide](#) for detailed information.

7. Repeat this process for each volume that requires SRM protection. SRM will not recognize a datastore as protected until it is both configured for replication and has an active schedule configured for it (see the next step, “Step 3: Configure replication schedule”).

## 4.3 Step 3: Configure replication schedule

Each volume can be set up with different replication properties and schedules. This granular control allows volumes to have different protection schemes based on the data hosted. 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 within each volume.

1. From the protected site Group Manager GUI click **Volumes management**.
2. Click a volume to configure a schedule. In the **Activities** tab under **Schedules** click **Create schedule**.
3. Give the schedule a name and choose the **Replication** schedule radio button. Choose the schedule option that meets the data needs: Run once, hourly, daily, or reusing an existing schedule. Check **Enable schedule** and then 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* and *Dell EqualLogic Auto-Replication: Best Practices and Sizing Guide*.
5. Verify the summary of the schedule and click **Finish**. Follow the same procedure on all the Datastore volumes that host VMs that are to be protected in SRM.

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, including having an active replication schedule, you can proceed with the configuration of SRM. These steps must be repeated for each volume added to the virtual environment that will be hosting VMs and need SRM protection.

## 5 Installation and configuration of VMware SRM

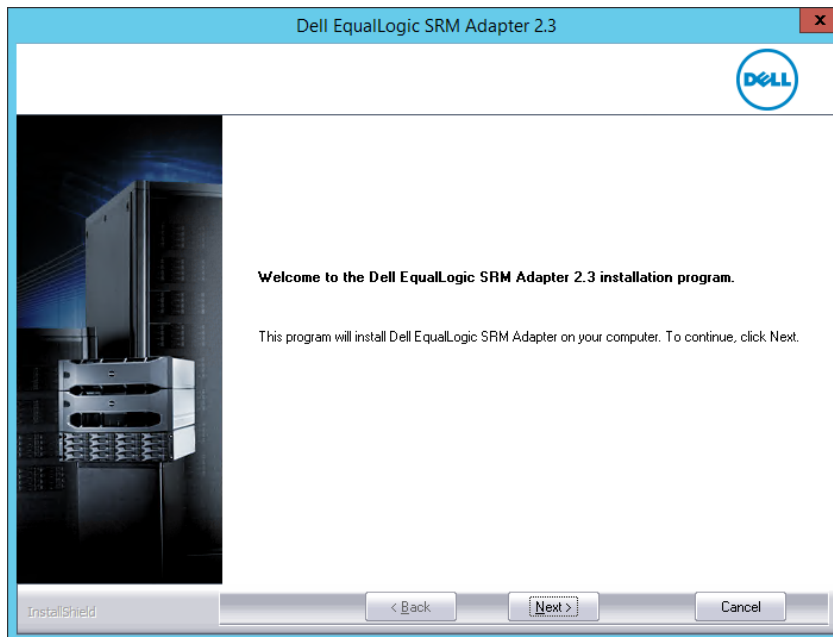
Before VMware vCenter Site Recovery Manager can be installed, both the protected site and recovery site must have their own instance of VMware vCenter Server installed and configured. The server where SRM is installed must be able to communicate with the remote SRM server as well as have connectivity to the local SAN. For more information consult the [VMware vSphere System Administrator Documentation](#).

Once the vSphere virtual environment is configured on both the protected site and the recovery site, install SRM 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. For environments with a small number of virtual machines to protect, SRM can be installed on the same server as the vCenter server but installations may differ. For more information consult the [SRM Installation and Configuration](#) document from VMware.

### 5.1 Step 1: Install Dell EqualLogic Storage Replication Adapter

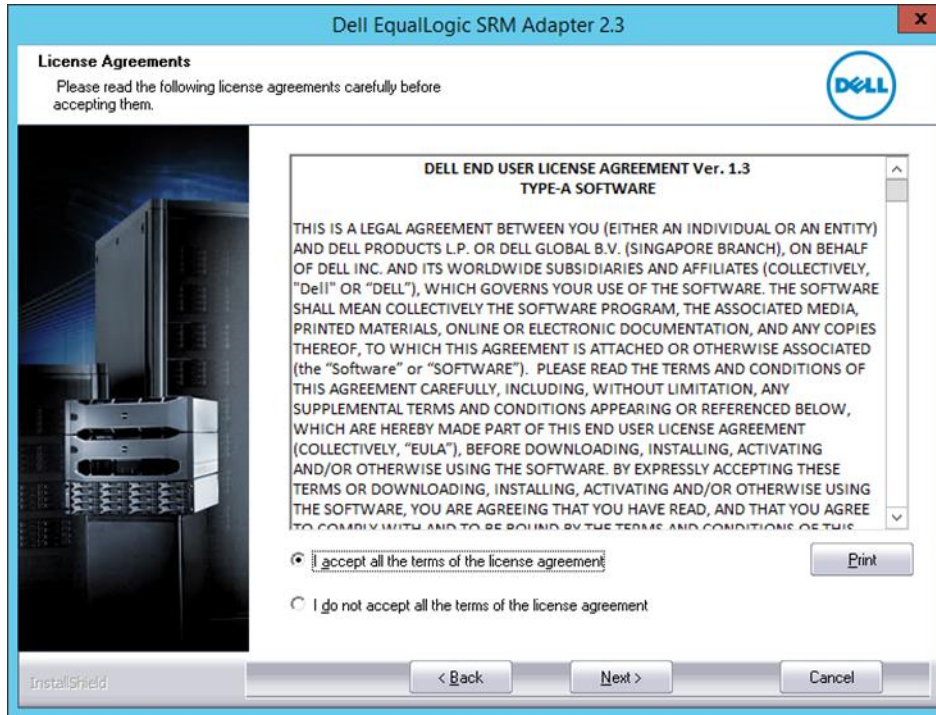
Once SRM is installed on both sites, the Dell Storage Replication Adapter for VMware Site Recovery Manager (sometimes referred to as *array scripts*) must be installed on each site. This adapter is necessary to allow SRM to communicate with the PS Series SANs and to coordinate the entire process of testing,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

1. You can download the Dell Storage Replication Adapter for VMware vCenter Site Recovery Manager from the [Dell PS Series support site](#) or VMware SRM SRA site.
2. The SRA must be installed on both sites, the procedure is the same. Run the executable on each site.
3. Click **Next**.

