Hewlett Packard Enterprise

HPE 3PAR Storage Replication Adapter 6.5.1 for VMware® vCenter Site Recovery Manager™ User Guide

Abstract

HPE 3PAR Storage Replication Adapter 6.5.1 for VMware® vCenter Site Recovery Manager™ (HPE 3PAR SRA) is an integration component that communicates with HPE 3PAR StoreServ to execute specific storage and HPE 3PAR Remote Copy functions needed for VMware vCenter Site Recovery Manager operation. This document provides relevant information for installing and configuring the 3PAR SRA. This document also provides relevant information for the 3PAR Remote Copy Software configuration so that the 3PAR SRA can execute specific 3PAR Remote Copy functions to build, manage, test, and execute disaster recovery. The information contained in this document must be used along with the documentation set provided by Hewlett Packard Enterprise for the HPE 3PAR StoreServ Storage system, HPE 3PAR Operating System Software, the documentation provided by VMware for vCenter, Site Recovery Manager, and other related products.

Part Number: QL226-99583
Published: June 2017
Edition: 6

Acknowledgments

Contents

Introduction

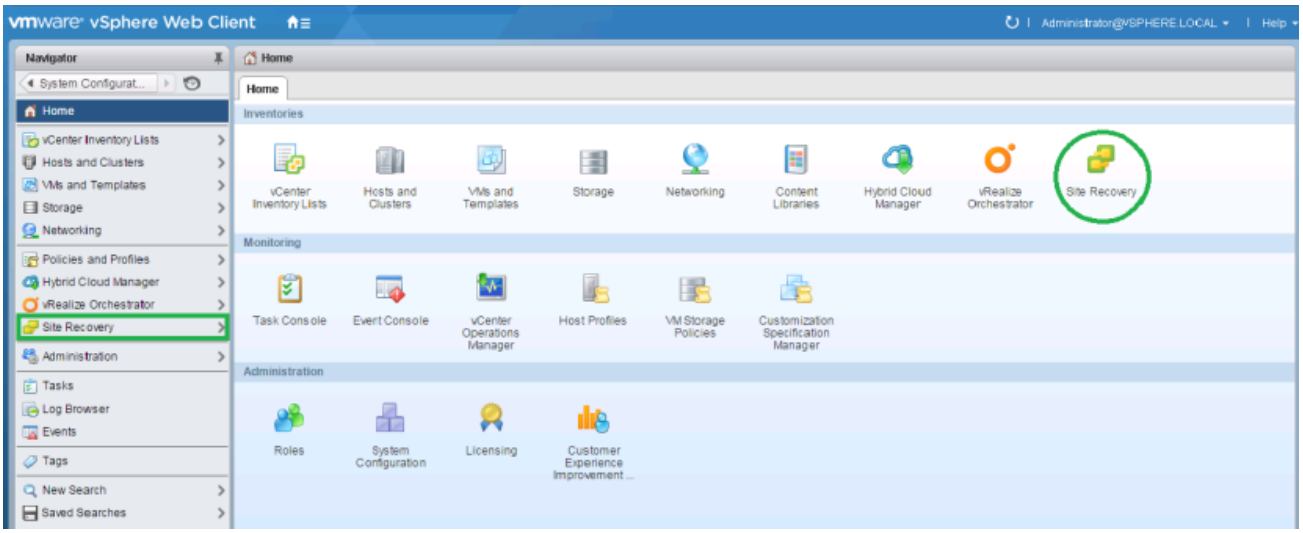
HPE 3PAR Storage Replication Adapter 6.5.1 for VMware® vCenter Site Recovery Manager™ (HPE 3PAR SRA) is an adapter to VMware vCenter Site Recovery Manager™ (SRM).

HPE 3PAR SRA enables SRM to work with HPE 3PAR StoreServ Storage systems for array-based replication. HPE 3PAR SRA is installed on SRM servers and enables communications between SRM and HPE 3PAR StoreServ Storage systems thus facilitating remote replication.

For information on VMware and the VMware Site Recovery Manager, see the VMware website **http://www.vmware.com/products/site-recovery-manager/**.

