

SolidFire Storage Replication Adapter User Guide

Version: 1.0

02/12/2015

TABLE OF CONTENTS

Introduction.....	4
Audience	4
Getting Started	5
Support Matrix	6
SolidFire SRA Prerequisites	6
Installing SolidFire SRA	6
Removing SolidFire SRA	9
Configuring SolidFire SRA	11
Configuring the SRM Settings	15
Using SolidFire SRA	16
Executing the SolidFire SRA Workflows	18
Viewing the SolidFire SRA and SRM Logs.....	25
Appendix A — Error Messages	28
Appendix B — Additional SolidFire SRA Tasks	31
Troubleshooting SolidFire SRA issues.....	31
Best Practices	32

Appendix C – Multiple Cluster Configurations	33
Configuring Replication to Multiple Clusters	33
Sample Working Screens of End-to-End Setup	35
Appendix D — Glossary	42
Appendix E — Related Documents	43

Introduction

This document provides information about how to install, configure, and use the SolidFire Storage Replication Adapter (SRA). This document contains features supported for the v1.0 release.

Audience

This document is intended for the administrators involved in installing, configuring, and using SolidFire SRA, or troubleshooting SRA related issues. Readers of this document should be familiar with the following:

- **SRM Administrators:** You should have training or have worked as an SRM administrator.
- **Networking:** You should be familiar with working on server networking and network storage, including IP addresses, netmasks, and gateways.

Getting Started

The SolidFire SRA integrates with the VMware Site Recovery Manager (SRM) and provides an interface to communicate with replicated SolidFire storage arrays and execute supported workflows. The SRA facilitates planned migration and disaster recovery management between protected and recovery sites. Administrators can easily use the SolidFire SRA through SRM to manage and configure replication of virtual machines with datastores hosted on the SolidFire storage clusters. The following figure provides a high-level architecture.

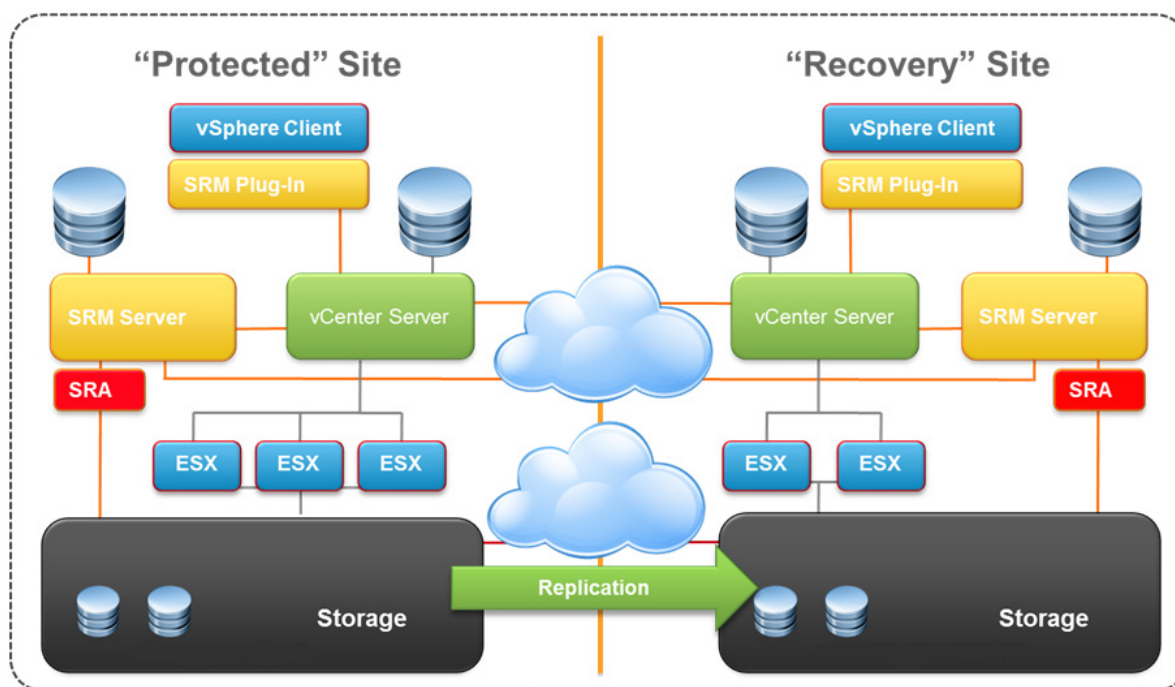


Figure 1: Site Recovery Manager (SRM) – Architecture High Level

Support Matrix

The [VMware Compatibility Guide](#) includes information about supported hardware and software, including available SolidFire node types, supported protocols, Element OS, and SRM version.

SolidFire SRA Prerequisites

This section provides the details of the prerequisites required prior to SolidFire SRA installation.

1. Install and configure VMware SRM 5.5.x or VMware SRM 5.8 on both the protected and recovery sites.
2. Create and configure the SolidFire cluster pair for replication.
3. Configure the replicated volumes on the cluster pairs.

Installing SolidFire SRA

The SolidFire SRA installer is distributed in MSI format. When you launch SolidFire_SRA_V1.0.7.msi, the installer adds the files in the user defined directories on the target machine.

The following section provides the details to install SRA at the protected and recovery site.



NOTE: You must install SolidFire SRA on both (protected and recovery) sites.

Procedure

1. Download the **SolidFire_SRA_V1.0.7** installer from the SolidFire [BrickFTP](#) site using your customer *username* and *password* credentials, and place it on the desktop of the vCenter server where SRM is installed.



NOTE: For BrickFTP access, contact SolidFire support at support@solidfire.com.

Keep the installer in case you need to uninstall the SRA in the future.

2. Double-click the **SolidFire_SRA_V1.0.7** installer from the desktop.

The *Welcome* window appears.



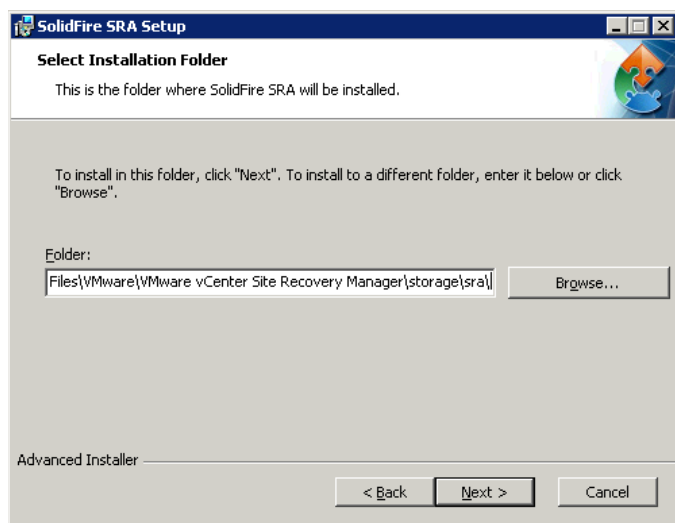
3. Click Next

The *End-User License Agreement* window appears.



4. Read and accept the terms of the license agreement and click **Next**.

The *Select Installation Folder* window appears.

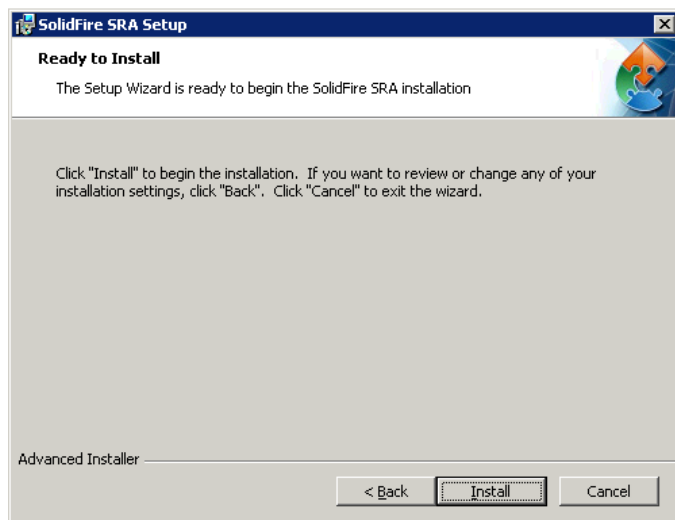


5. Select the `<VMware vCenter Site Recovery Manager install location>\storage\sra\` directory as the SRA installation location, and then click **Next**.

The *Ready to Install* window appears.

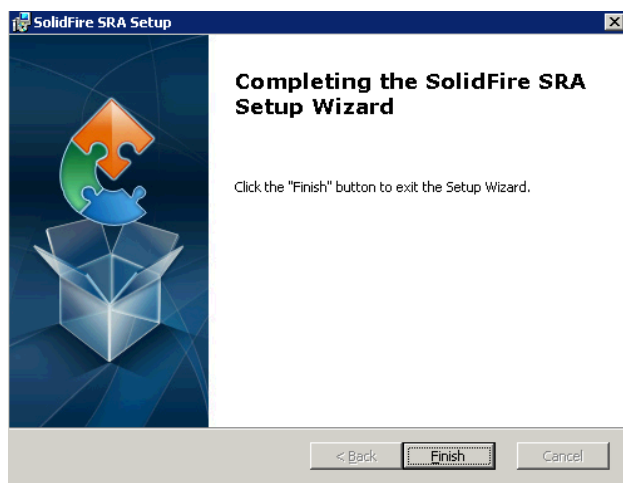


NOTE: SRM recommends installing the SolidFire SRA at the default location only.



6. Click **Install** to begin the installation.

The *Finish* window appears.



7. Click **Finish** to complete the SRA installation.

After SRA installation, verify the following:

- SolidFire SRA is installed successfully at the `<VMware vCenter Site Recovery Manager install location>\storage\sra\SolidFire` location.
- A SolidFire directory is created and the following binaries are copied into it:
 - jre7
 - Command.pl
 - solidfire_sra-1.0.<x>.jar

For details on how to configure SRA after installation, see [Configuring SolidFire SRA](#).

Removing SolidFire SRA

You can remove SolidFire SRA by either using the MSI installer or from the control panel. The following section provides instructions to remove the adapter using the installer.

Procedure

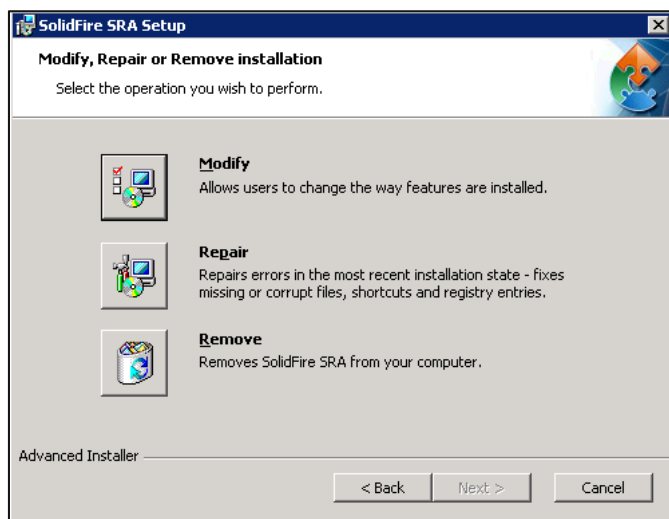
1. Double-click the `SolidFire_SRA_V1.0.7` installer.

The *Welcome* window appears.



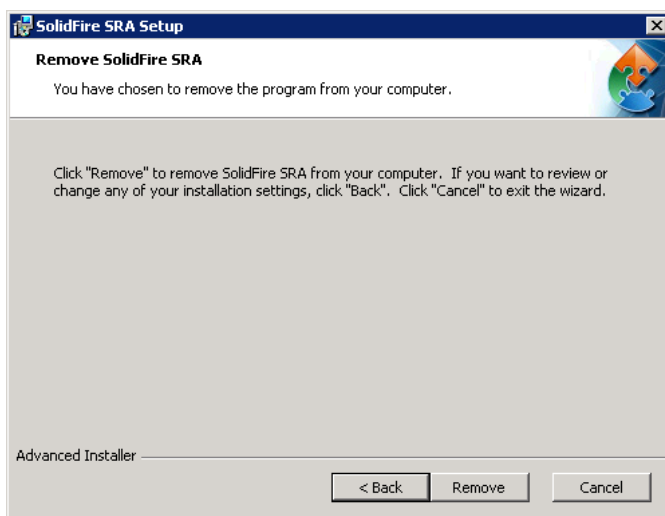
2. Click **Next**.

The *Modify, Repair or Remove installation* window appears. SRA supports the **Remove** option only.



3. Click **Remove** to remove the SolidFire SRA, and then click **Next**.

The *Remove SolidFire SRA* window appears.



4. Click **Remove** to remove the SolidFire SRA.

The **Finish** window appears.

5. Click **Finish** to remove the SRA.



NOTE: You can also remove SolidFire SRA by selecting SolidFire SRA in the Programs and Features menu in the Control Panel and clicking Uninstall.

After removing SolidFire SRA, verify that the SolidFire directory is removed from the `<VMware vCenter Site Recovery Manager install location>\storage\sra` location.

Configuring SolidFire SRA

After SolidFire SRA is installed and discovered on both (protected and recovery) sites, configure SRA to work with SRM as follows.

Procedure

1. From the home screen in vSphere Client, click the **Site Recovery** icon to open SRM and select **Array Managers**.
2. Select `<Protected Site>` in the left panel and click the **SRAs** tab in the right panel.
3. Click **Rescan SRAs**. The adapter is discovered at the protected site and the **Status** displays **OK**.