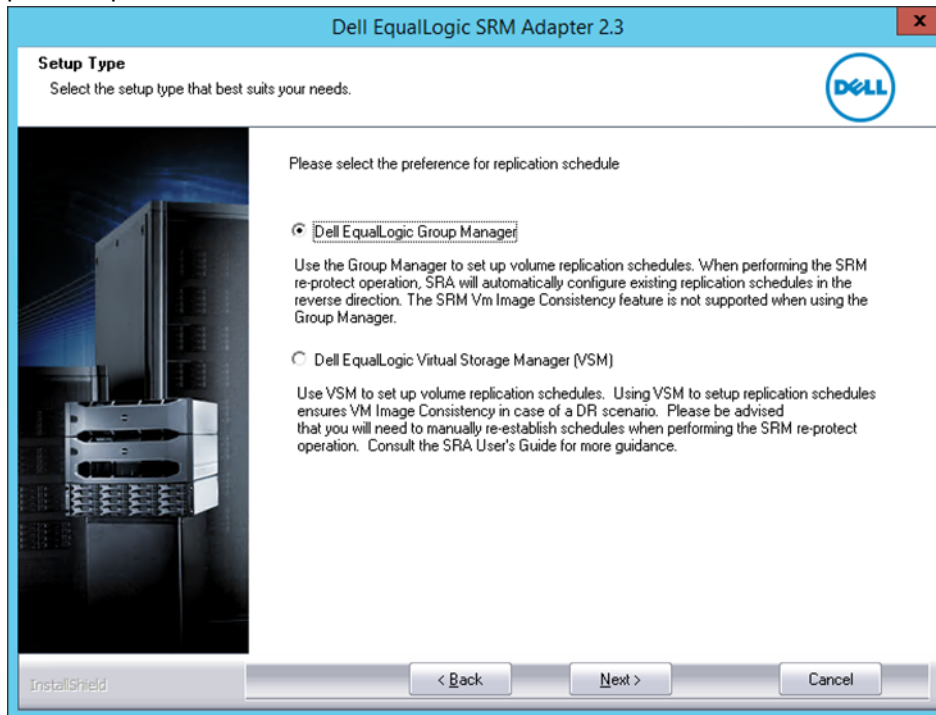




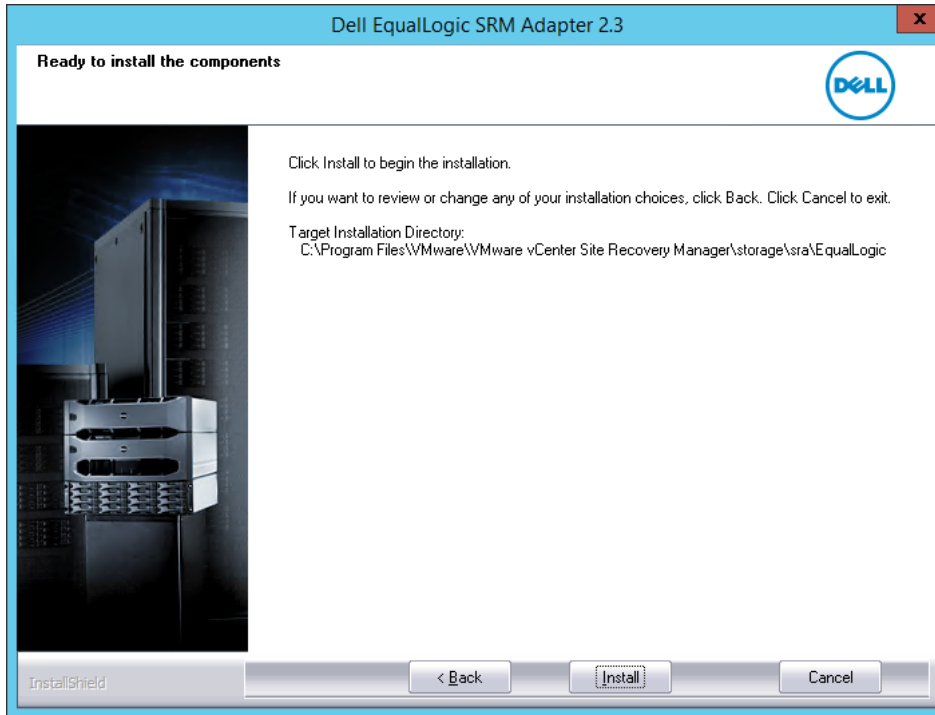
4. Review and agree to the terms of the license agreements. Click **Next**.



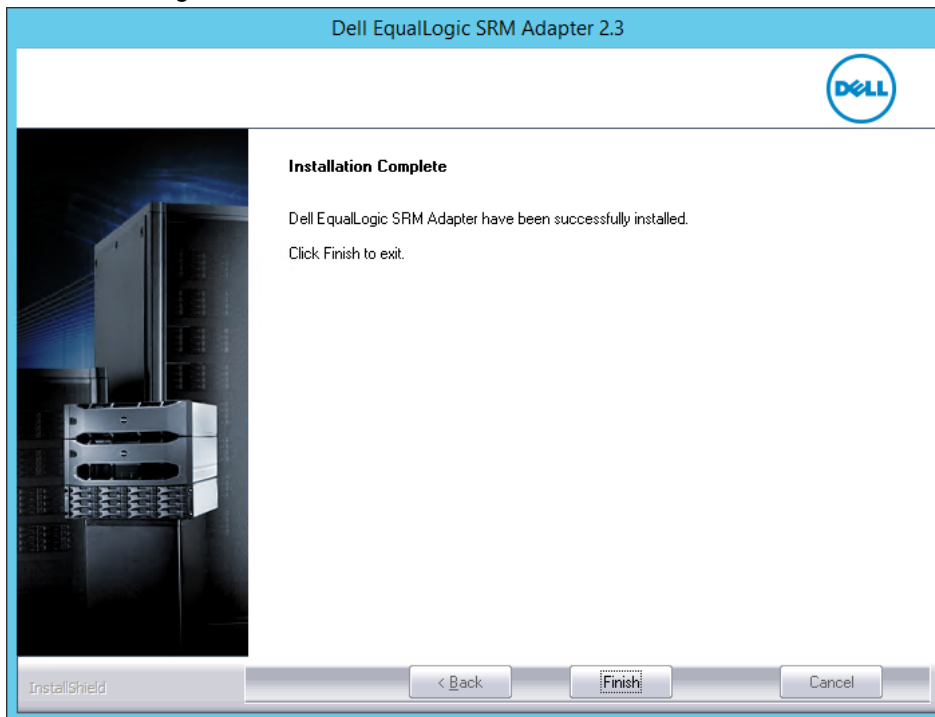
5. The Dell SRA can optionally coordinate with the Dell Virtual Storage Manager (VSM) to create VM Image Consistency replicas. Note that this feature requires manual steps when performing SRM re-protect operations. Review the VSM documentation for more information on this feature.



6. Verify the target installation directory and click **Install**.



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

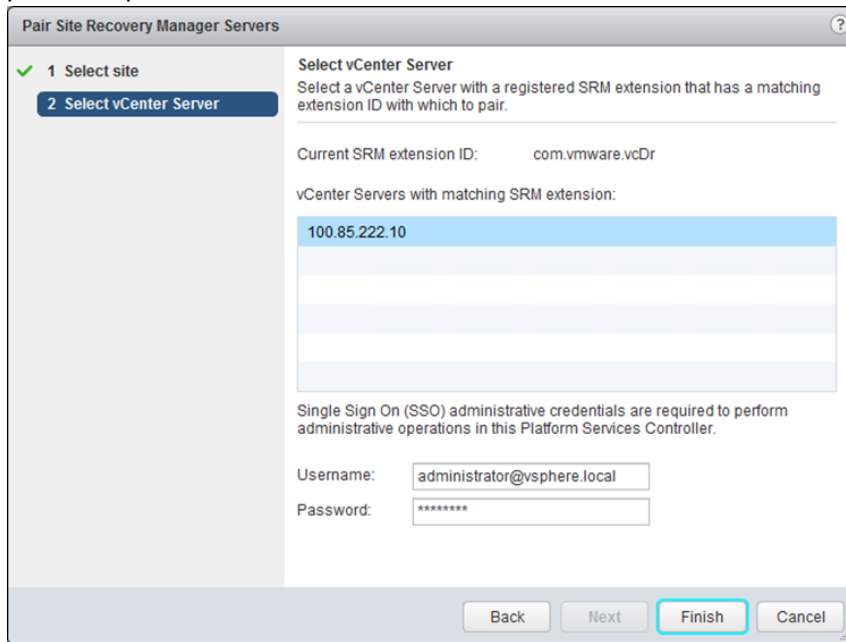




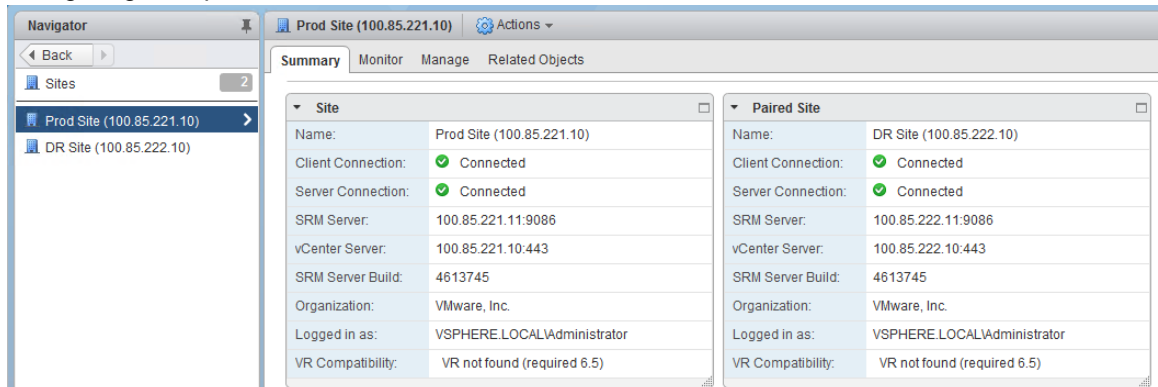
## 5.2 Step 2: Configure SRM connection

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

1. To get to the SRM configuration screen, select **Home**. Then under Inventories click **Site Recovery**.
2. From the Sites section click **Pair Site**. Enter the hostname or IP address of the Platform Services Controller at the recovery site. Enter in credentials for the remote site, and click **Finish**. The partnership will be established.