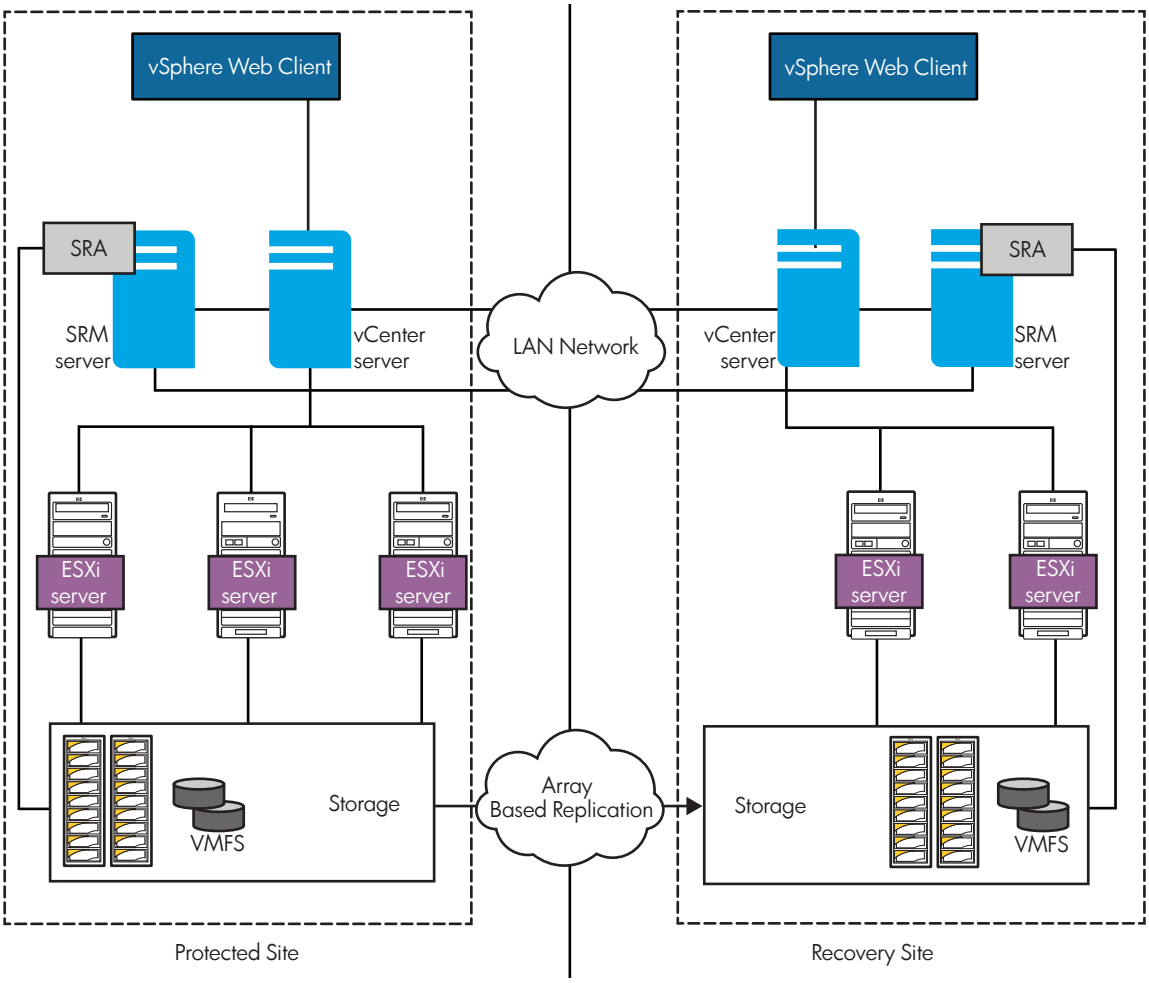
VMware vCenter Site Recovery Manager Overview

SRM works as a plug-in component for VMware vCenter and integrates its functionality in VMware vCenter.



VMware vCenter Site Recovery Manager:

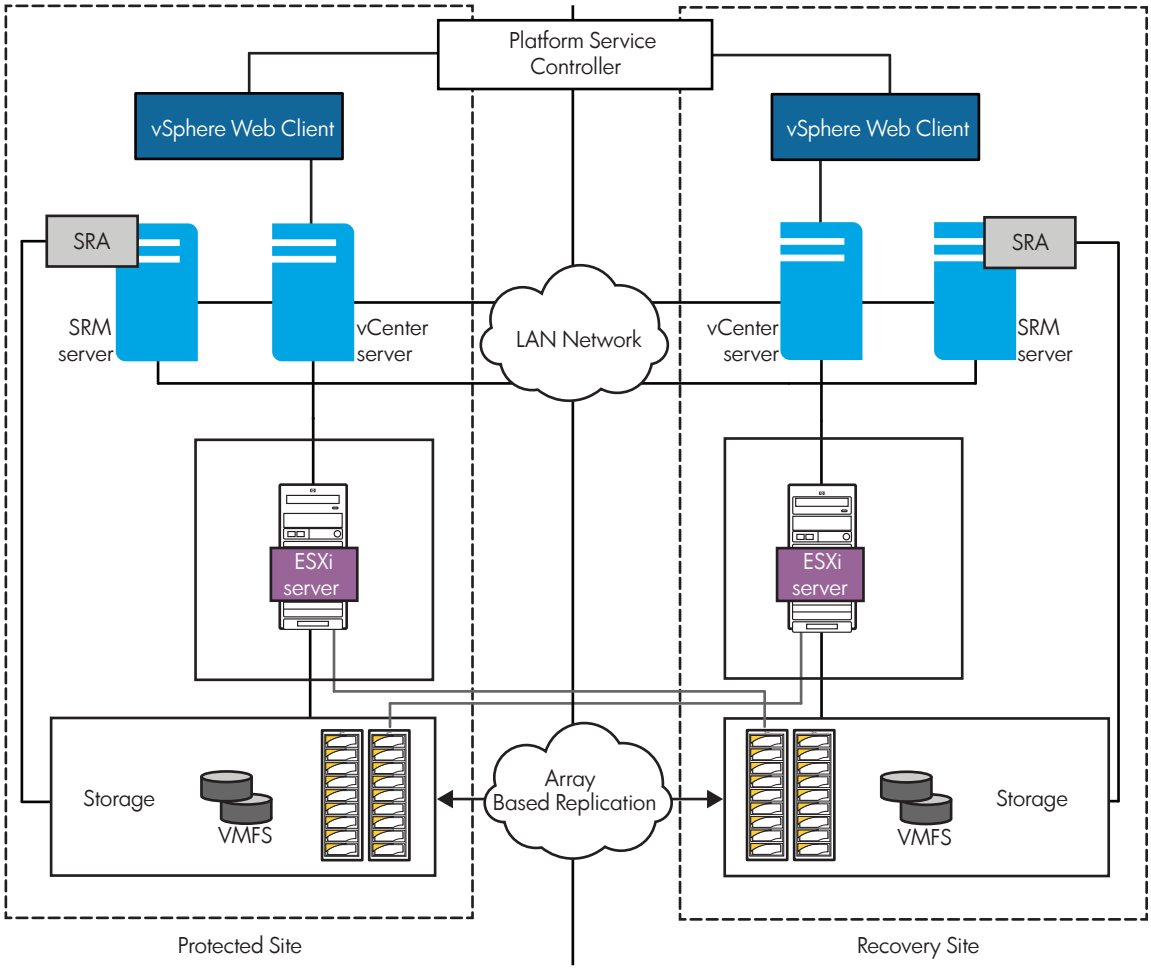
- Builds, manages, tests, and executes disaster recovery solutions for virtual infrastructure implementations.
- Uses the storage replication mechanism between the protected site and the recovery site for disaster recovery of the protected site virtual infrastructure.
- Creates a recovery point objective by creating a protection group at the protected site. The protection group contains replicated virtual machines.
- Creates a recovery plan at the recovery site for the protection group at the protection site.
    - The recovery plan can be tested at any time at the recovery site to verify that recovery point objective can be achieved at the time of disaster.
    - The recovery plan can be executed at disaster time or at any desired time at the recovery site to guarantee that recovery point objective is met.



SRM communicates with HPE 3PAR Remote Copy Software for storage replication through HPE 3PAR SRA. You can get information about Remote Copy volume groups that exist in HPE 3PAR StoreServ to SRM from HPE 3PAR SRA. The Site Recovery Manager identifies datastores and RDM devices in the Remote Copy volume group (also known as consistency groups). These datastores and RDM devices have corresponding virtual volumes in the Remote Copy volume group and replicates between the protected site and the recovery site.

Stretched Storage

HPE 3PAR SRA supports a new feature called stretched storage with the SRM 6.5.1 release. Stretched storage is implemented in environments where disaster/downtime avoidance is a key requirement. This combines synchronous replication with array-based clustering.



The integration of stretched storage with Site Recovery Manager 6.5.1 allows users to achieve:

- Planned maintenance downtime avoidance
- Zero-downtime disaster avoidance

> **NOTE:** You must install vCenter in Enhanced Linked mode, for Stretched storage to function correctly. For details, refer **https://blogs.vmware.com/consulting/2015/03/vsphere-datacenter-design-vcenter-architecture-changes-vsphere-6-0-part-1.html**.

For more information see VMWare vCenter installation procedure documentation, **https://www.vmware.com/support/pubs/**.

SRA Overview

HPE 3PAR Storage Replication Adapter (SRA) is a plug-in to VMware vCenter Site Recovery Manager that enables interaction between Site Recovery Manager (SRM) and the storage controller. HPE 3PAR SRA Software for VMware vCenter SRM integrates VMware SRM with HPE 3PAR StoreServ Remote Copy replication software. HPE 3PAR SRA software combines HPE 3PAR Remote Copy Software and HPE 3PAR Virtual Copy Software with VMware SRM to ensure the highest performing and most reliable disaster protection for all virtualized applications.

Features

- SRA Interface enables SRM to execute the workflows like, query SRA properties and capabilities and discovery of replicated storage.
- Accelerate recovery for the virtual environment through automation.
- Promote reliable recovery by enabling nondisruptive testing.
- Automated site recovery
- Leverage the high performance, reliability, and simplicity of HPE 3PAR replication capabilities.