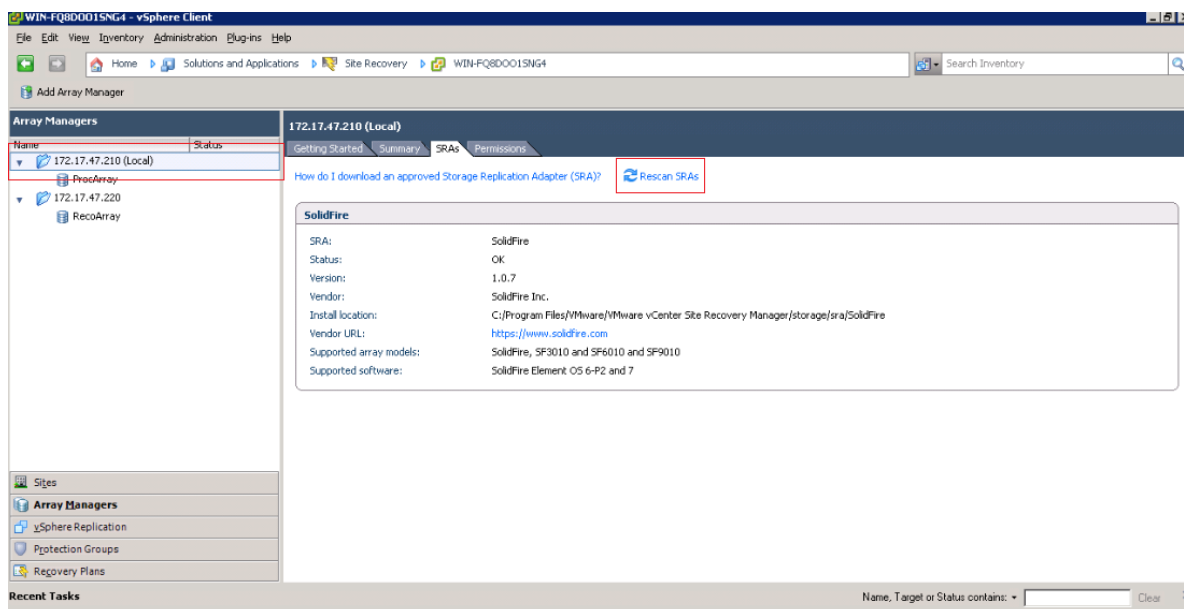


Figure 2: Rescan SRAs

4. Repeat the steps above for <Recovery Site>.
5. Add an Array Manager on both the protected and recovery sites. Do this by selecting the **Add an Array Manager** link as shown below:

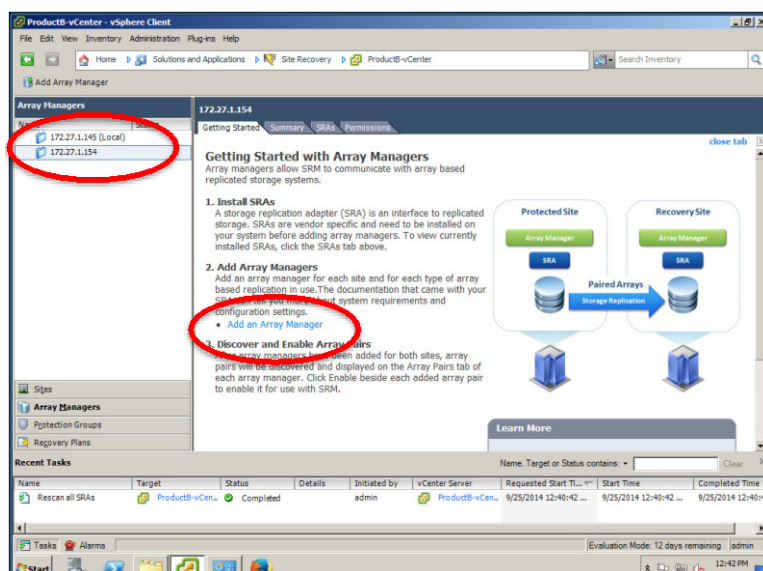


Figure 3: Add an Array Manager

6. Enter a meaningful name for the Array Manager, such as Protected_Site_Array_Manager.

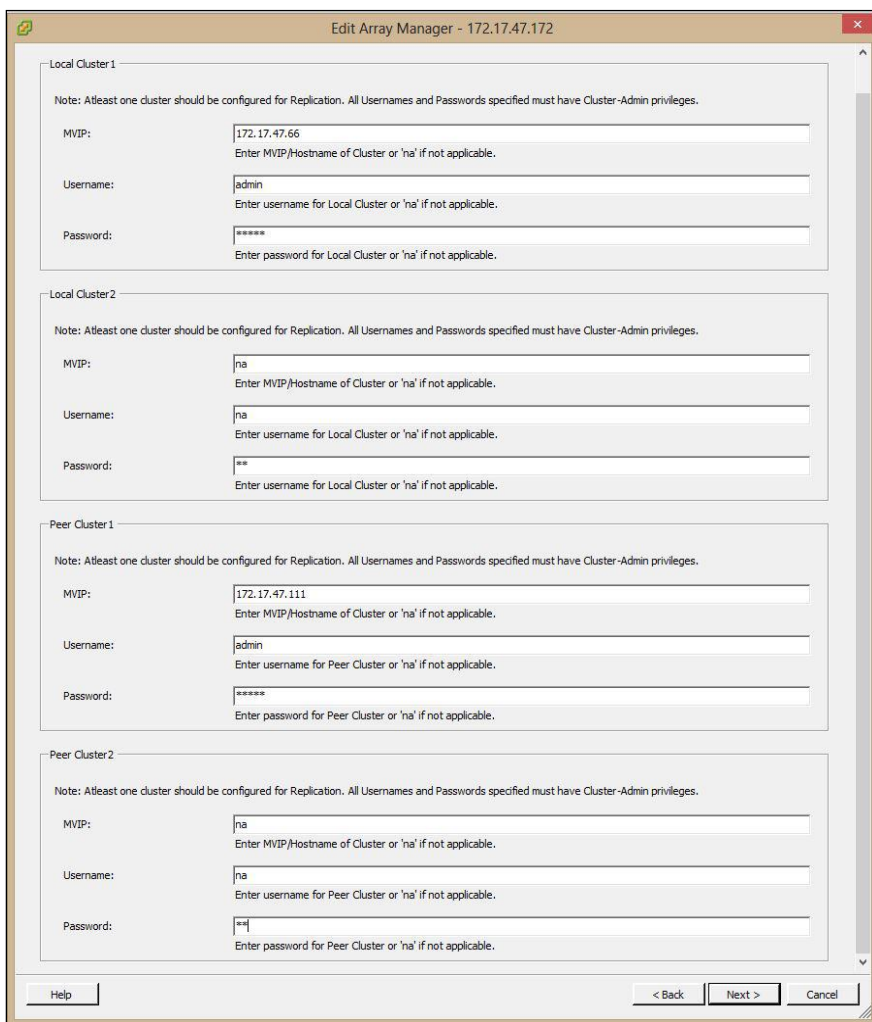


NOTE: To change logger settings, see <http://pubs.vmware.com/srm-55/index.jsp>.

7. Enter the local and peer cluster details for the protected site. Provide information for at least one local cluster and one peer cluster.

If other fields are not required, enter `na`, even in the password field.

For standard peer-to-peer configurations, where you have one protected storage cluster and one recovery storage cluster, Local Cluster 1 (see example in the following figure) will have your protected cluster and Peer Cluster 1 will have your recovery cluster. The SolidFire SRA is capable of more complex protection profiles, however. For more details on advanced configurations, see [Appendix C – Multiple Cluster Configurations](#).



The screenshot shows the 'Edit Array Manager' window for IP 172.17.47.172. It contains four sections for configuring clusters:

- Local Cluster 1:**
 - MVIP: 172.17.47.66 (Note: Enter MVIP/Hostname of Cluster or 'na' if not applicable.)
 - Username: admin (Note: Enter username for Local Cluster or 'na' if not applicable.)
 - Password: ***** (Note: Enter password for Local Cluster or 'na' if not applicable.)
- Local Cluster 2:**
 - MVIP: na (Note: Enter MVIP/Hostname of Cluster or 'na' if not applicable.)
 - Username: na (Note: Enter username for Local Cluster or 'na' if not applicable.)
 - Password: ** (Note: Enter password for Local Cluster or 'na' if not applicable.)
- Peer Cluster 1:**
 - MVIP: 172.17.47.111 (Note: Enter MVIP/Hostname of Cluster or 'na' if not applicable.)
 - Username: admin (Note: Enter username for Peer Cluster or 'na' if not applicable.)
 - Password: ***** (Note: Enter password for Peer Cluster or 'na' if not applicable.)
- Peer Cluster 2:**
 - MVIP: na (Note: Enter MVIP/Hostname of Cluster or 'na' if not applicable.)
 - Username: na (Note: Enter username for Peer Cluster or 'na' if not applicable.)
 - Password: ** (Note: Enter password for Peer Cluster or 'na' if not applicable.)

At the bottom, there are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

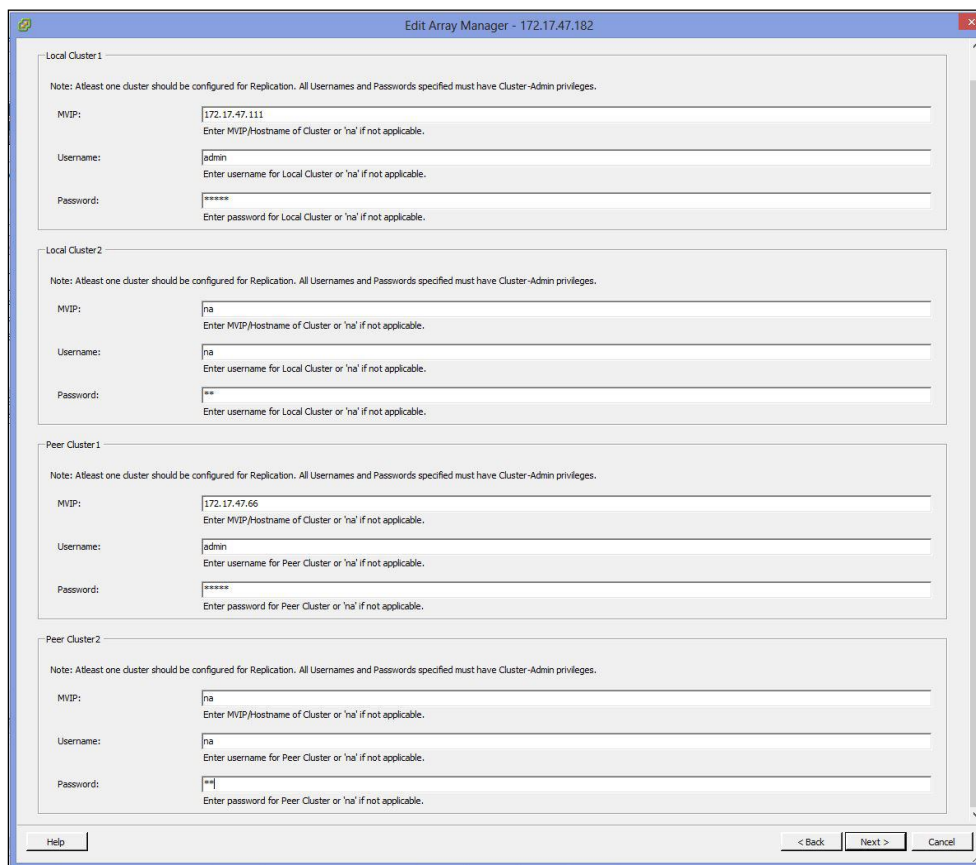
Figure 4: Enter Cluster Details for Protected Site



NOTE: You must provide valid user credentials with administrative privileges to connect to the storage.

8. Enter values for the recovery site **Array Manager** in the reverse order (see example in following figure). You must provide information for at least one local cluster and one peer cluster.

If other fields are not required, enter `na`.



The screenshot shows the 'Edit Array Manager' window with the title bar 'Edit Array Manager - 172.17.47.182'. It contains four sections for cluster configuration, each with a 'Note: At least one cluster should be configured for Replication. All Usernames and Passwords specified must have Cluster-Admin privileges.'

- Local Cluster 1:** MVIP: 172.17.47.111, Username: admin, Password: *****
- Local Cluster 2:** MVIP: na, Username: na, Password: **
- Peer Cluster 1:** MVIP: 172.17.47.66, Username: admin, Password: *****
- Peer Cluster 2:** MVIP: na, Username: na, Password: **

Each field has a placeholder text: 'Enter MVIP/hostname of Cluster or 'na' if not applicable.', 'Enter username for Local Cluster or 'na' if not applicable.', and 'Enter password for Local Cluster or 'na' if not applicable.' respectively. At the bottom, there are 'Help', '< Back', 'Next >', and 'Cancel' buttons.

Figure 5: Enter Cluster Details for Recovery Site

9. Select the added Array Manager on the left pane and click the **Array Pairs** tab.
10. Click **Enable** in the **Actions** column. The replicated device displays in the **Devices** tab. You only need to enable the array for one of the sites (protected or recovery), and the other site will automatically enable.

If any errors are displayed, see [Troubleshooting SolidFire SRA issues](#).

After the Array Managers are configured and array pairs are enabled on both the sites, the SRA shows replicated volume information in SRM.

Configuring the SRM Settings

After SolidFire SRA array managers and array pairs are established, configure SRM protection as you would do for any SRM scenario, by configuring all the pairings, placeholder datastores, protection groups and recovery plans. Details on how to accomplish these tasks are given in VMware's [SRM manual](#).

Using SolidFire SRA

SolidFire SRA provides an interface to SRM to support storage-based replication using SolidFire storage devices. By using the SolidFire SRA, SRM administrators can manage and configure replication of virtual machines hosted on the SolidFire clusters.

SolidFire SRA supports following workflows:

- View all replicated sources and targets configured on the storage arrays from protected and recovery sites.
- Perform planned migration of virtual machines with datastores on the SolidFire cluster from protected site to the recovery site.
- Perform disaster recovery of virtual machines with datastores on the SolidFire cluster from the protected site to the recovery site.
- Reprotect virtual machines with datastores after failover from the recovery site. You can get back the virtual machines to original protected sites with datastore after failover to recovery site.
- Cleanup placeholders created while simulating a failover.
- View SolidFire SRA and SRM message logs.

SolidFire SRA Workflows

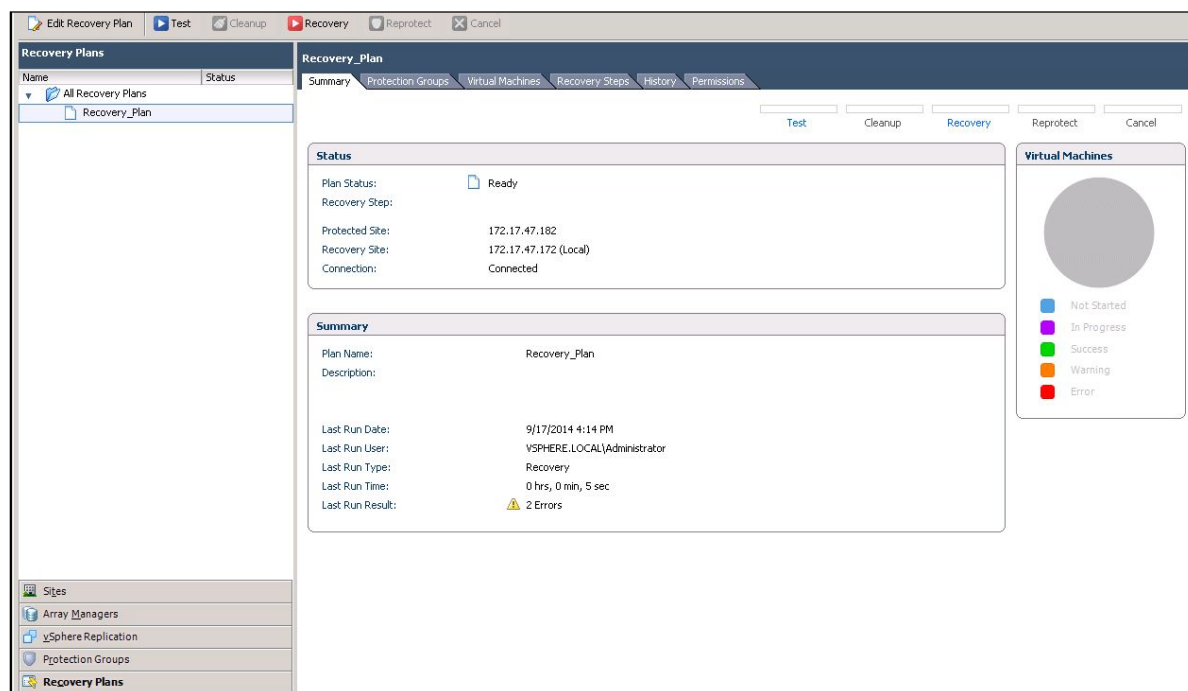


Figure 6: SolidFire SRA landing page

SolidFire SRA is used to manage the discovered clusters and supports the following workflows:

Test: Click to perform a test recovery of virtual machines with datastores on SolidFire cluster from protected site to the recovery site.