3. This is covered in more detail in the *SRM Administrator Guide*, but once 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.

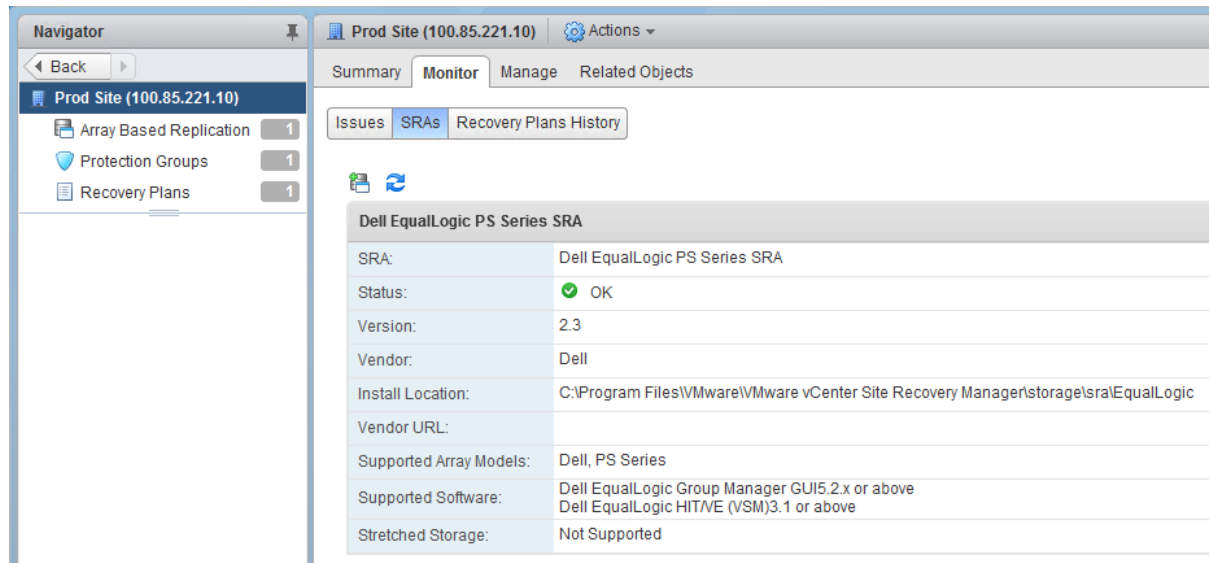


4. From the example screenshot above, note that the protected vCenter server is 100.85.221.10 and protected SRM server is 100.85.221.11, and have been given the site name Prod Site. On the recovery site, the vCenter server 100.85.222.10 and SRM server is 100.85.222.11, and the site name is DR Site.

## 5.3 Step 3: Configure array managers

Once the SRM partnership between the two sites is established and the Array Manager needs to be configured.

1. From the SRM section of the vSphere client, select one of the sites. Click on the **Monitor** tab and then select **SRAs**.
2. The previously installed SRA will be displayed here. It may be necessary to do a manual rescan on first use. Click **Rescan SRAs** to discover the SRA.



The screenshot shows the vSphere web client interface for a 'Prod Site (100.85.221.10)'. The left sidebar shows a 'Navigator' with 'Prod Site (100.85.221.10)' selected, containing 'Array Based Replication' (1), 'Protection Groups' (1), and 'Recovery Plans' (1). The main content area has tabs for 'Summary', 'Monitor', 'Manage', and 'Related Objects'. Under the 'Monitor' tab, there are sub-tabs for 'Issues', 'SRAs', and 'Recovery Plans History'. The 'SRAs' sub-tab is active, displaying a table for 'Dell EqualLogic PS Series SRA'.

Dell EqualLogic PS Series SRA	
SRA:	Dell EqualLogic PS Series SRA
Status:	OK
Version:	2.3
Vendor:	Dell
Install Location:	C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\EqualLogic
Vendor URL:	
Supported Array Models:	Dell, PS Series
Supported Software:	Dell EqualLogic Group Manager GUI 5.2.x or above Dell EqualLogic HIT/VE (VSM) 3.1 or above
Stretched Storage:	Not Supported

Once the SRA has been discovered at both locations, each side needs to have its Array Manager configured. This is the PS Series group that is local to each SRM instance. In order for the SRM server to see the Array Manager correctly it must have access to the group management IP address.

3. Continuing from the same location in the vSphere web client, click **Add Array Manager**. This option is also accessible from the **Actions** drop down menu.
4. On the Options page, select **Add a pair of array managers** and click **Next**.
5. On the Location page, select the relevant pair of sites and click **Next**.

- Select the Dell EqualLogic PS Series SRA type and click **Next**.

**Add Array Manager**

1 Options  
2 Location  
3 **Select SRA type**  
4 Configure array manager  
5 Configure paired array manager  
6 Enable array pairs  
7 Ready to complete

Select SRA type  
Specify an installed SRA for both array managers.

SRA Type	Status
Dell EqualLogic PS Series SRA	OK

1 items Export Copy

SRA Type: Dell EqualLogic PS Series SRA  
Version: 2.3  
Vendor: Dell  
Supported Array Models: Dell, PS Series  
Supported Software: Dell EqualLogic Group Manager GUI 5.2.x or above  
Dell EqualLogic HIT/VE (VSM) 3.1 or above  
Stretched Storage: Not Supported

Back Next Finish Cancel

- On the Configure array manager page enter a **Display Name** that is descriptive and makes the array easy to identify, for example the PS Series group name can be used.
- Under Managed Group, fill in the Group IP Address or Hostname of the local PS array and the Group Manager credentials. Under Partner Group, in the **Partner Name** field, enter in the Group name of the replication partner (case sensitive), as well as the credentials. Click **Next**.

**Add Array Manager**

1 Options  
2 Location  
3 Select SRA type  
4 **Configure array manager**  
5 Configure paired array manager  
6 Enable array pairs  
7 Ready to complete

Configure array manager  
Enter the name and connection parameters for the array manager.

Specify parameters for site 'DR Site (100.85.222.10)'  
Display Name: tmkt-skynetgrp

**Managed Group**

Local Group connection parameters  
Group IP Address: 100.85.220.240  
Enter IP address of the Group  
Volume name prefix limiting discovery: [ ]  
Leave empty for full discovery  
Username: grpadmin  
Enter Username for Group  
Password: [ ]  
Enter Password for Group


**Partner Group**

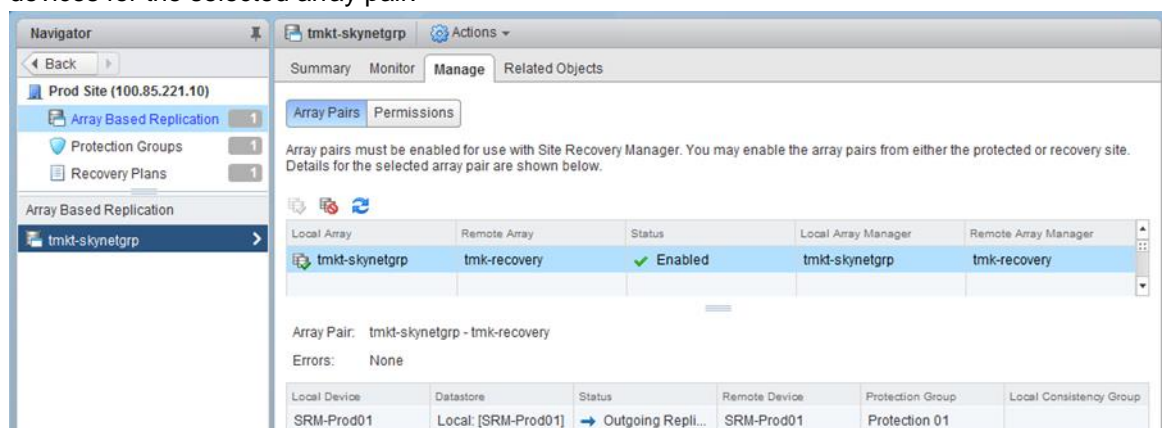
Partner Group Replication Parameters  
Partner Name: thmk-recovery  
Enter Partner Group Name  
Partner Replication Username: grpadmin  
Enter Partner Group Replication Username  
Partner Replication Password: [ ]  
Enter Partner Group Replication Password

Back Next Finish Cancel

9. On the Configure paired array manager page, repeat the previous two steps for the PS Series array at the DR site. Click **Next**.
10. On the Enable array pairs page, select the array pair and click **Next**.
11. On the Ready to complete page, review the setting and click **Finish**  
This will establish the protection site array manager.