Cleanup: Click to cleanup placeholders used while simulating non-disruptive test failover. The link is active only when a Test workflow is performed.

Recovery: Click to perform recovery of virtual machines from protected to recovery sites.

Reprotect: Click to reprotect the virtual machines with datastores after failover from the recovery site. The link is active only after a Recovery workflow is performed.

Cancel: Click to cancel the ongoing workflow.

Executing the SolidFire SRA Workflows

This section provides the details to execute the following SolidFire SRA workflows:

- Test
- Cleanup
- Recovery
- Reprotect

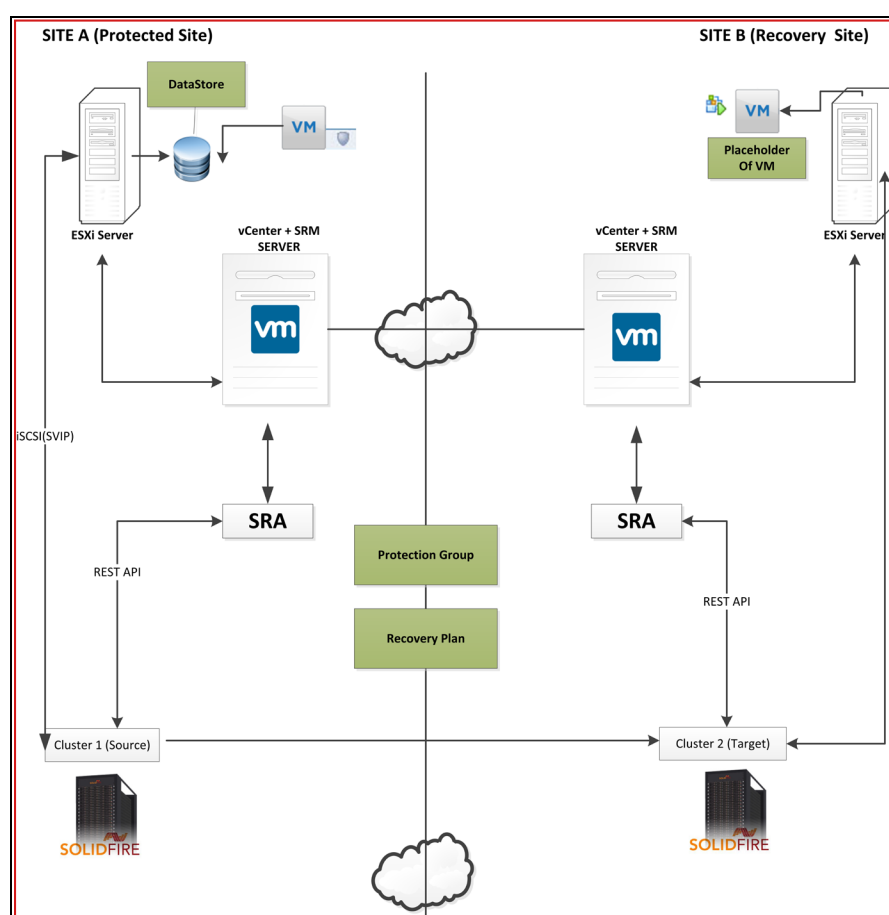


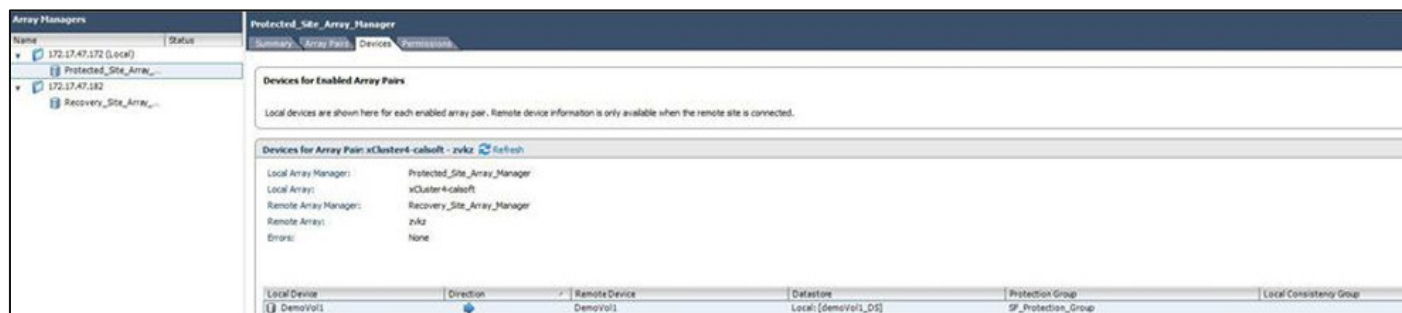
Figure 7: Test and Recovery Workflow Configuration

After execution of any workflow, you can view the execution details in the **History** tab. You can export the test result in the SRM supported format.

Prerequisites

1. Create a datastore and create a virtual machine (VM) whose VMDK resides on that datastore.
2. Create a **Protection Group** and recovery plan and provide a valid name to them.

3. Ensure that you are able to view the device in the **Devices** tab.



4. The arrow indicates that the replication is configured from the protected site to the recovery site.

Executing a Test Workflow

The test workflow is a simulation of an entire configuration of the virtual machines from the protected sites to the recovery sites in a non-disruptive environment. This helps you to confirm that the configuration has been setup correctly for the protected virtual machines. Instead of disabling or deactivating the main production datastore(s), SRM will create a copy that can run in parallel with production for testing.

When you start the test workflow, a simulated failover is executed and SRM ensures that the protected VMs at the protected site are not subject to any interruption during a test workflow execution. SolidFire SRA enables that workflow by translating SRM actions into SolidFire commands.

Procedure

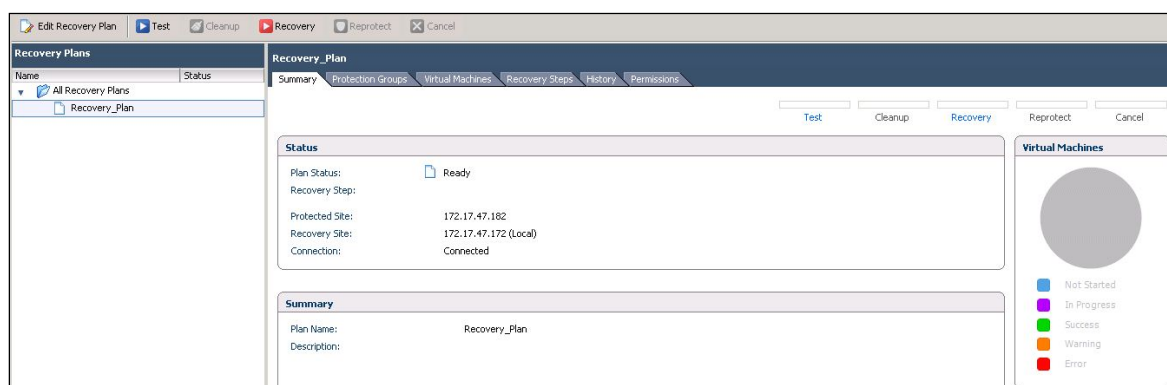
1. Select the required site and click **Recovery Plans**.

The available plans display in the left navigation pane.

2. Select the required plan.

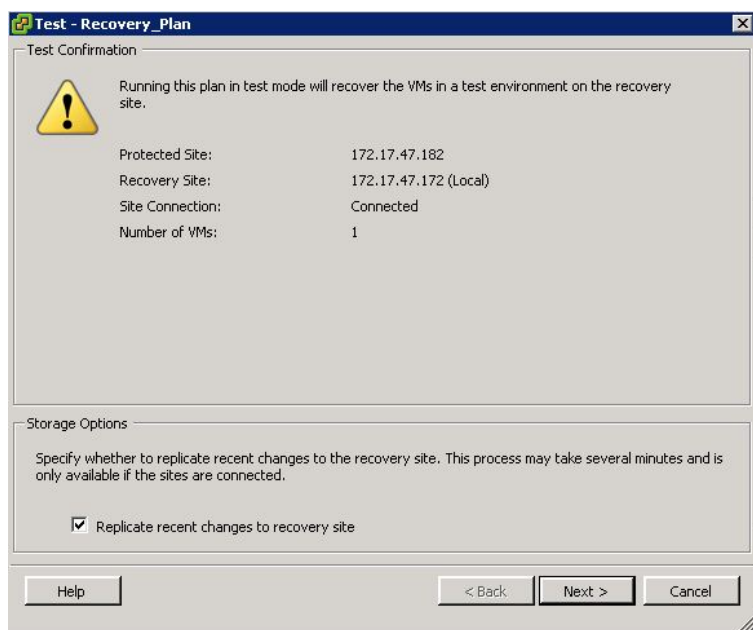


NOTE: The Plan Status should be *Ready*. Click the **Recovery Steps** tab to view the execution details.



3. Click the **Test** workflow.

The **Test Confirmation** window appears displaying the protected and recovery site IPs and the connection status.



4. In the **Storage Options** section, check the **Replicate recent changes to recovery site** checkbox if you need to replicate the changes to the recovery site and click **Next**.
5. Review the test recovery details and click **Start** to start the **Test** workflow.

You can view the details of the test recovery in the **Status** section. You can cancel the test recovery workflow by clicking **Cancel** at any time.

Cleaning up the Placeholders

The Cleanup workflow cleans up the placeholders created during simulation of non-disruptive test failover.

Prerequisites

- Test workflow must be executed.

Procedure

1. Select the required site and click **Recovery Plans**.
The available plans appear in the left navigation pane.
2. Select the required plan.



NOTE: The Plan Status should be *Ready*. Click the **Recovery Steps** tab to view the execution details.

3. Click the **Cleanup** link. The placeholders created during **Test** workflow are cleaned up.

Performing Recovery

After installing SolidFire SRA, you can run a recovery plan under planned circumstances to recover virtual machines from the protected site to the recovery site. You can also run a recovery plan under unplanned circumstances if the protected site suffers an event that might result in data loss.

SolidFire SRA supports the following recovery types:

- **Planned Migration:** Planned migration includes planned decommissioning of virtual machines at the protected site and commissioning them at the recovery site. Both (protected and recovery) sites must be up and running.
- **Disaster Recovery:** Disaster recovery restores the virtual machines on the recovery site when the protected site goes down.

Procedure

1. Select the required site and click **Recovery Plans**.

The available plans appear in the left navigation pane.

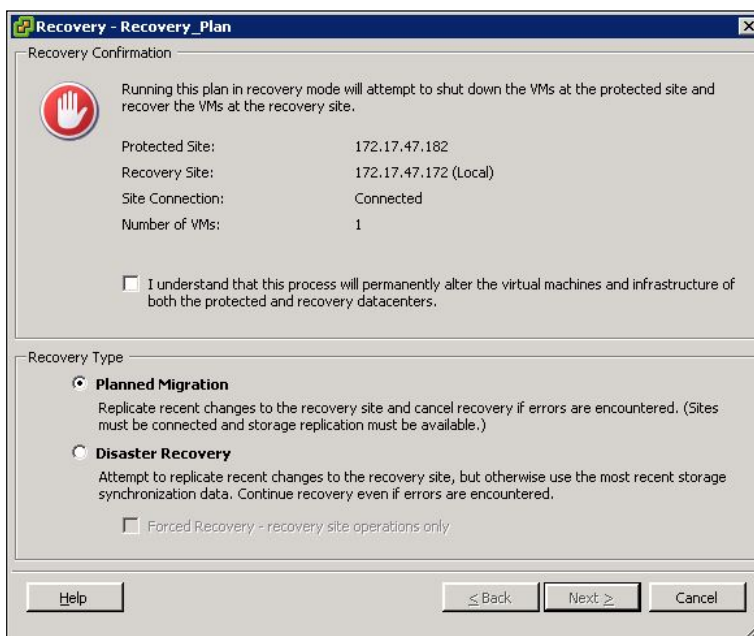
2. Select the required plan.



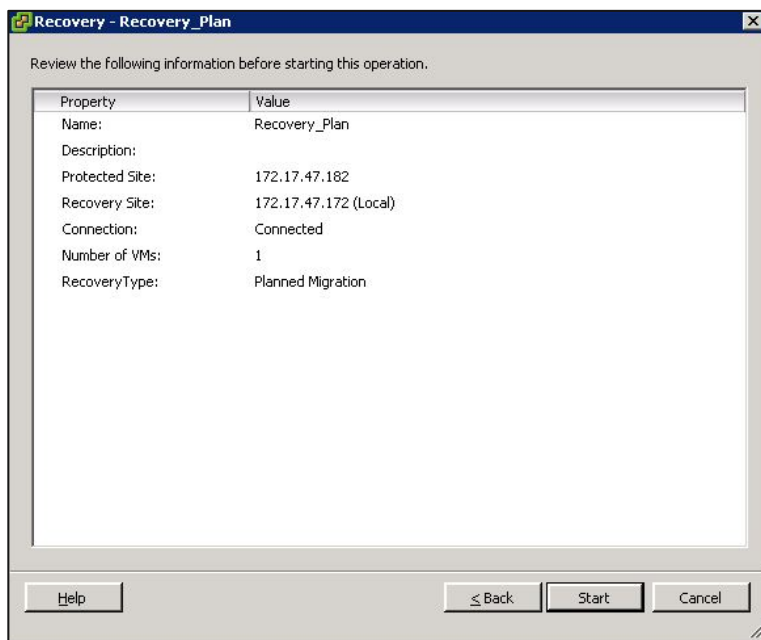
NOTE: The Plan Status should be *Ready*. Click the **Recovery Steps** tab to view the execution details.

3. Click **Recovery**.

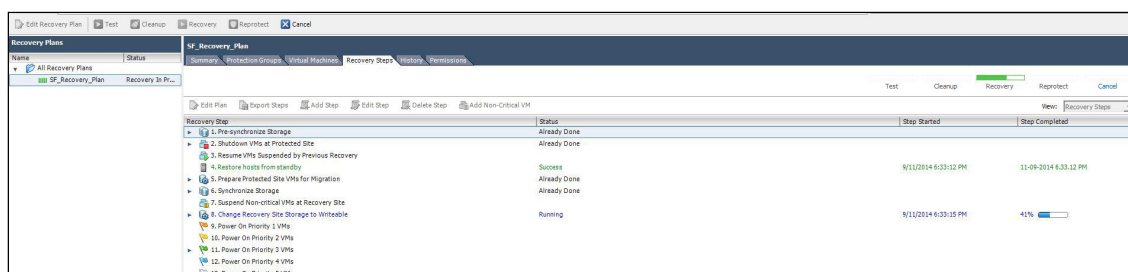
The **Recovery Confirmation** window appears and includes the protected and recovery site IPs and the connection status.



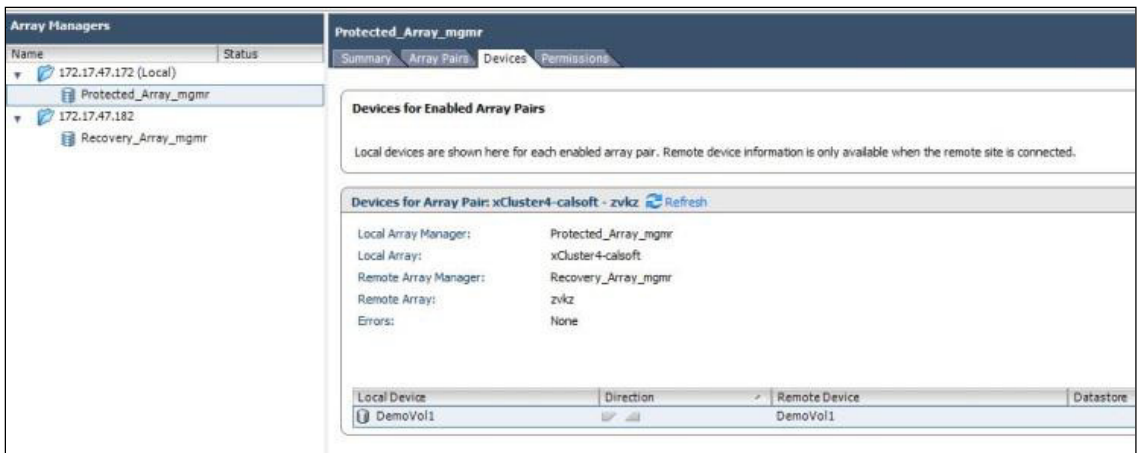
4. In the **Recovery Type** section, click **Planned Migration** or **Disaster Recovery** as required.
5. In the **Recovery Confirmation** section, select the confirmation checkbox to proceed further with the recovery and then click **Next**.
6. Review the recovery details and click **Start** to start the recovery.



You can view the details of the recovery in the **Status** section. You can cancel the recovery workflow by clicking **Cancel**.



After **Recovery**, the replication is broken between the devices as follows.



Reprotecting a Site

SolidFire SRA allows you to protect virtual machines with datastores after failover from the recovery site. A reverse workflow is followed where the recovery site works as Site A and protected site works as Site B.



NOTE: You can execute the **Reprotect** workflow only after a **Recovery** workflow is executed.

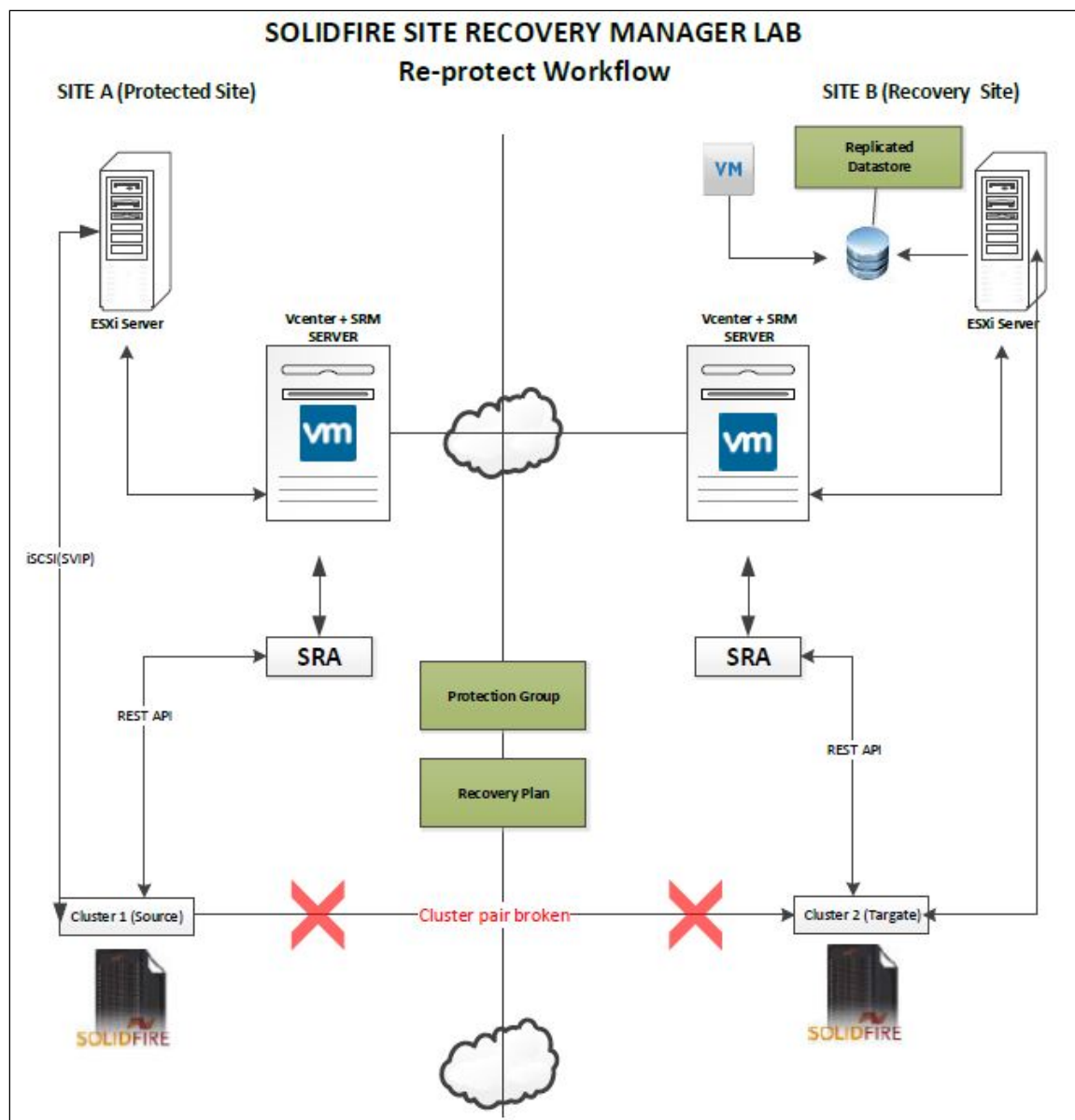


Figure 8: The Reprotect Workflow

Prerequisites

Recovery workflow must be executed.

Procedure

1. Select the required site and click **Recovery Plans**.
The available plans appear in the left navigation pane.
2. Select the required plan and select **Array Managers**.



NOTE: The Plan Status should be *Ready*. Click the **Recovery Steps** tab to view the execution details.

3. Click **Reprotect**.

You can view the details of the reprotect workflow in the **Status** section. You can cancel the reprotect workflow by clicking **Cancel**. After the **Reprotect** workflow, the direction of replication is reversed as follows.



The screenshot shows the 'Array Managers' section on the left with a tree view containing 'Protected_Array_mgr' and 'Recovery_Array_mgr'. The main panel displays the 'Protected_Array_mgr' configuration under the 'Summary' tab. It shows the 'Devices for Enabled Array Pairs' section, which includes a table for 'Devices for Array Pair: xCluster4-calsoft - zvklz'. The table lists the Local Array Manager as 'Protected_Array_mgr', the Local Array as 'xCluster4-calsoft', the Remote Array Manager as 'Recovery_Array_mgr', the Remote Array as 'zvklz', and the Errors as 'None'. Below this, there is a table for 'Local Device' and 'Remote Device' showing the direction of replication from 'DemoVol1' to 'DemoVol1' with a 'Datastore' of 'Remote:[snap-1211e3fa-demovol1_ds]'.

Local Device	Direction	Remote Device	Datastore
DemoVol1	→	DemoVol1	Remote:[snap-1211e3fa-demovol1_ds]

Viewing the SolidFire SRA and SRM Logs

SRA Logs

The SolidFire SRA exports log messages into a log file. Command requests sent by SRM to SRA are logged in a standard SRA log file.

The log file is saved in the `solidfire_sra_<year>_<month>_<date>.log` format; for example, as `solidfire_sra_2014_08_21.log`.

You can view the log file in the `<VMware vCenter Site Recovery Manager install location>\Logs\SRAs\solidfire` directory as follows.

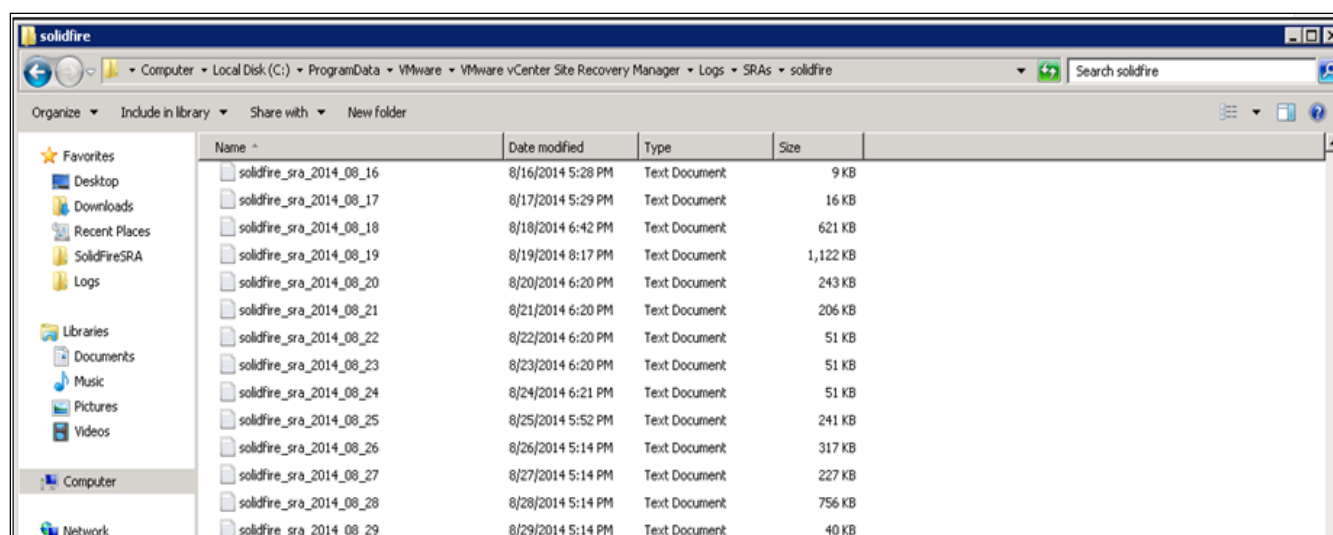


Figure 9: SRA Logs Location

SRM Logs

Logging messages specific to SRM are saved in the <VMware vCenter Site Recovery Manager install location>\Logs\ directory.

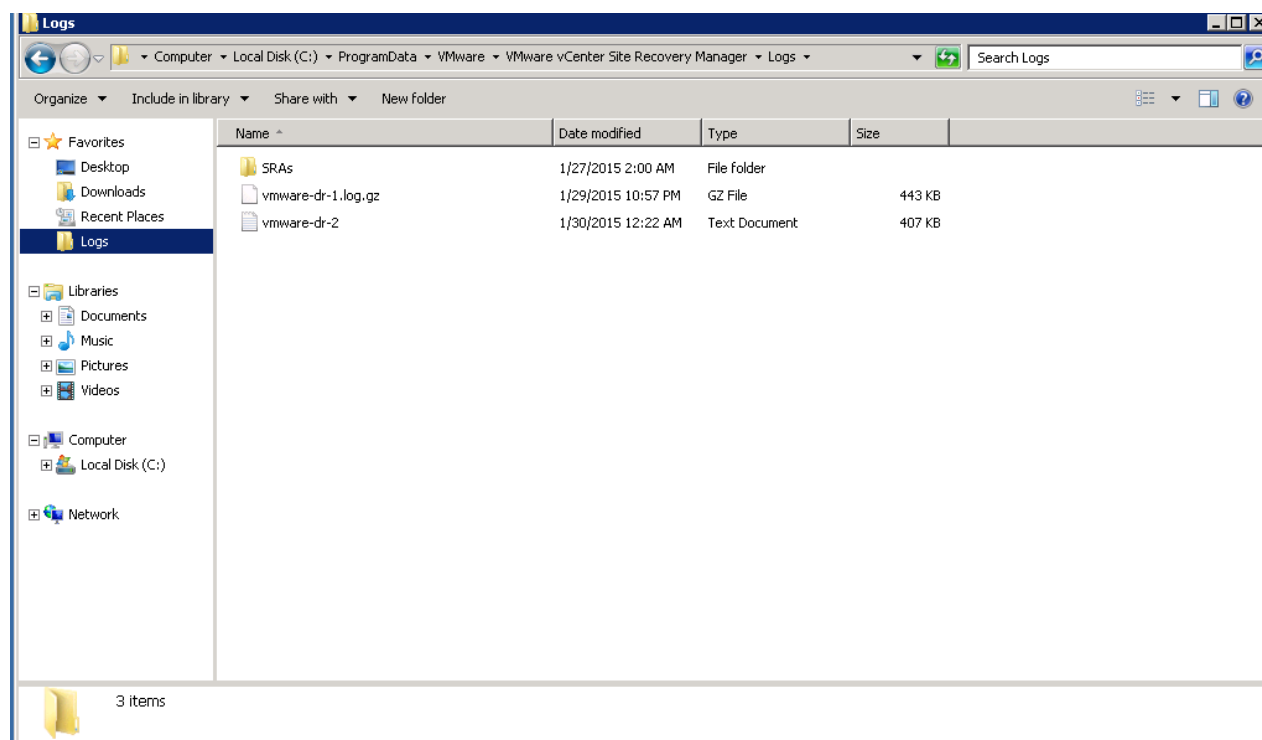


Figure 10: SRM Logs Location

You might encounter an error message while using SolidFire SRA with SRM. The user interface of SRM displays the error log messages and possible solutions. You can use the log files of SRM and SolidFire SRA to troubleshoot issues that you might encounter while using SolidFire SRA. For details about error messages, see [Appendix A — Error Messages](#).