To view the status of the relationship between the array pairs, and the status of datastore replication perform the following:

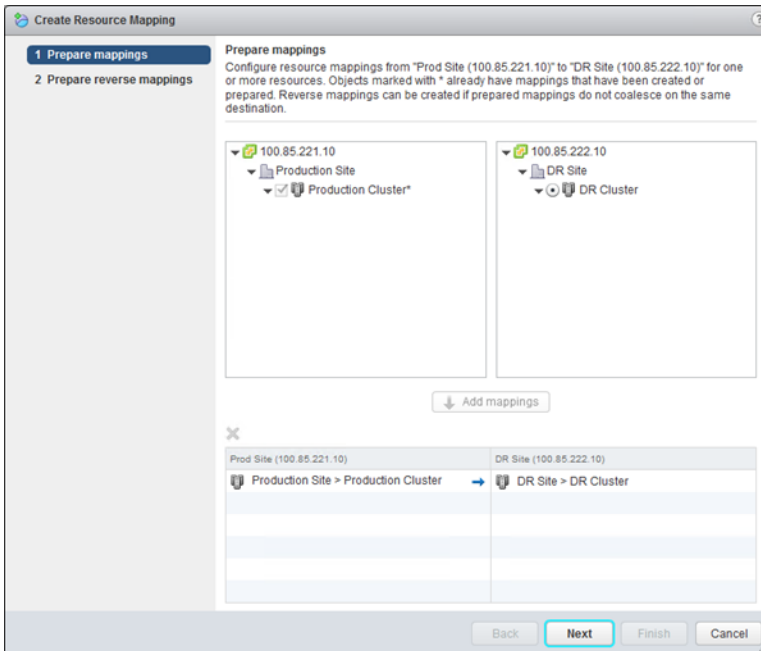
1. Select Array Based Replication from any of the site, then click on the **Manage** tab, and then **Array Pairs**.
2. Next select the array pair of interest to display a list of the datastores and their current status.
3. Anytime new datastores are added and configured for replication, simply click  to discover new devices for the selected array pair.



## 5.4 Step 4: Configure inventory mappings

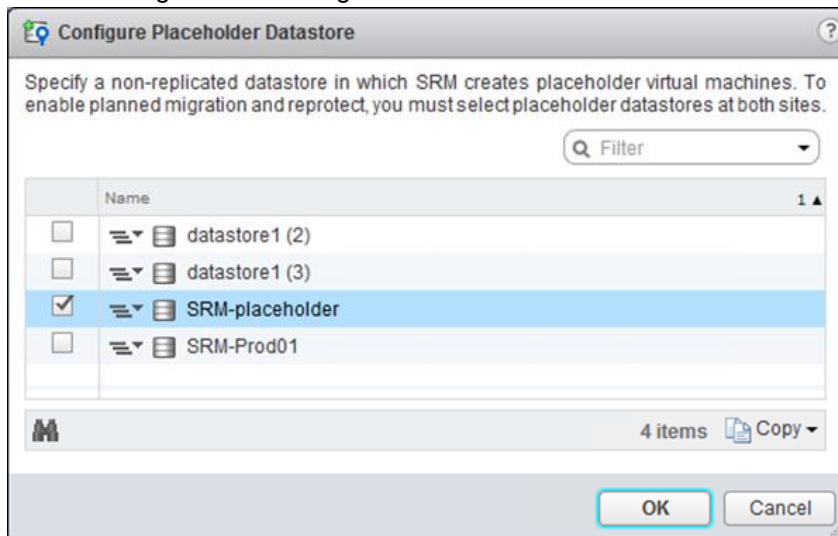
Inventory mappings are settings that match the protected site resources with the recovery site resources. This can be used to match data centers, resource pools, folders, storage policies, and networks on the protected site with data centers, resource pools, folders, storage policies, and networks on the recovery site for testing and failover. 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 settings can be overwritten at the individual VM level. Consult the SRM Administration Guide on how to configure the inventory mappings for SRM.

To configure inventory mappings, select Sites from the Site Recovery Home in the vSphere Web Client. Select one of the sites, and then click on the Manage tab. Select one of the options (Network Mappings, Folder Mappings, Resource Mappings and Storage Policy Mappings) and then click **New...** to create a new mapping for that type. In the example below, the production cluster at the production site is being mapped to the DR cluster at the DR site. Similar options are available for network, folder and storage policy mappings.



## 5.5 Step 5: Configure placeholder datastore

1. Once the inventory mappings are created, click **Placeholder Datastores**.
2. Click **Configure Placeholder Datastore** and 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 because it is a temporary space to hold the small .vmx and other configuration files for each of the protected VMs. It is recommended to use a volume datastore that is shared among all of the recovery ESXi servers.
3. Click **OK**. This also needs to be done on the protected site in the case of a reprotect. This will be used to unregister and re-register the VMs on failback.



## 6 SRM protection groups

A protection group is a datastore volume or group of datastore volumes with virtual machines that need to be protected or it can be based on a storage policy. A protection group can be configured from either site through the VMware vSphere Web Client. More detailed information can be found in the *SRM Administration Guide*. The steps are an example of creating a datastore protection group.

**Note:** Recovery plans can only consist of storage policy protection groups or array based replication datastore protection groups.

1. From the vSphere Web Client, log into the protected site, click on Home and select **Site Recovery** from Inventories. Select the Protection Groups and click **Create Protection Group** from the menu bar.
2. Provide a name and description that clearly identify what will be protected, and then select the relevant site-pair. Click **Next**.
3. Select the direction of protection (in this example the Prod Site will failover to the DR Site) and then select the protection group type (in this example datastore groups). Finally, select the array pair and click **Next**.

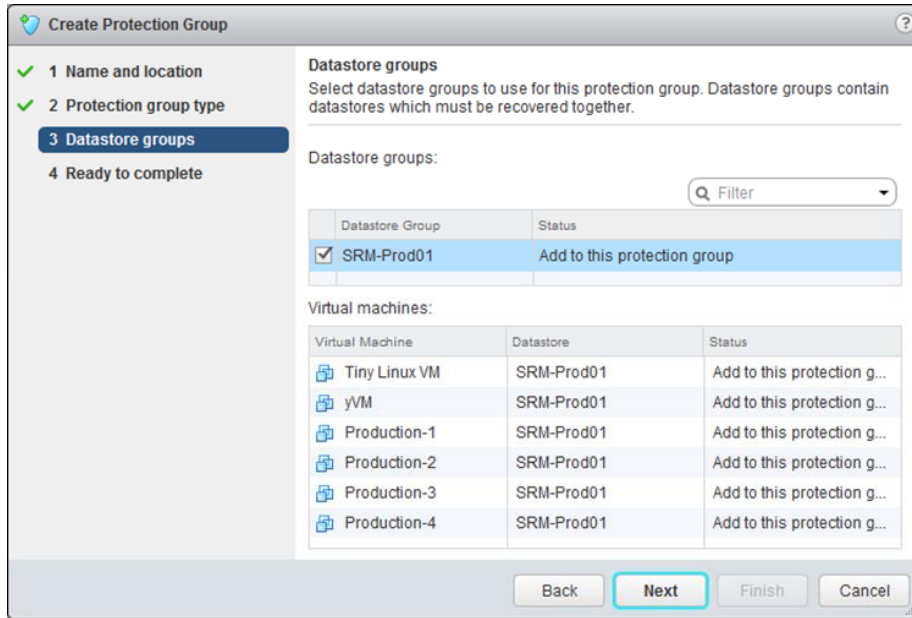
The screenshot shows the 'Create Protection Group' wizard in the vSphere Web Client. The wizard is currently on step 2, 'Protection group type'. The left sidebar shows the progress: 1 Name and location (completed), 2 Protection group type (current step), 3 Datastore groups, and 4 Ready to complete. The main area shows the following options:

- Protection group type:** Select the protected site and protection group type.
- Direction of protection:**  Prod Site (100.85.221.10) -> DR Site (100.85.222.10)  DR Site (100.85.222.10) -> Prod Site (100.85.221.10)
- Protection group type:**  Datastore groups (array-based replication)  Individual VMs (vSphere Replication)  Storage policies (array-based replication)
- Array pair:** A list showing 'tmkt-skynetgrp' expanded with 'tmkt-skynetgrp - tmk-recovery' selected.