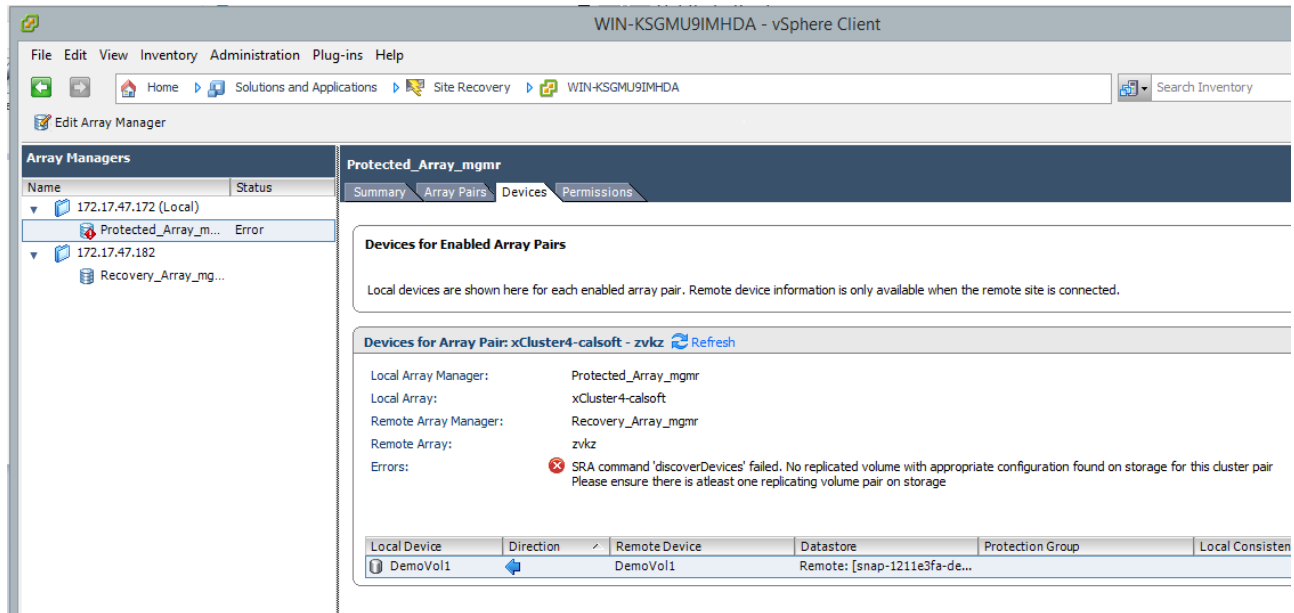


Figure 11: Viewing Error Log Message in SRM UI

Appendix A — Error Messages

SolidFire SRA displays the following error messages when an error is encountered:

Error Code	Error Message	Cause	Action
1001	Authentication fail due to incorrect username or password	The username or password of storage array is invalid.	Ensure that you provide a valid username and password in the connection parameters of the Array Manager.
1003	Connection timeout while connecting to cluster. Check if the IP/Hostname is entered correctly	Either the storage array is down or provided IP address is incorrect.	Ensure that the storage array is up and running and the IP address of the storage array is reachable. Also, make sure the credentials are correct.
1004	Cluster pairing is not there between local and peer clusters	Cluster pairing is not configured between the specified arrays in the SRA input.	Ensure that the cluster pairing is configured between the specified local and peer clusters in the SRA input.
1005	Invalid IP Address entered.	The IP address provided for the storage system is either null or invalid.	Provide a valid IP address of the storage system.
1006	Username or password cannot be empty	The username or password provided for the storage system is null.	Provide a valid username or password of the storage system.
1007	Hostname or IP Address cannot be empty	The IP address or hostname provided for the storage system is null.	Provide a valid IP address or hostname of the storage system.
1008	Volume is either inactive or not paired correctly	The error message displays for the following conditions: • Volume pairing is not configured on the device. • The device provided in the input is not in the active state. • The device provided in the input does not exist.	Ensure that the volume exists on the storage, is in active state, and is paired with the volume on the peer cluster on storage.
1009	Replicated device not found on storage. Device-Id not found	The device provided in the input does not exist on storage.	Ensure that the volume exists on storage.
1010	Replicated Target Device on storage is in inactive state.	The device provided in the input is not active on the storage.	Ensure that the volume is in active state.
1011	User has permission denied.	The user does not have permission to connect to the storage.	Provide valid user credentials with the administrative privileges.
1012	API Exception - Error while executing command. Please check log file for details	Error occurred while executing the REST API command from SRA.	For more details about the error, see the SRA Logs .

1013	Snapshot could not be deleted.	The error message displays for one of the following conditions: - Specified snapshot does not exist on storage. - Exception occurs while deleting snapshot on storage from SRA.	For more details about the error, see the SRA Logs .
1014	Cloned Volume could not be deleted.	The error message displays for the following conditions: - Specified volume does not exist on storage. - Exception occurs while deleting cloned volume on storage from SRA.	For more details about the error, see the SRA Logs .
1015	Peer ArrayID and actual Peer Storage ArrayID do not match.	Peer array ID in the SRM input is invalid.	Check the SRA logs and make sure that the provided array IP exists on the storage.
1016	Primary ArrayID and actual Primary Storage ArrayID do not match.	The primary array ID in the SRM input is invalid.	Check the SRA logs and make sure that the provided array IP exists on the storage.
1017	No volumes are configured for replication.	Volume pairing is not configured on the device.	Ensure that the volume pairing is configured at least between one pair of volume on the storage.
1018	No Cluster Pairing found for given storage cluster ID.	Cluster pairing for the specified storage cluster ID is not found on the storage.	Ensure that there exists at least one cluster pair for the specified cluster ID in the SRM input.
1019	No replicated volume with appropriate configuration found on storage for this cluster pair	The error message displays for the following conditions: - Volume pairing is not configured for the specified cluster pair in the SRM input. - The volumes paired on the storage are not in the active state.	Ensure there is at least one replicating volume pair on the storage in the active state.
1020	Requested target device does not exist	The device provided in the input does not exist on storage.	Ensure that the device specified in the SRM input exists on storage.
1021	Local and Peer Clusters cannot be configured with same MVIP/Hostname.	The local and peer clusters specified have same MVIP/Hostname.	Ensure that the source and destination MVIP/Hostname are different. SRA does not support cluster pairing with same MVIP/Hostname.
1022	Administrative user are not found	The user provided does not have permission for connecting with the storage.	Provide a valid username with administrative privileges and execute the <code>discoverArray</code> command with admin user privileges.
1023	User do not have administrative privileges	The user does not have permission to connect to the storage.	Provide a valid username with administrative privileges and execute the <code>discoverArray</code> command with admin user privileges.

1024	At least one Local Cluster details and one Peer Cluster details are mandatory.	The MVIP/Hostname, username and password provided for the local and peer cluster are null.	Make sure that you at least provide details of one local and one peer cluster while configuring array with SRM.
1025	Requested device does not exist.	The provided device does not exist on the storage.	Ensure that the device specified in the SRM input exists on the storage.
1026	Requested device was not failed over.	Either the device is not in the active state or is not mapped properly.	Ensure that the device is in the active state and is mapped or promoted/demoted properly.
1027	Volume pair state is in inconsistent state. Please correct the state	Volume pairing between the volumes on storage is not in active state.	Ensure that the volume pairing state is consistent.
1028	SyncId and ID in the request does not match	SyncId might not be present on the storage system.	Check the SRM logs to verify the SyncId.
1029	Source Device mentioned is not valid	If the source device ID is other than an integer, the error displays.	Ensure that you provide the source device ID as an integer.
1030	Request is not valid	The error displays if the request is invalid.	Ensure that you provide the correct request.

Appendix B — Additional SolidFire SRA Tasks

Troubleshooting SolidFire SRA issues

Recovery Plan Times Out While Waiting for VMware Tools

Running a recovery plan fails with a timeout error while waiting for the VMware Tools to start.

Issue

Recovery operations fail at the Waiting for VMware Tools step of a recovery plan.

Cause

SRM uses VMware Tools heartbeat to discover when recovered virtual machines are running on the recovery site. Recovery operations require that you install VMware Tools on the protected virtual machines. Recovery fails if you did not install VMware Tools on the protected virtual machines, or if you did not configure SRM to start without waiting for VMware Tools to start.

Solution

Install VMware Tools on the protected virtual machines. If you do not or cannot install VMware Tools on the protected virtual machines, you must configure SRM such that it does not wait for VMware Tools to start in the recovered virtual machines.

If protected virtual machines do not have VMware Tools installed, set the `recovery.powerOnTimeout` value to `zero` in the advanced settings of SRM on both sites.

For further details to Change Recovery Settings, see [VMware Documentation Center](#).

Failure or Reconfiguration on the Configured Array Manager from Backend

Issue

A problem is faced in the cluster nodes of array from backend or reconfiguration of storage.

Cause

The Array ID changes on failure or reconfiguration due to which the array pairing breaks.

Solution

To resolve this issue, remove the Array Manager and add Array Manager again with correct credentials.

A Workflow Fails

Issue

A workflow fails due to stale entries in the underneath volume of the datastore in which VM is configured.

Cause

Volume on the storage has been deleted. VMware continues to report the virtual machine that was a part of a datastore (volume). Reconfiguration of the array from backend and removing volume, in which the VM is created with protected group, retains back stale entries in the volume.

Solution

The VM and the underlined datastore with stale entries should be deleted. New volume should be mapped from backend and the new VM should be created with new protection group on that datastore. Start the workflow again.

Best Practices

1. Do not change the access level of volumes from the cluster side. This is applicable for both the protected and recovery clusters.
2. For replicating volumes, avoid volume misconfiguration such as modifying or deleting a volume from the backend (SolidFire management UI). If you face such a problem, you must reconfigure the whole setup again starting from the SRM workflows.
3. The replicating volume status must be active while starting the SRM workflows.

Appendix C – Multiple Cluster Configurations

Configuring Replication to Multiple Clusters

This section provides the details to configure replication to multiple clusters with scenarios.

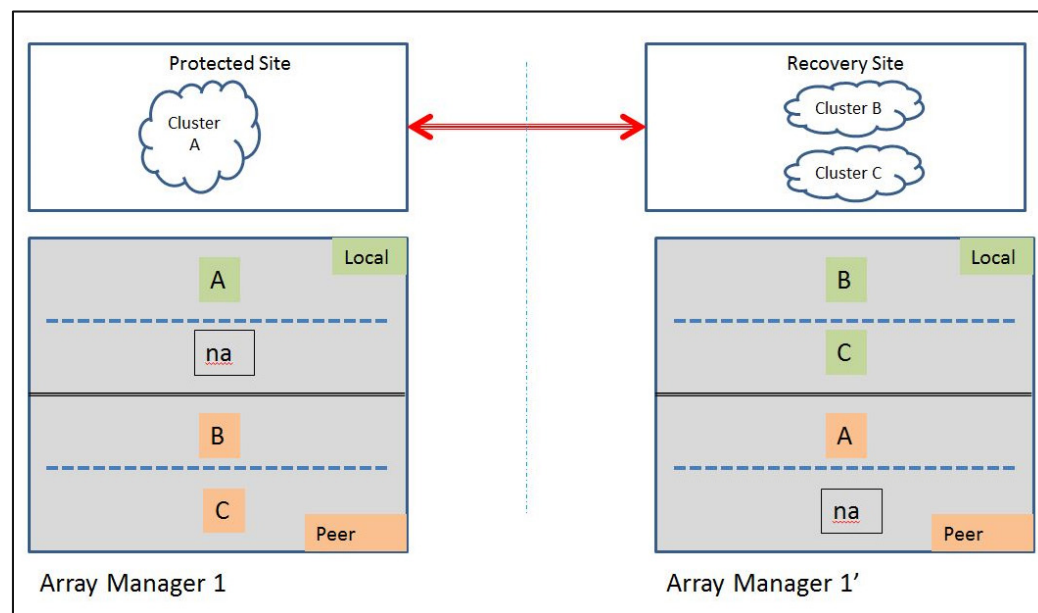
1. An Array Manager should be configured for each cluster on the protected site. Therefore, if there are two clusters deployed on the protected site, then there must be two Array Managers at both sites.
2. Clusters that are locally present at that particular site go in the first half of the configuration page of the Array Manager at that site. Clusters that are remote to that particular site shall be configured in the lower half.

For example, if Cluster A is present on the protected site and Clusters B and C are present on the recovery site; while filling the configuration page for Array Manager on protected site:

- Cluster A is local, and, hence is filled in the first half of the configuration page
 - Clusters B and C are remote, and hence are entered in the lower half of the Array Manager window.
 - Similarly, while filling the configuration page for Array Manager on the recovery site, Clusters B and C are local and Cluster A is remote.
3. The configuration page is the same for both protected site and the recovery site.

Scenario 1

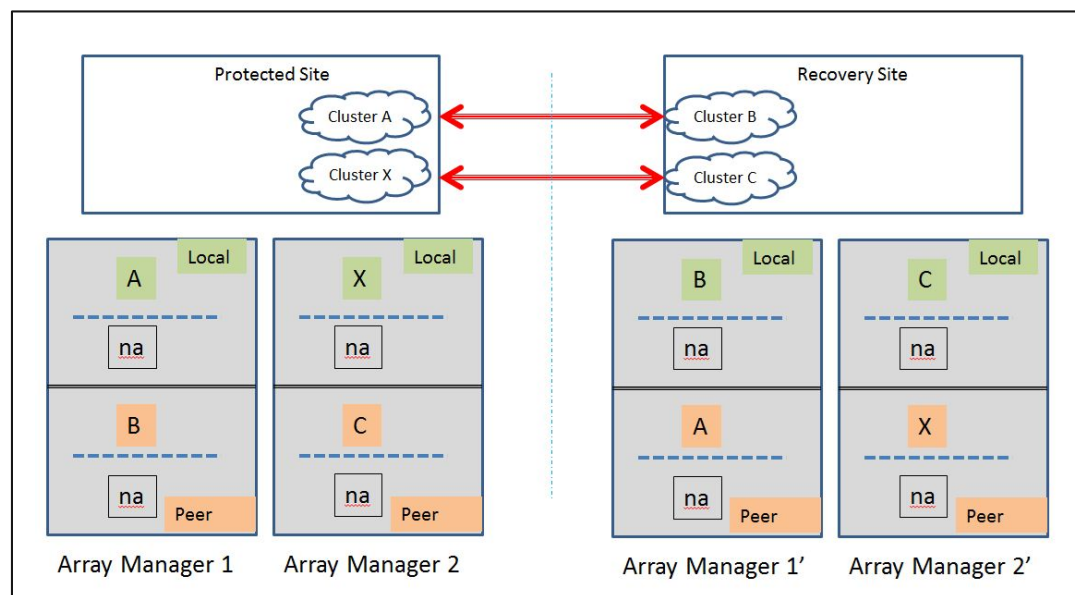
Cluster A on protected site paired with both Cluster B and Cluster C on recovery site.