At the bottom of the wizard are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

4. On the next screen, select all of the datastores to be included in the protection group. If a VM has entities that reside across multiple datastores, they will all be included in the same group. By selecting each datastore group you will see which VMs will be associated with the protection group. Protection groups are used by SRM when creating recovery plans. Make your selection and click **Next**.

**Note:** A datastore can only reside in one protection group, but a protection group can be a part of one or more recovery plans. This enables the creation of recovery plans that recover only a single datastore of VMs, multiple datastores of VMs, or the entire site.



5. Verify the setting on the final screen and click **Finish**.
6. Follow this same procedure for all of the protection groups that need to be configured. In order to be protected with SRM, each replicated datastore must belong to a protection group.
7. As the protection groups are created, you will see placeholder VMs being registered on the recovery site. SRM will also notify you if there are any errors in protecting the VMs. The following is an example of a finished protection group.



## 6.1 Datastore cluster considerations in protection groups

vSphere includes a functionality for datastores called a datastore cluster. A datastore cluster is a grouping of datastores that allows for ease of VM placement as well as load balancing and capacity balancing across datastores in the cluster. It leverages storage DRS to move VMs to the appropriate datastore either manually or automatically. Storage DRS can recognize if a datastore is replicated, and this information is then used by Storage DRS in deciding which automatic moves it can make. Storage DRS will not perform any automatic migrations that would impair the recoverability of a VM with SRM.

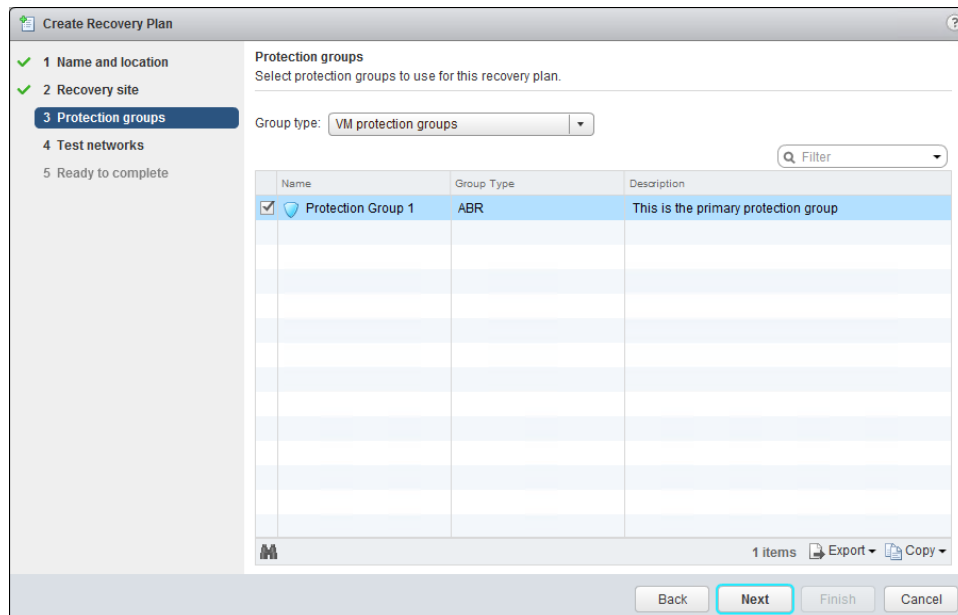
However, SAN replication is configured at the datastore volume level. When a VM is storage vMotioned to another datastore this is seen at the SAN level new data, not the movement of data from one volume to another. This new data must be replicated to the DR site before the vMotioned VM can be fully protected again. Care should be taken to avoid excessive relocation of VM storage to avoid unnecessary data replication.



## 7 Recovery plans

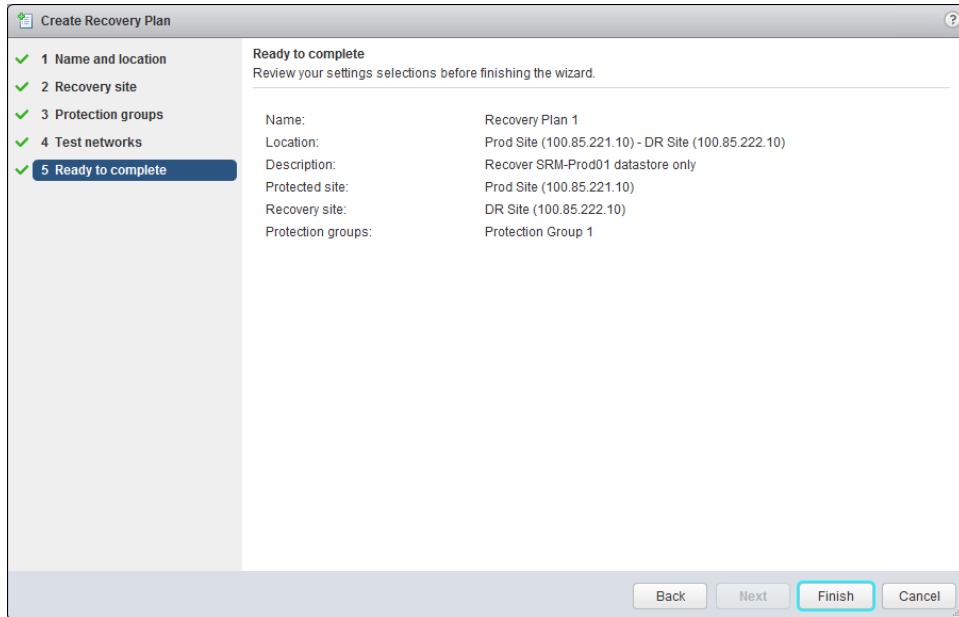
A recovery plan is a run book plan that facilitates and automates the process of testing and failing over virtual machines. The recovery plan can encompass any or all of the protection groups created on the protected site. This allows administrators to configure and run various test scenarios. It also 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. Recovery plans can be configured from either the protected site or the recovery site and will prompt for the recovery plan location.

1. From the vSphere Web Client, log into either site, click on **Home** and select **Site Recovery** from Inventories. Click **Recovery Plans** and then **Create Recovery Plan** from the menu bar.
2. Provide a name and description that clearly identifies what will be recovered by this recovery plan, then select the relevant site-pair, and click **Next**.
3. Select the recovery site where the VMs will be recovered and click **Next**.
4. Select the Protection Groups that will make up this Recovery Plan. This process gives administrators multiple granular recovery options for both testing and full site failover. Make the selection and click **Next**.