Scenario 2

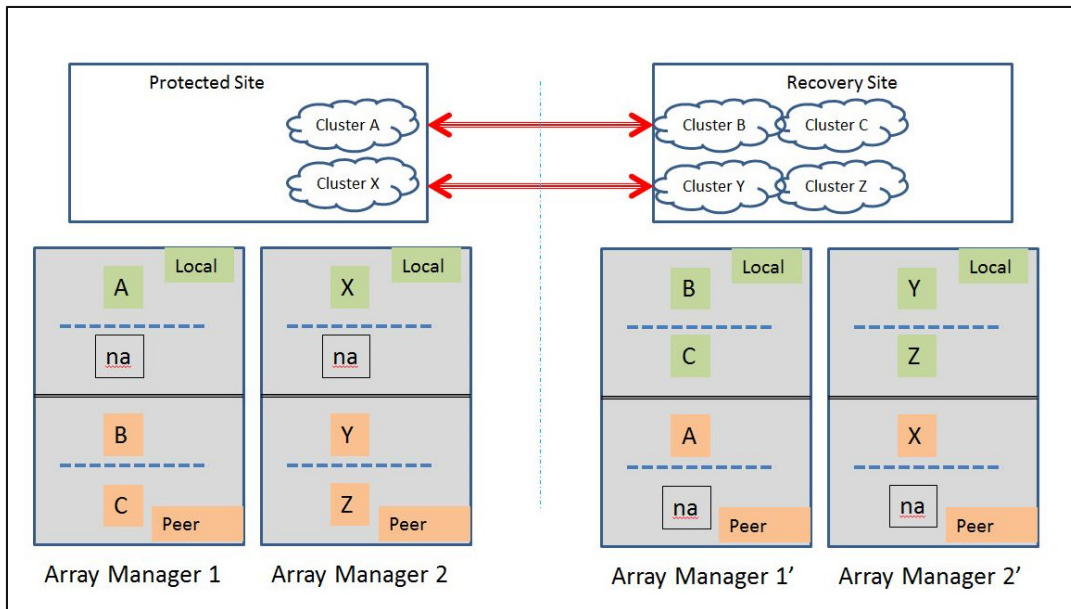
Cluster A on protected site paired with both Cluster B and Cluster C on recovery site.

- Cluster A on protected site paired with Cluster B on recovery site.
- Cluster X on protected site paired with Cluster C on recovery site.



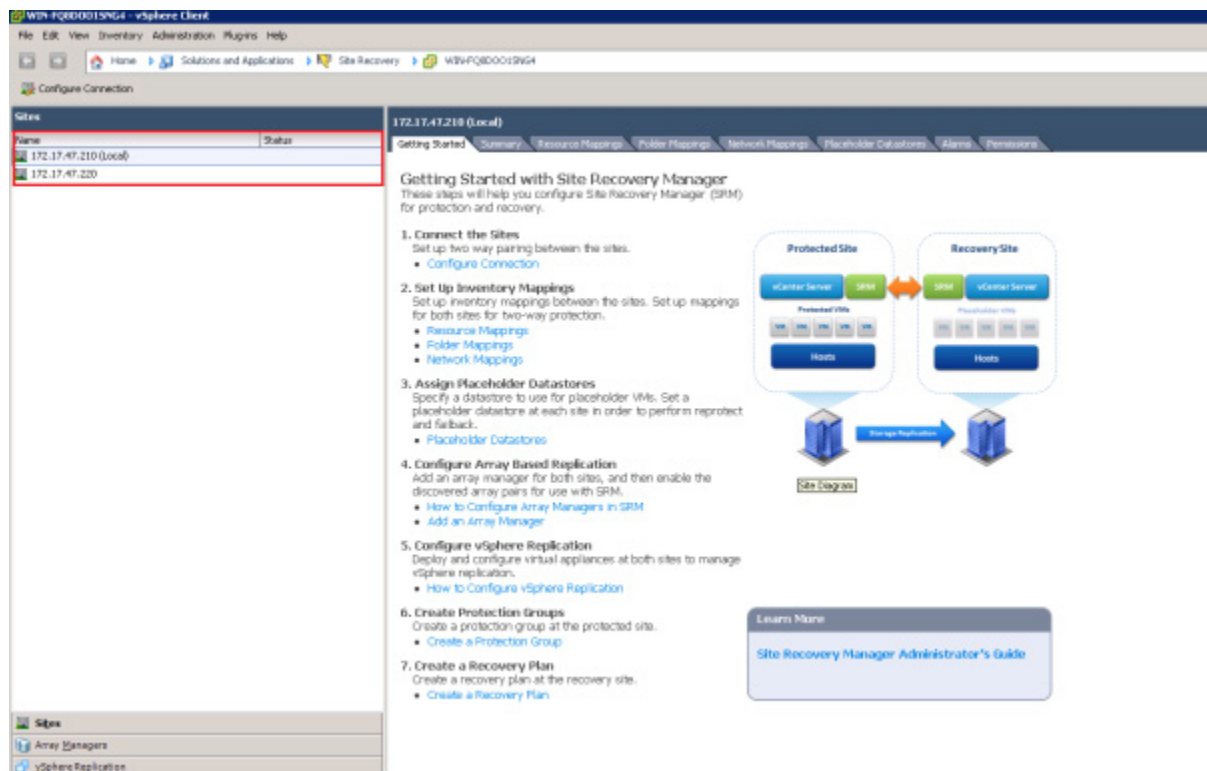
Scenario 3

- Cluster A on protected site paired with both Cluster B and Cluster C on recovery site.
- Cluster X on protected site paired with both Cluster Y and Cluster Z on recovery site.



Sample Working Screens of End-to-End Setup

Configuration Connected



The screenshot shows the VMware vSphere Client interface with the Site Recovery Manager (SRM) configuration steps displayed. The left sidebar shows the navigation tree with "Sites" selected. The main content area displays the "Getting Started with Site Recovery Manager" wizard.

Getting Started with Site Recovery Manager

These steps will help you configure Site Recovery Manager (SRM) for protection and recovery.

- 1. Connect the Sites**
Set up two way pairing between the sites.
• [Configure Connection](#)
- 2. Set Up Inventory Mappings**
Set up inventory mappings between the sites. Set up mappings for both sites for two-way protection.
• [Resource Mappings](#)
• [Folder Mappings](#)
• [Network Mappings](#)
- 3. Assign Placeholder Datastores**
Specify a datastore to use for placeholder VMs. Set a placeholder datastore at each site in order to perform reprotect and failback.
• [Placeholder Datastores](#)
- 4. Configure Array Based Replication**
Add an array manager for both sites, and then enable the discovered array pairs for use with SRM.
• [How to Configure Array Managers in SRM](#)
• [Add an Array Manager](#)
- 5. Configure vSphere Replication**
Deploy and configure virtual appliances at both sites to manage vSphere replication.
• [How to Configure vSphere Replication](#)
- 6. Create Protection Groups**
Create a protection group at the protected site.
• [Create a Protection Group](#)
- 7. Create a Recovery Plan**
Create a recovery plan at the recovery site.
• [Create a Recovery Plan](#)

Learn More
[Site Recovery Manager Administrator's Guide](#)

The diagram on the right shows the Protected Site and Recovery Site connected via Site Recovery Manager, with a Site Diagram below it.

Resource Mapping

WIN-FQ8D001SNG4 - vSphere Client

File Edit View Inventory Administration Plug-ins Help

Home Solutions and Applications Site Recovery WIN-FQ8D001SNG4 Search Inventory

Configure Connection

Sites

Name	Status
172.17.47.210 (Local)	
172.17.47.220	

172.17.47.210 (Local)

Getting Started Summary Resource Mappings Folder Mappings Network Mappings Placeholder Datastores Alarms Permissions

Map resources from 172.17.47.210 (Local) to resources at 172.17.47.220.

Mappings specified here will be used to determine the resources for protected virtual machines when they are recovered to 172.17.47.220.

Configure Mapping Remove Mapping Refresh

Protected Site Resource	Recovery Site Resource	Recovery Site Path
WIN-FQ8D001SNG4	WIN-MI4L2RRM34H	WIN-MI4L2RRM34H/
Protected_DC		
Prot_cluster	Reco_cluster	WIN-MI4L2RRM34H/Recovery_DC/
Prot_RP	Reco_RP	WIN-MI4L2RRM34H/Recovery_DC/Reco_cluster/

Sites

- Array Managers
- vSphere Replication
- Protection Groups
- Recovery Plans

Recent Tasks

Name, Target or Status contains: Clear X

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time	Completed Time
------	--------	--------	---------	--------------	----------------	----------------------	------------	----------------

Tasks Alarms Evaluation Mode: 52 days remaining Administrator

Folder Mapping

WIN-FQ8D001SNG4 - vSphere Client

File Edit View Inventory Administration Plug-ins Help

Home Solutions and Applications Site Recovery WIN-FQ8D001SNG4 Search Inventory

Configure Connection

Sites

Name	Status
172.17.47.210 (Local)	
172.17.47.220	

172.17.47.210 (Local)

Getting Started Summary Resource Mappings Folder Mappings Network Mappings Placeholder Datastores Alarms Permissions

Map folders from 172.17.47.210 (Local) to folders at 172.17.47.220.

Mappings specified here will be used to determine the location for protected virtual machines when they are recovered to 172.17.47.220.

Configure Mapping Remove Mapping Refresh

Protected Site Resource	Recovery Site Resource	Recovery Site Path
WIN-FQ8D001SNG4	WIN-MI4L2RRM34H	WIN-MI4L2RRM34H/
Protected_DC		
Discovered virtual machine	Discovered virtual machine	WIN-MI4L2RRM34H/Recovery_DC/

Sites

- Array Managers
- vSphere Replication
- Protection Groups
- Recovery Plans

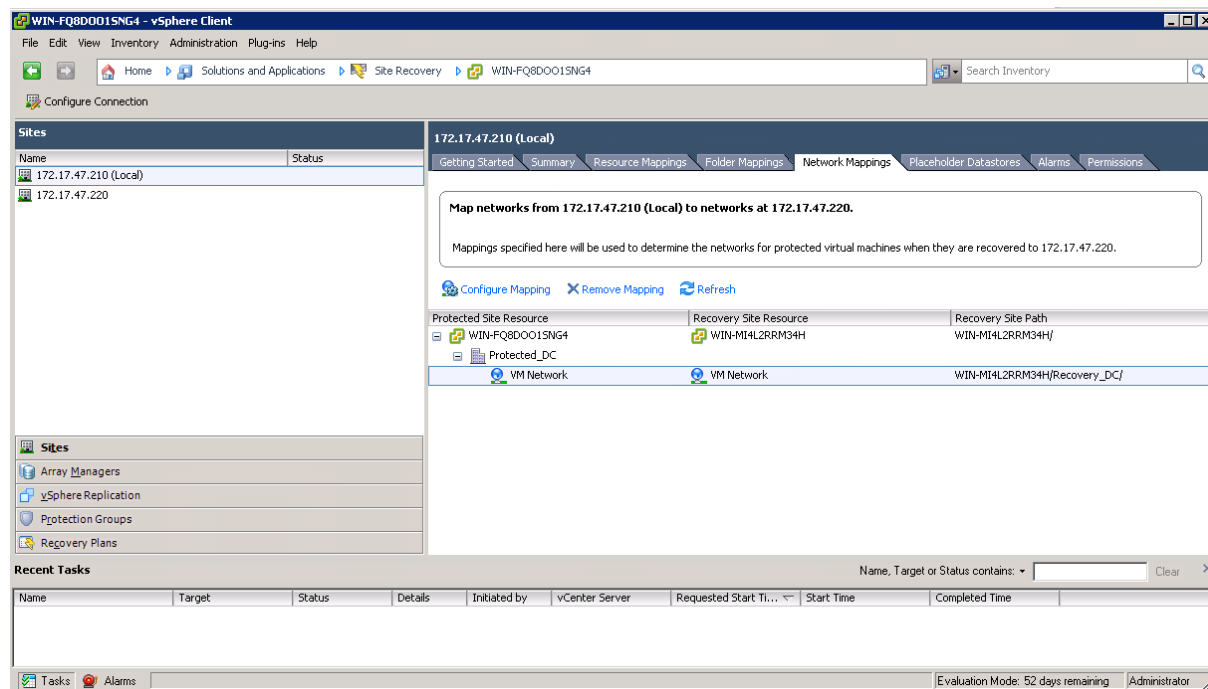
Recent Tasks

Name, Target or Status contains: Clear X

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time	Completed Time
------	--------	--------	---------	--------------	----------------	----------------------	------------	----------------

Tasks Alarms Evaluation Mode: 52 days remaining Administrator

Network Mapping



WIN-FQ8D001SNG4 - vSphere Client

File Edit View Inventory Administration Plug-ins Help

Home Solutions and Applications Site Recovery WIN-FQ8D001SNG4 Search Inventory

Configure Connection

Sites

Name	Status
172.17.47.210 (Local)	
172.17.47.220	

172.17.47.210 (Local)

Getting Started Summary Resource Mappings Folder Mappings **Network Mappings** Placeholder Datastores Alarms Permissions

Map networks from 172.17.47.210 (Local) to networks at 172.17.47.220.

Mappings specified here will be used to determine the networks for protected virtual machines when they are recovered to 172.17.47.220.

Configure Mapping Remove Mapping Refresh

Protected Site Resource	Recovery Site Resource	Recovery Site Path
WIN-FQ8D001SNG4	WIN-MI4L2RRM34H	WIN-MI4L2RRM34H/
Protected_DC		
VM Network	VM Network	WIN-MI4L2RRM34H/Recovery_DC/

Sites

- Array Managers
- ySphere Replication
- Protection Groups
- Recovery Plans

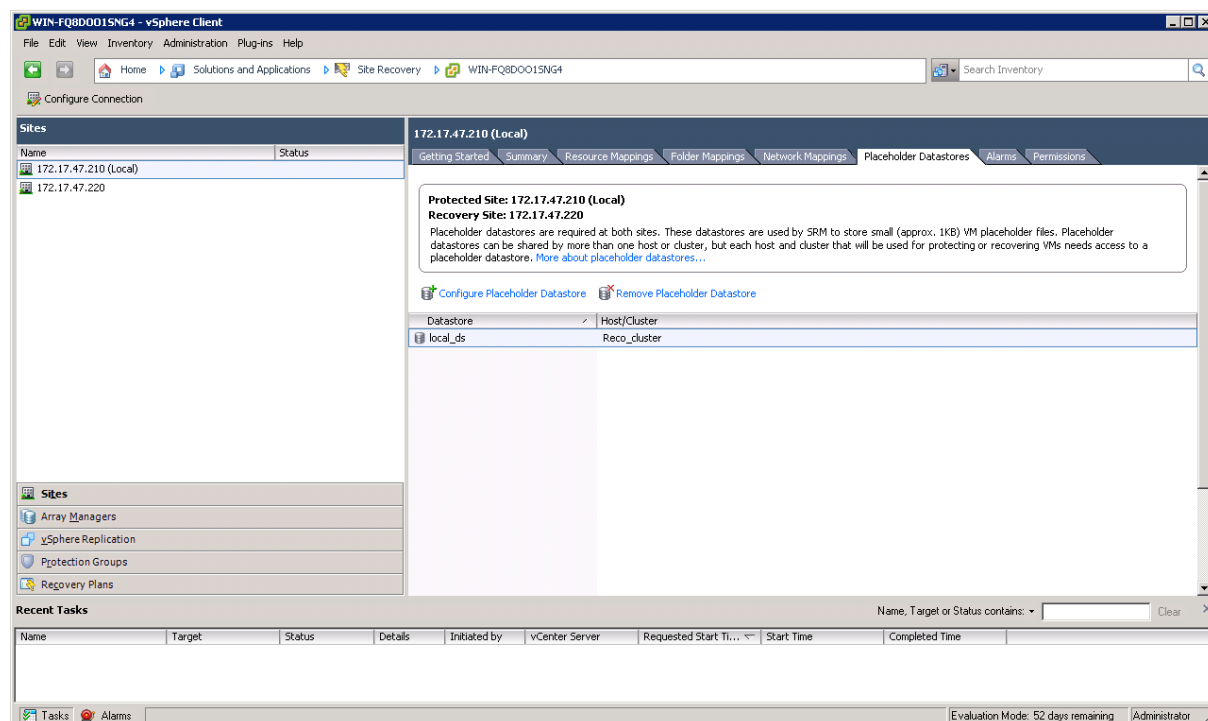
Recent Tasks

Name, Target or Status contains: Clear X

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time	Completed Time
------	--------	--------	---------	--------------	----------------	----------------------	------------	----------------

Tasks Alarms Evaluation Mode: 52 days remaining Administrator

Placeholder Datastore



WIN-FQ8D001SNG4 - vSphere Client

File Edit View Inventory Administration Plug-ins Help

Home Solutions and Applications Site Recovery WIN-FQ8D001SNG4 Search Inventory

Configure Connection

Sites

Name	Status
172.17.47.210 (Local)	
172.17.47.220	

172.17.47.210 (Local)

Getting Started Summary Resource Mappings Folder Mappings Network Mappings **Placeholder Datastores** Alarms Permissions

Protected Site: 172.17.47.210 (Local)
Recovery Site: 172.17.47.220

Placeholder datastores are required at both sites. These datastores are used by SRM to store small (approx. 1KB) VM placeholder files. Placeholder datastores can be shared by more than one host or cluster, but each host and cluster that will be used for protecting or recovering VMs needs access to a placeholder datastore. [More about placeholder datastores...](#)

Configure Placeholder Datastore Remove Placeholder Datastore

Datastore	Host/Cluster
local_ds	Reco_cluster

Sites

- Array Managers
- ySphere Replication
- Protection Groups
- Recovery Plans

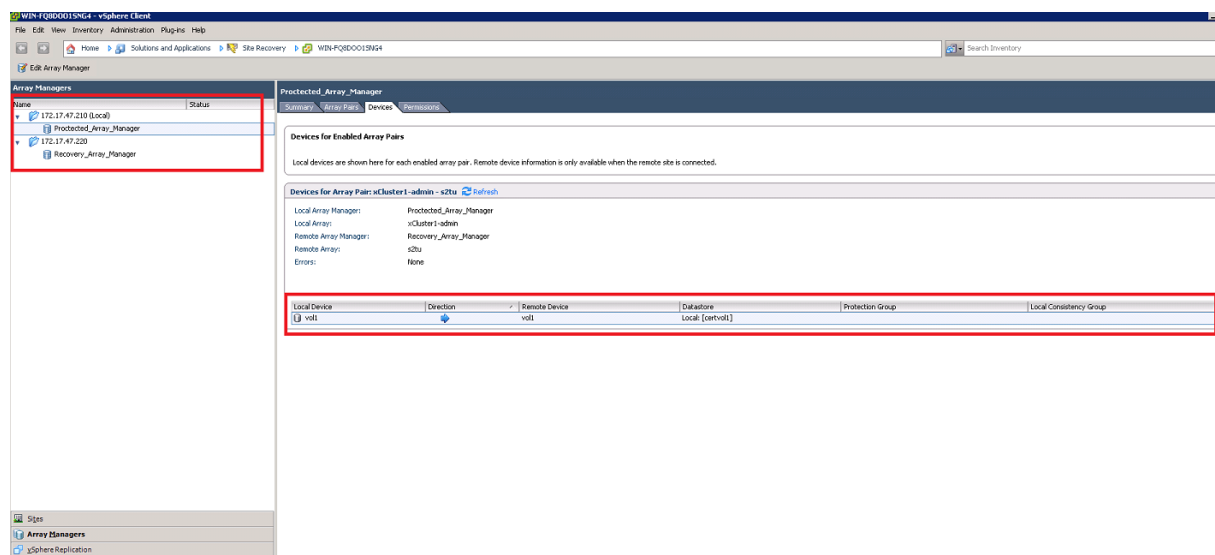
Recent Tasks

Name, Target or Status contains: Clear X

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time	Completed Time
------	--------	--------	---------	--------------	----------------	----------------------	------------	----------------

Tasks Alarms Evaluation Mode: 52 days remaining Administrator

Configure Array Manager



Array Managers

Name	Status
172.17.47.210 (Local)	
Protected_Array_Manager	
172.17.47.220	
Recovery_Array_Manager	

Protected_Array_Manager

Devices for Enabled Array Pairs

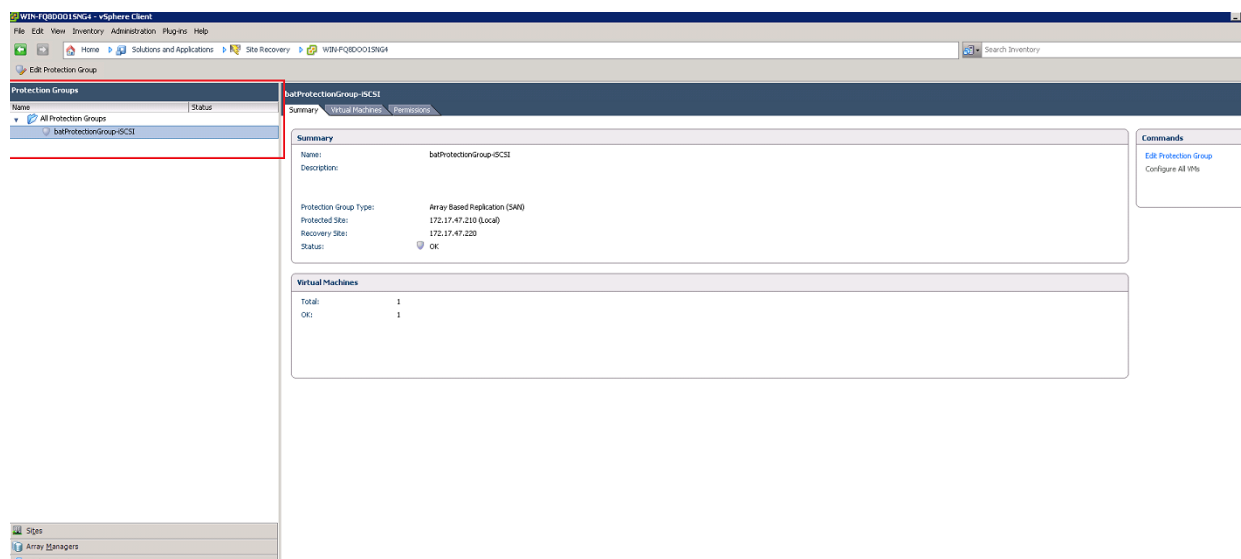
Local devices are shown here for each enabled array pair. Remote device information is only available when the remote site is connected.

Devices for Array Pair: xCluster1-admin - s2tu

Local Array Manager: Protected_Array_Manager
 Local Array: xCluster1-admin
 Remote Array Manager: Recovery_Array_Manager
 Remote Array: s2tu
 Errors: None

Local Device	Direction	Remote Device	Datastore	Protection Group	Local Consistency Group
vvol1	↓	vvol1	Local [centvol1]		

Protection Group



Protection Groups

Name	Status
All Protection Groups	
batProtectionGroup-SCSI	

batProtectionGroup-SCSI

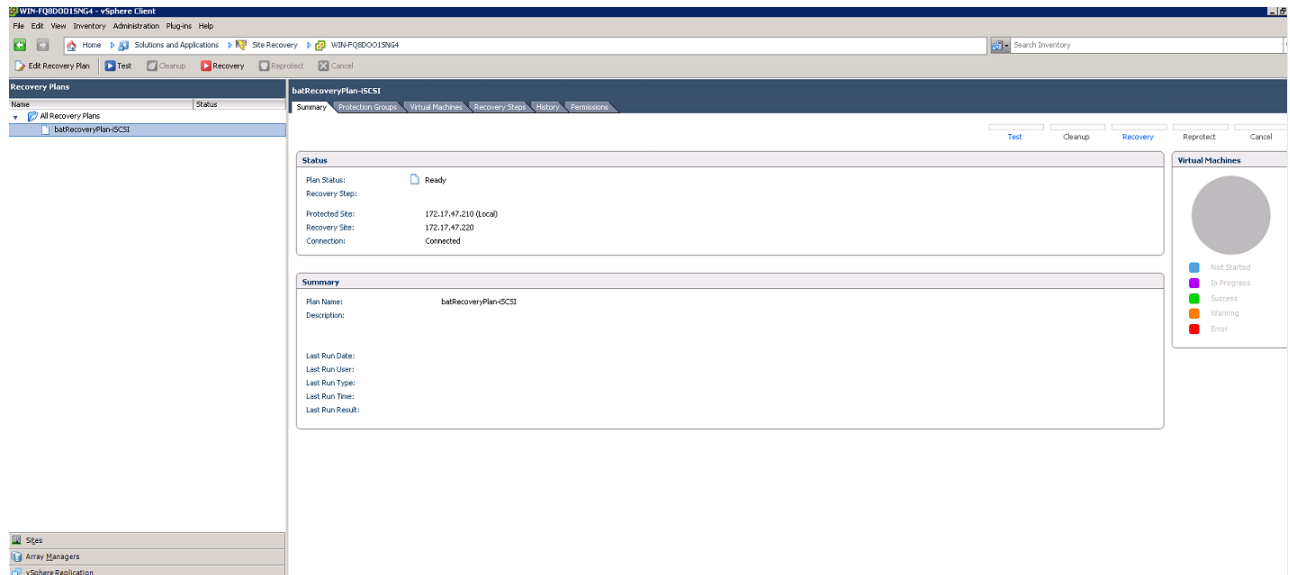
Summary

Name: batProtectionGroup-SCSI
 Description:
 Protection Group Type: Array Based Replication (SAN)
 Protected Site: 172.17.47.210 (Local)
 Recovery Site: 172.17.47.220
 Status: OK

Virtual Machines

Virtual Machine	Count
Total	1
OK	1

Recovery Plan



Recovery Plans

Name: batRecoveryPlan-SCSI Status: Ready

Plan Status: Ready

Recovery Step:

Protected Site: 172.17.47.210 (local)

Recovery Site: 172.17.47.220

Connections: Connected

Summary

Plan Name: batRecoveryPlan-SCSI

Description:

Last Run Date:

Last Run User:

Last Run Type:

Last Run Time:

Last Run Result:

Virtual Machines

Not Started

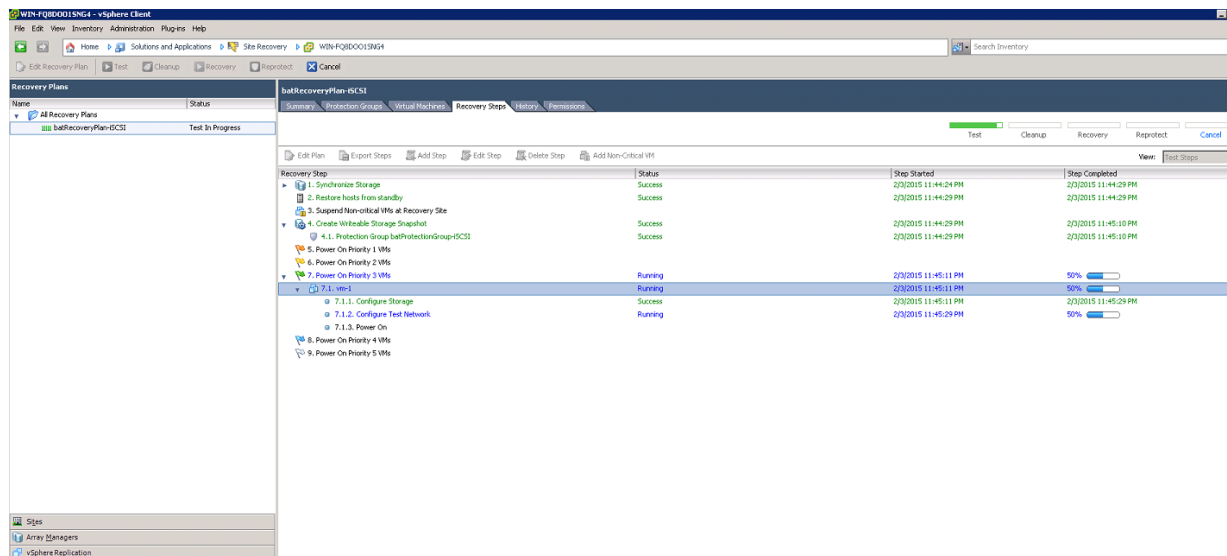
In Progress

Success

Warning

Error

Test Workflow



Recovery Plans

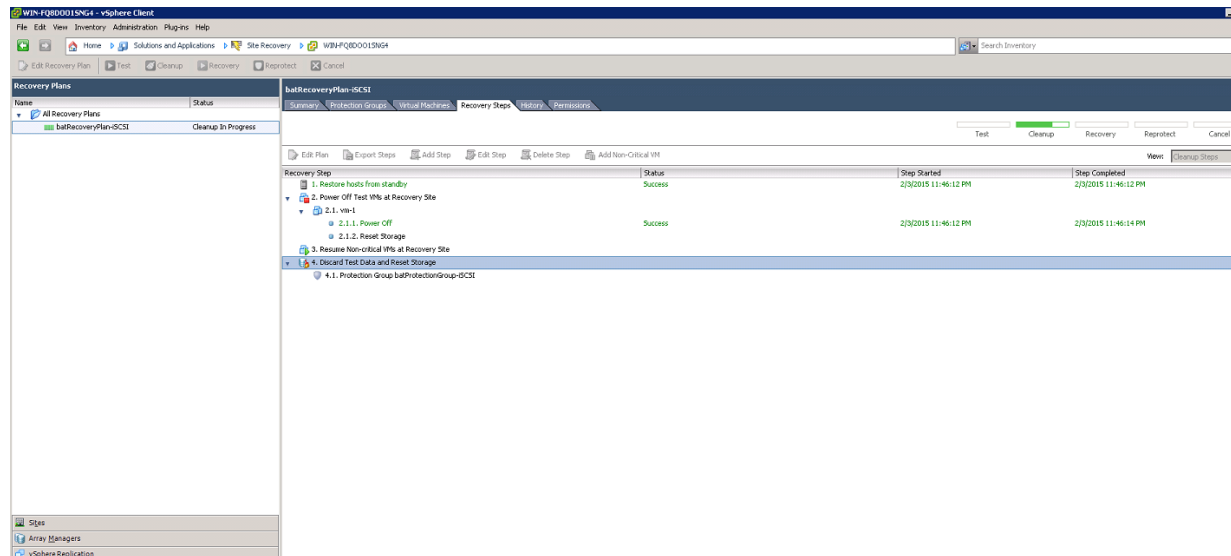
Name: batRecoveryPlan-SCSI Status: Test In Progress

Plan Status: Test In Progress

Recovery Step

Recovery Step	Status	Step Started	Step Completed
1. Synchronize Storage	Success	2/3/2015 11:44:24 PM	2/3/2015 11:44:29 PM
2. Restore hosts from standby	Success	2/3/2015 11:44:29 PM	2/3/2015 11:44:29 PM
3. Suspend Non-critical VMs at Recovery Site	Success	2/3/2015 11:44:29 PM	2/3/2015 11:45:10 PM
4. Create Writeable Storage Snapshot	Success	2/3/2015 11:44:29 PM	2/3/2015 11:45:10 PM
4.1. Protection Group batProtectionGroup-SCSI	Success	2/3/2015 11:44:29 PM	2/3/2015 11:45:10 PM
5. Power On Priority 1 VMs	Success	2/3/2015 11:44:29 PM	2/3/2015 11:45:10 PM
6. Power On Priority 2 VMs	Success	2/3/2015 11:44:29 PM	2/3/2015 11:45:10 PM
7. Power On Priority 3 VMs	Running	2/3/2015 11:45:11 PM	50%
7.1.1. vm-1	Running	2/3/2015 11:45:11 PM	50%
7.1.1.1. Configure Storage	Success	2/3/2015 11:45:11 PM	2/3/2015 11:45:29 PM
7.1.1.2. Configure Test Network	Running	2/3/2015 11:45:11 PM	50%
7.1.2. Power On	Success	2/3/2015 11:45:29 PM	50%
8. Power On Priority 4 VMs	Success	2/3/2015 11:45:29 PM	50%
9. Power On Priority 5 VMs	Success	2/3/2015 11:45:29 PM	50%

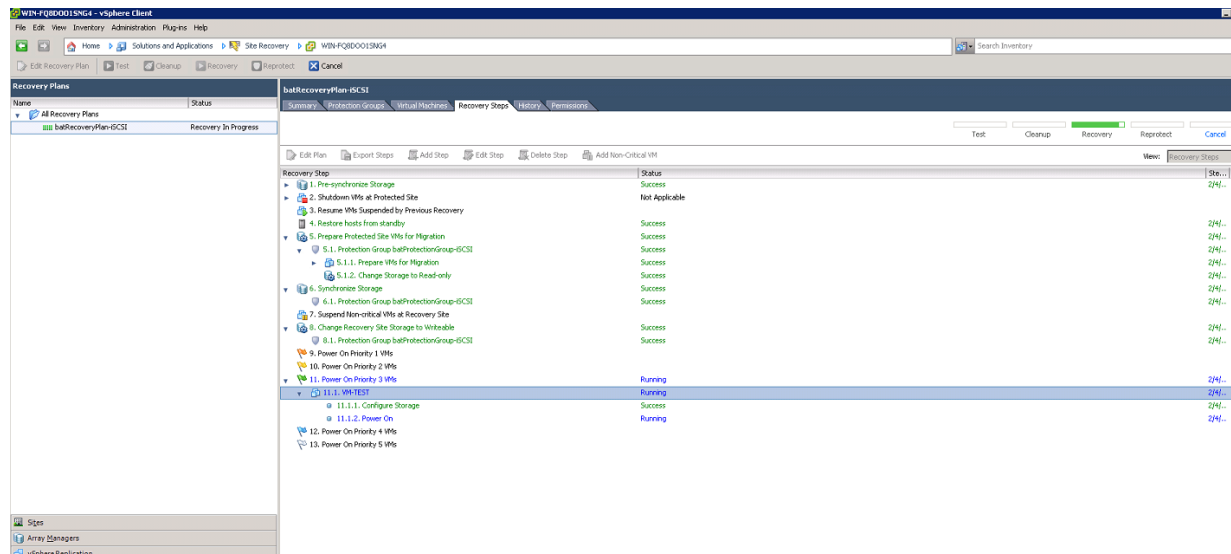
Clean-up Workflow



The screenshot shows the vSphere Client interface with the 'Clean-up Workflow' for a Recovery Plan named 'batlRecoveryPlan-DCSI'. The workflow is currently in the 'Cleanup In Progress' state. The main pane displays the 'Recovery Steps' tab, which lists the following steps:

- 1. Restore hosts from standby (Status: Success, Step Started: 2/3/2015 11:46:12 PM, Step Completed: 2/3/2015 11:46:12 PM)
- 2. Power Off Test VMs at Recovery Site (Status: Success, Step Started: 2/3/2015 11:46:12 PM, Step Completed: 2/3/2015 11:46:14 PM)
 - 2.1. VM-1 (Status: Success, Step Started: 2/3/2015 11:46:12 PM, Step Completed: 2/3/2015 11:46:14 PM)
 - 2.1.1. Power Off (Status: Success, Step Started: 2/3/2015 11:46:12 PM, Step Completed: 2/3/2015 11:46:14 PM)
 - 2.1.2. Reset Storage (Status: Success, Step Started: 2/3/2015 11:46:12 PM, Step Completed: 2/3/2015 11:46:14 PM)
- 3. Resume Non-critical VMs at Recovery Site (Status: Success, Step Started: 2/3/2015 11:46:12 PM, Step Completed: 2/3/2015 11:46:14 PM)
- 4. Guard Test Data and Reset Storage (Status: Success, Step Started: 2/3/2015 11:46:12 PM, Step Completed: 2/3/2015 11:46:14 PM)
- 4.1. Protection Group batlProtectionGroup-DCSI (Status: Success, Step Started: 2/3/2015 11:46:12 PM, Step Completed: 2/3/2015 11:46:14 PM)

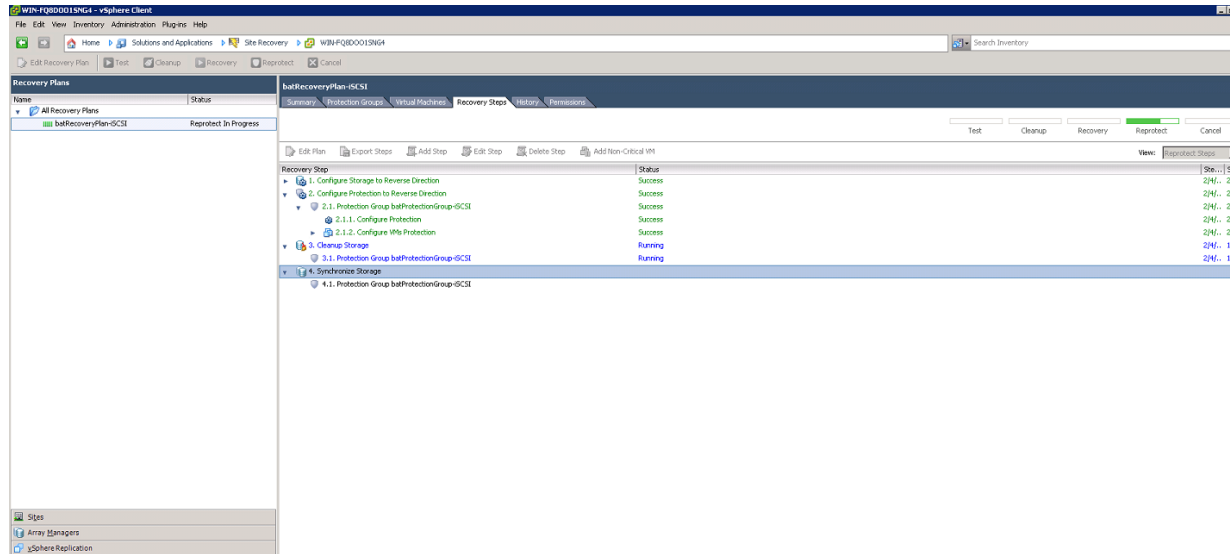
Recovery Workflow



The screenshot shows the vSphere Client interface with the 'Recovery Workflow' for a Recovery Plan named 'batlRecoveryPlan-DCSI'. The workflow is currently in the 'Recovery In Progress' state. The main pane displays the 'Recovery Steps' tab, which lists the following steps:

- 1. Pre-synchronize Storage (Status: Success, Step Started: 2/4/... 2/4/...)
- 2. Shutdown VMs at Protected Site (Status: Not Applicable, Step Started: 2/4/... 2/4/...)
- 3. Resume VMs Suspended by Previous Recovery (Status: Success, Step Started: 2/4/... 2/4/...)
- 4. Restore hosts from standby (Status: Success, Step Started: 2/4/... 2/4/...)
- 5. Prepare Protected Site VMs for Migration (Status: Success, Step Started: 2/4/... 2/4/...)
- 5.1. Protection Group batlProtectionGroup-DCSI (Status: Success, Step Started: 2/4/... 2/4/...)
- 5.1.1. Prepare VMs for Migration (Status: Success, Step Started: 2/4/... 2/4/...)
- 5.1.2. Change Storage to Read-only (Status: Success, Step Started: 2/4/... 2/4/...)
- 6. Synchronize Storage (Status: Success, Step Started: 2/4/... 2/4/...)
- 6.1. Protection Group batlProtectionGroup-DCSI (Status: Success, Step Started: 2/4/... 2/4/...)
- 7. Suspend Non-critical VMs at Recovery Site (Status: Success, Step Started: 2/4/... 2/4/...)
- 8. Change Recovery Site Storage to Writable (Status: Success, Step Started: 2/4/... 2/4/...)
- 8.1. Protection Group batlProtectionGroup-DCSI (Status: Success, Step Started: 2/4/... 2/4/...)
- 9. Power On Priority 1 VMs (Status: Running, Step Started: 2/4/... 2/4/...)
- 10. Power On Priority 2 VMs (Status: Running, Step Started: 2/4/... 2/4/...)
- 11. Power On Priority 3 VMs (Status: Running, Step Started: 2/4/... 2/4/...)
- 11.1. VM-TEST (Status: Running, Step Started: 2/4/... 2/4/...)
- 11.1.1. Configure Storage (Status: Success, Step Started: 2/4/... 2/4/...)
- 11.1.2. Power On (Status: Running, Step Started: 2/4/... 2/4/...)
- 12. Power On Priority 4 VMs (Status: Running, Step Started: 2/4/... 2/4/...)
- 13. Power On Priority 5 VMs (Status: Running, Step Started: 2/4/... 2/4/...)

Reprotect Workflow



The screenshot displays the vSphere Client interface for a VM named WIN-FQDD001SNG4. The 'Recovery Plans' tab is active, showing a list of recovery plans. The 'batRecoveryPlan-SCSI' plan is selected, and its 'Reprotect In Progress' status is visible. The 'Recovery Steps' tab is also active, showing a list of steps with their status and progress.

Recovery Step	Status	Progress
1. Configure Storage to Reverse Direction	Success	24% / 24%
2. Configure Protection to Reverse Direction	Success	24% / 24%
2.1. Protection Group batProtectionGroup-SCSI	Success	24% / 24%
2.1.1. Configure Protection	Success	24% / 24%
2.1.2. Configure iOPS Protection	Success	24% / 24%
3. Cleanup Storage	Running	24% / 10%
3.1. Protection Group batProtectionGroup-SCSI	Running	24% / 10%
4. Synchronize Storage		
4.1. Protection Group batProtectionGroup-SCSI		

Appendix D — Glossary

C

Cleanup

Placeholders created during non-disruptive test workflow failover are cleaned up during the cleanup workflow.

Cluster

A contiguous group of nodes on a storage system.

M

MVIP

Management Virtual IP. A 1GbE Management Network used for API traffic.

P

Placeholders

Placeholder virtual machine/datastores that gets created on the recovery sites for all VMs that are a part of the protection group.

Protected site

Protected site is the site where the protected VMs are running.

S

SRA

Storage Replication Adapter.

SRM

VMware vCenter Site Recovery Manager.

R

Recovery plan

A recovery plan specifies the order in which virtual machines start up on the recovery site.

Recovery Site

The recovery site is the site to which SolidFire SRA can replicate the services.

Reprotect

SRA facilitates to reprotect virtual machines with datastores after failover from the recovery site. The virtual machines can be brought back to original protected sites with datastore after failover to recovery site.

V

Volume

Block device accessed over an iSCSI network.

Appendix E — Related Documents

Document Title	Description
SolidFire Element OS User Guide	Reference for understanding SolidFire concepts and configuring SolidFire nodes and clusters
Arista Configuration Guide	Reference for configuring Arista EOS on Arista Switches. Refer to the Software Documentation page at www.arista.com



1600 Pearl Street, Suite 200
Boulder, Colorado 80302

Phone: 720.523.3278
Email: Support@solidfire.com

www.solidfire.com