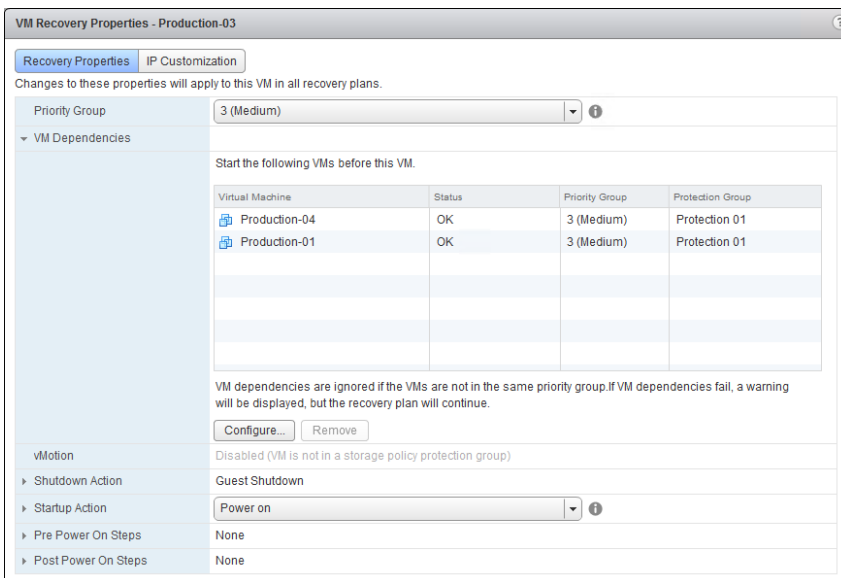
5. The next screen provides test network options. Test networks are isolated network environments that are created on the fly during the test to make sure that the VMs being brought online cannot interfere with other running VMs including those in production. The test network can be changed if you have additional switching requirements configured at the DR site such as an isolated test LAN with physical systems. By default, SRM is set to automatically create a new vSwitch for the duration of test failover. These vSwitches are isolated from other vSwitches that were created by other failover tests run at the same time. Make your selection and click **Next**.

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



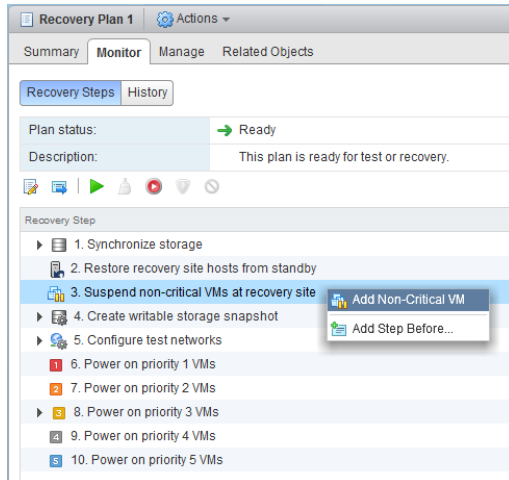
After configuring a recovery plan, you can adjust individual VM recovery options by selecting the recovery plan and then clicking **Virtual Machines** on the **Related Objects** tab. There are many options including recovery priority, VM dependencies, IP customization, pre- and post-power on scripts. The power of SRM gives the ability to modify the needs of each VM for recovery and testing, and then test these changes without impacting the production environment.

To modify the individual protection schemes of a VM, right click the VM and select **Configuration Recovery** to modify the options.



Another option is to suspend the non-critical VMs at the recovery site. This allows administrators to use the DR location to host VMs that are not necessary in the event of a failover from the protected site. To do this:

1. Open the **Monitor** tab in the recovery plan.
2. To suspend virtual machines on the recovery site, right click **Suspend Non-critical VMs at recovery site** and select **Add Non-Critical VM**.
3. Select the virtual machines to be suspended when this recovery plan is run.



There can be multiple recovery plans configured with multiple scenarios. The benefit of SRM is the ability to configure multiple recovery plans and also non-disruptively test them to assure they meet the ever changing organization's needs. Once there is at least one recovery plan, testing can begin.

## 8 Testing

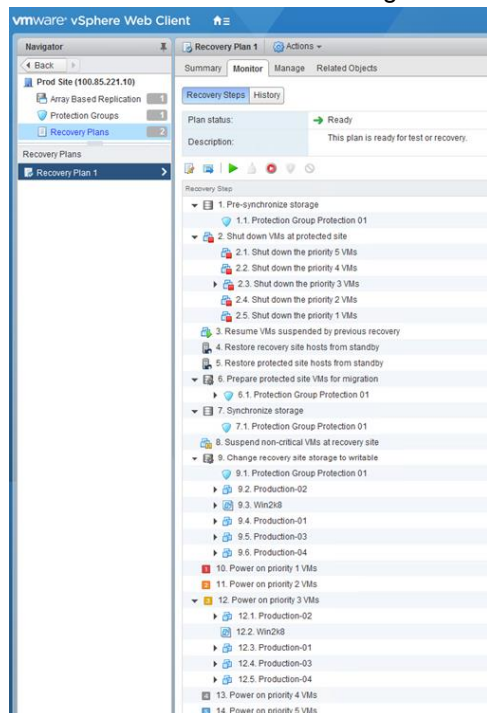
One of the greatest attributes of SRM is the ability to non-disruptively test the recovery plan before there is a failure. This allows administrators the ability to tune their recovery process and ensure a plan will perform as intended in the event of an actual failover. It also allows for comprehensive auditing of the recovery plans without affecting production virtual machines.

A test failover scenario is designed to completely eliminate any impact on the production VMs and datastore volumes. When a test is run on the recovery site, the recovery site PS Series group is instructed by SRM by the SRA to create a clone of the replica volumes and bring the clones online. The cloning of the replica allows the replication of the production datastores to continue, while also still allowing exact copies of the VMs to be made available at the recovery site. However, there needs to be sufficient free space available in the DR 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.

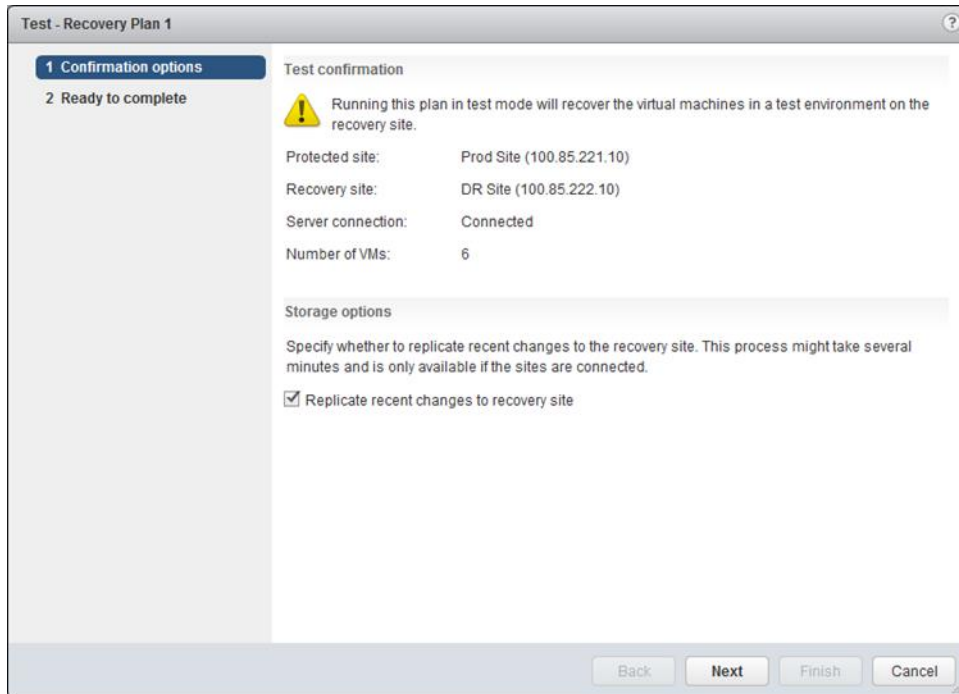
Once the clone is created, SRM will send the information about the recovery ESXi hosts to the SAN group, add to the access control list and bring the clone online. This allows SRM to rescan the storage at the ESXi host level. The volume will re-signature as needed in order to bring that clone online as a new datastore.

SRM will then re-configure the recovery VMs to point to the new clone volumes and start powering them up in the order specified in the 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 recovery vSwitch with no external NIC connections. Again, this is done along with everything else to protect the production environment.

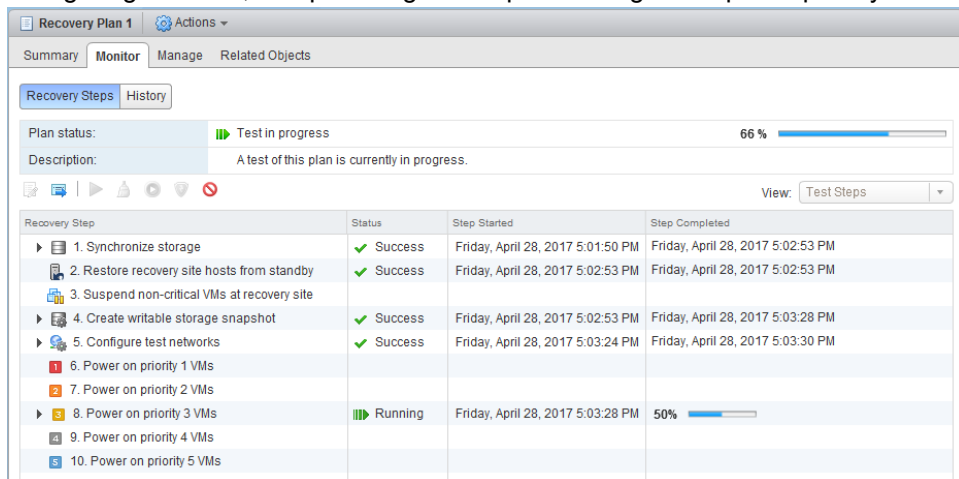
1. From the vSphere Web Client: log in to either site, click on **Home** and select **Site Recovery** from inventories. Click **Recovery Plans** and select a recovery plan. This will show the recovery run book and then execute for both testing and recovery.



2. Click **Test** at the top of the recovery plan to begin.
3. During a test you have the option of replicating recent changes to the recovery site. This is independent of any replication schedules you may have, and could take several minutes depending data that has changed since the last replication. Select your option and click **Next**.

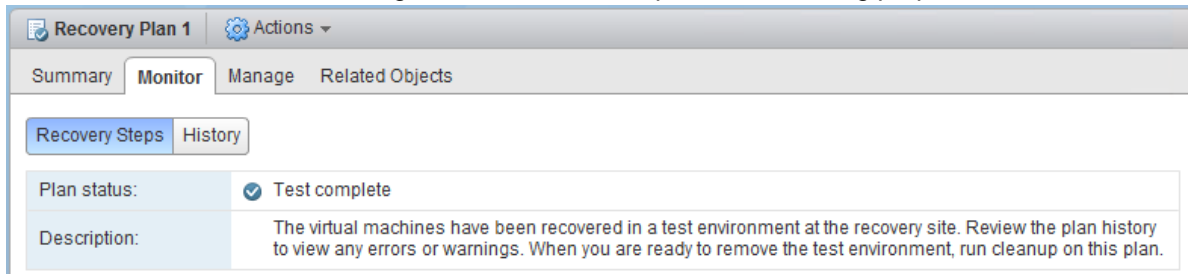


4. Review the recovery plan steps and click **Finish**.
5. The progress of the test will fill up the Recovery Steps screen. It will go through and prepare the storage by creating the clones, bringing the clones online, rescanning the storage subsystem, re-configuring the VMs, and powering them up according to the plan's priority order.



6. Once the entire Recovery plan has been run, it will display the status: **Test Complete**. 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

RDP sessions, 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, troubleshoot the issue, correct the error and re-run the test. A log of the test can be exported for auditing purposes.



7. Once you have verified the test failover of the individual virtual machines, click **Cleanup** to finish the test and clean up the environment. SRM will re-configure the VMs to point towards the temporary datastore, and remove the isolated test network. It will then unregister the storage from ESXi hosts and delete the clone volumes to free space on the array. Within a few minutes the recovery site environment will be back to the way it was before the test was run.

This testing process provides the ability to find errors or mistakes and to fine tuning the DR recovery plan before a true disaster happens. All without disrupting the production environment.

## 9 Recovery

In case of a full site failure, a site migration or simply wanting to fail over individual protection groups, running the recovery plan follows a slightly different process. First, SRM tries to communicate with the protected site vCenter Server. If it can, SRM shuts down any VMs on the protected site to make sure they are not online with both sites. It also takes the original protected datastores offline. When running the recovery plan, instead of making a clone of the replicas on the DR array, the replicas are promoted but with the ability to be later demoted. Once all the replicas are promoted, SRM prompts vCenter to rescan all of the storage adapters and bring the promoted volumes online as storage.

Next, SRM re-registers the recovery VMs to point to the newly promoted volumes. Unlike a test, the network configuration is changed to match the recovery settings so the test isolated vSwitch will not be created. Each of the VMs power on based on their priority level and the rest of the recovery plan runs. Once the entire recovery plan is complete, the protected site's virtual environment is in production on the recovery site.

The replicas that were promoted are not fully promoted volumes, because they retain the ability to be demoted in order to utilize the fast failback procedure on the group. Because the promotion is not permanent, there are a few actions 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, however, this will impact SRM's ability to reprotect and failback that volume.

1. To begin a recovery process, click **Recovery Plans**, select a recovery plan and click **Run Recovery Plan**. A planned migration or disaster recovery is an executive decision and should not be invoked without planning and thought. SRM will verify that this is the option you wish to take by requiring the administrator to check the box acknowledging that the process will change the environment. You can select between two types of recovery processes:  
**Planned Migration:** Used when migrate between datacenters. The plan will stop on any failure and not complete the site migration. It will also try to take one last replication to obtain all of the latest changes.  
**Disaster Recovery:** Used when the protected site is unavailable or in the event of a true disaster. The plan will attempt to synchronize and power down VMs on the protected site but if there are any errors it will continue moving forward with the plan.
2. Acknowledge the warning, select the recovery type and click **Next** to begin the failover process.

Recovery - Recovery Plan 1

1 Confirmation options

2 Ready to complete

Recovery confirmation

! Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

Protected site: Prod Site (100.85.221.10)

Recovery site: DR Site (100.85.222.10)

Server connection: Connected

Number of VMs: 5

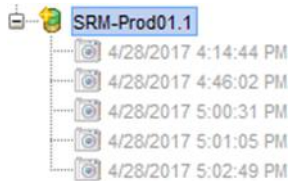
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

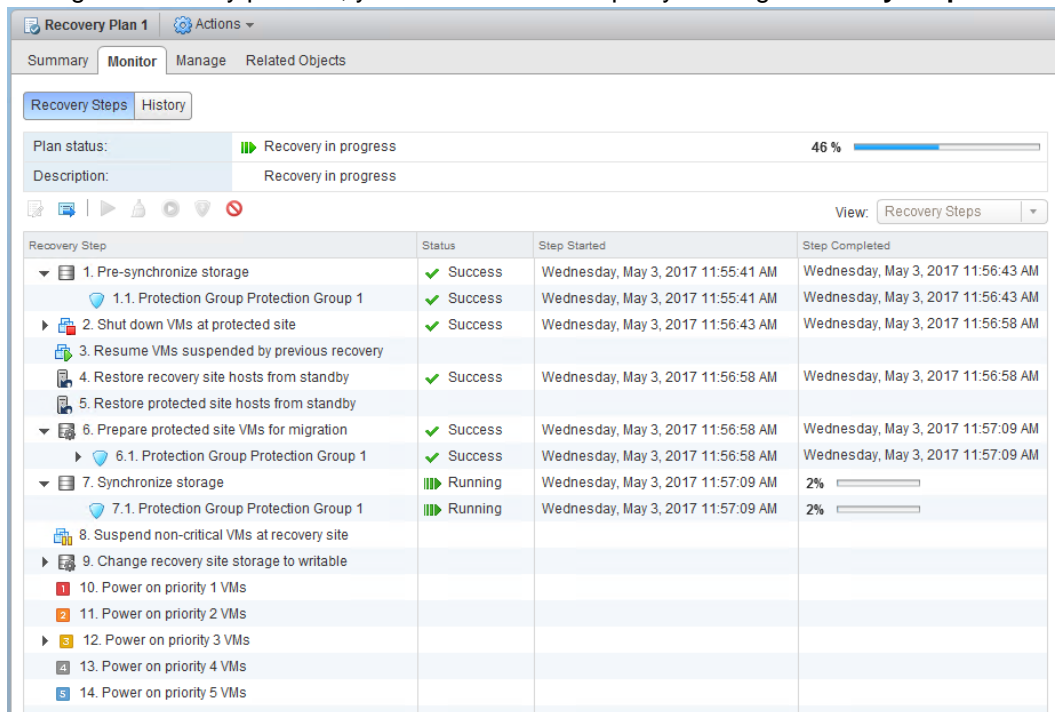
Planned migration  
Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

Disaster recovery  
Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

- There will be one last screen to review before the recovery process begins. Verify the settings and click **Finish**.
- From the recovery site PS Series Group Manager GUI all of the promoted replicas are displayed as recovery volumes.



- During the recovery process, you can follow the steps by clicking **Recovery Steps**.



- When the recovery process is complete, SRM shows that the recovery is complete in the monitor tab. If there are any errors during the recovery they are displayed as well. Each of the VMs will show up on the recovery site registered to the correct recovery datastore and be running according to the plan.

This completes the recovery failover and you can utilize the recovery site as full production according to the disaster recovery plans for your organization.

**Note:** For a planned failover or migration it is recommended that a planned downtime occur and the VMs are powered off before the final replica to ensure that all of the data is in a clean and consistent state on the DR site.



## 10 Failback

Failback is the process that brings the recovered VMs at the DR 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.

Regardless of the reason that the recovery site is now servicing production VMs, there are two basic scenarios for utilizing failback: The original SAN on the protected site is still in service and has some subset of data from the production environment before the failover or the SAN is completely new because it is new hardware or has been re-initialized. There may even be an instance where both of these techniques are used depending on the reason for failover. Site Recovery Manager provides the ability to failback to the original protected site using a process called reprotect. Reprotect is only available when the original protected site and the associated data is still available.

With careful planning, bringing the recovery site virtual environment back into production on the original protected site can happen with very little downtime.

During planning, the role of protected site and recovery site may change. This section denotes site A as the original protected site that had data in production and site B as the original recovery site as the fail-over destination.

### 10.1 Recovery scenario 1: Reprotect and failback

The first scenario is where the original protected site A still has a functioning SAN with some subset of data. The failover could have been invoked due to a planned hardware outage or unplanned power failure, but nothing involving the underlying server and storage environment. While disaster recovery failovers are seldom planned, the failback process can be planned and controlled to ensure that there is no loss of data and minimum disruption.

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 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.

#### 10.1.1 Reprotect

SRM provides the ability to failback to the original protected site using a process called reprotect. Reprotect automates the process of re-establishing the replication going from the array at site B (the recovery site) back to the array at site A (the protected site). Reprotect does not failback, but configures everything so that you can test going back to the original protected site A, and if testing proves successful, then do a planned migration. During the reprotect, fast failback can shorten the time period of the replication sync back. From a high level the process is as follows:

1. Demote the protected site A volume to an inbound replica set.

2. Make the recovery site B volume promotion permanent.
3. Reverse the replication setup and configure replication from site B to site A for the re-protected volumes.
4. Reverses protection groups and recovery plans so they can be run going from site B to site A.

Once the reprotect is finished, the protection groups and recovery plans will have been switched. This makes site B the protected site and site A the recovery site for these particular groups and plans.

**Note:** At the time of this publication, during the reprotect option replication schedules from the recovery site B back to the protected site A are not recreated. Re-establish replication schedules from site B to site A to meet the organization SLAs put in place. Refer to the *Dell EqualLogic Storage Replication Adapter* release notes.

### 10.1.2 Test

Now that the reprotect has occurred, run a test recovery to go from the now protected site B to the recovery site A. Verify the test plan is successful before committing to failing back the environment.

### 10.1.3 Failback

Once the testing has been verified, it is time to failback to the original site A. There is no failback button since the roles of protected site and recovery site were reversed there is just the recovery option. Run the recovery to bring the virtual machines from protected site B to recovery site A as normal.

### 10.1.4 Reprotect

Once the VMs are back on site A, the promoted volumes will still need to be made permanent and replication back to site B re-established. To do this, run the reprotect function one more time to make site A the protected site again and site B the recovery site. Once this final reprotect is finished, your complete site failback is finished. Continue to run tests and update protection groups and recovery plans as needed to protect the environment.

## 10.2 Recovery scenario 2: Re-establish SRM

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

## 10.2.1 Make promotions permanent

During full recovery the replicas on the recovery 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.

1. From the Group Manager GUI on site B, 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**.

Storage pool	Capacity	Free	Drives	Pool encryption
<input checked="" type="radio"/> default		4.96 TB	3.71 TB SAS HDD	<input checked="" type="checkbox"/> None

In Step 2 you can include additional iSCSI access. The volume was already given the access control list from SRM when the volume was promoted. Choose No Access or add access control and click **Next**.

**Note:** If you select **None** it does not remove the existing access list.

What kind of access type do you want for this volume?

- Copy access controls from another volume
- Select or define access control policies
- Define one or more basic access points
- None (do not allow access)

3. 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.
4. Do this step for all volumes that were promoted during the SRM failover.  
Now that the volumes have been promoted, treat this as a new configuration for SRM with the failover site B becoming the new protected site and the original protected site A becoming a temporary recovery site.

## 10.2.2 Configure replication partnership

Since this example assumes that there is no partnership established between the current protected site B and the new recovery site A, recreate 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 B and recreate it with the new information.

## 10.2.3 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.

## 10.2.4 Create a new vSphere environment

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

## 10.2.5 Configure Site Recovery Manager

Now that 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 protecting site A.

1. Install Site Recovery Manager
2. Install the Dell EqualLogic SRM SRA
3. Configure the SRM connections
4. Configure the SRM Inventory mappings
5. Configure the SRM Array Managers
6. Delete any old Protection Groups and Recovery Plans

## 10.2.6 Configure protection groups

Once SRM is installed and configured, treat 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 A.

## 10.2.7 Configure Recovery Plans

On the new recovery 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 to be able to dictate when machines return to the original protected 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.

### 10.2.8 Reprotect the Environment

Now that everything is back onto the original protected site A, you can utilize the reprotect option to re-enable SRM protection from site A to site B. Test recovery plans to verify everything is back and the virtual environment is once again protected.

## 11 Considerations for guest 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, data isolation, 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 iSCSI volumes on the protected 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.

## 12 Summary

With today's business environment dependency on the applications, data and communications, disaster recovery is not an option but a requirement. Dell PS Series auto replication feature provides a cost effective disaster recovery solution using manual processes and lengthy detailed run books. When combined with VMware's vSphere Site Recovery Manager to automate recovery processes, and more importantly allow for non-disruptive testing of these plans, a complete DR solution can be created for any virtual environment.

# A Technical support and resources

[Dell.com/support](http://Dell.com/support) is focused on meeting customer needs with proven services and support.

[Dell TechCenter](#) is an online technical community where IT professionals have access to numerous resources for Dell EMC software, hardware and services.

[Storage Solutions Technical Documents](#) on Dell TechCenter provide expertise that helps to ensure customer success on Dell EMC Storage platforms.

## A.1 Related resources

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

Vendor	Model	Software Revision
VMware	vSphere ESXi	6.5
VMware	vCenter Server	6.5
VMware	vCenter Site Recovery Manager	6.5
Dell	Dell EqualLogic PS Series Storage	9.0
Dell	Dell EqualLogic Storage Replication Adaptor	2.3

The following table lists the documents referred to in this Technical Report.

Vendor	Document Title
VMware	VMware Site Recovery Manager Administration
VMware	VMware Site Recovery Product Documentation
VMware	VMware Site Recovery Manager Performance and Best Practices
VMware	VMware vSphere System Administrator Documentation
Dell	Dell EqualLogic PS Series Installation and Setup
Dell	Dell EqualLogic PS Series Group Administration Guide
Dell	Using Dell PS Series Asynchronous Replication
Dell	PS Series Asynchronous Replication Best Practices and Sizing Guide