SRM Operations

The following operations are supported for Standard storage and Stretched storage:

- **Test Failover**

  When you create or modify a recovery plan, test it before you use it for planned migration or disaster recovery.

  Testing a recovery plan, ensures that the virtual machines are recovered correctly to the recovery site. If you do not test recovery plans, a disaster recovery situation might not recover all virtual machines, which may result in data loss.

  Testing a recovery plan exercises nearly every aspect of a recovery plan, although Site Recovery Manager makes several concessions to avoid disrupting ongoing operations on the protected and recovery sites.

  Site Recovery Manager with the help of 3PAR SRA, creates temporary snapshots of replicated storage at the recovery site. For array-based replication, Site Recovery Manager rescans the arrays to discover them. If you explicitly assign test networks, Site Recovery Manager connects recovered virtual machines to a test network. If virtual machine network assignment is Auto, Site Recovery Manager assigns virtual machines to temporary networks that are not connected to any physical network.
- **Clean up**

  After you test a recovery plan, you can return the recovery plan to the Ready-state by running a cleanup operation. Site Recovery Manager performs several cleanup operations after a test.

  - Powers off the recovered virtual machines
  - Replaces recovered virtual machines with placeholders, preserving their identity and configuration information
  - Cleans up replicated storage snapshots that the recovered virtual machines used during the test
- **Recovery**

  You can use Site Recovery Manager to implement different types of recovery from the protected site to the recovery site.

  - Planned Migration

    The orderly evacuation of virtual machines from the protected site to the recovery site. Planned Migration prevents data loss when migrating workloads in an orderly fashion. For planned migration to succeed, both sites must be running and fully functioning.
  - Disaster Recovery

Similar to planned migration except that the disaster recovery does not require that both sites be up and running, for example if the protected site goes offline unexpectedly. During a disaster recovery operation, failure of operations on the protected site are reported but otherwise ignored.

- **Reprotect**

  After a recovery, the recovery site becomes the new protected site, but it is not protected yet. If the original protected site is operational, you can reverse the direction of protection to use the original protected site as a new recovery site to protect the new protected site.

  Manually reestablishing protection in the opposite direction by recreating all protection groups and recovery plans is time consuming and prone to errors. Site Recovery Manager provides the reprotect function, which is an automated way to reverse protection.

  After Site Recovery Manager performs a recovery, the protected virtual machines start up on the recovery site. Because the former protected site might be offline, these virtual machines are not protected. By running reprotect when the protected site comes back online, you reverse the direction of replication to protect the recovered virtual machines on the recovery site back to the original protected site.

  For the reprotect operation to succeed, the remote copy links between the 3PAR arrays configured between the protected and recovery arrays should be up and running.

Supported features

HPE 3PAR SRA integrates with SRM to support the following HPE 3PAR configurations for SRM Standard storage (Non-Stretched storage) and Stretched storage features:

- **Two data center configuration**: The arrays in the protected and recovery sites, configured in VMware SRM and 3PAR SRA are connected with each other using either 3PAR synchronous or asynchronous periodic or asynchronous streaming replication modes for Standard storage (Non-Stretched storage) configurations or with synchronous replication mode for SRM Stretched storage feature.
- **Synchronous Long Distance (SLD)**: SLD combines synchronous and periodic asynchronous replication to replicate a Remote Copy group to two separate target arrays. VMware SRM/3PAR SRA is configured with protected and recovery sites between the arrays which have periodic replication modes.
- **3 data center (3DCC-PP)**: In 3DC-PP, the primary (site A) and secondary (site B) arrays has the Peer Persistence relationship characterized by synchronous replication and a quorum witness enabled by the auto_failover and path_management polices. The remote copy group policy associated is "mt_pp". A VMware metro cluster has access to the Peer Persistence volumes on sites A and B. The remote copy group is extended to site C with periodic replication mode from both site A and site B. The ESX hosts and the 3PAR array in site C, the ESX hosts and one of the 3PAR arrays in sites A or B are part of the VMware SRM configuration with site A and site B hosts in SRM protected site and the site C hosts in the SRM recovery site.

Supported configurations

For information about the supported hardware and software platforms, see the Single Point of Connectivity Knowledge for HPE Storage Products (SPOCK) website **http://www.hpe.com/storage/spock**.

Prerequisites for installing and configuring HPE 3PAR SRA

HPE 3PAR SRA is packaged in MSI format and installed on the host where SRM is installed.

- HPE 3PAR SRA requires the following companion packages to be installed on the host before you start the installation:
  - VMware vCenter Site Recovery Manager 5.0 or later
  - Microsoft .NET Framework 4.6.1
- HPE 3PAR SRA requires the following configurations on the HPE 3PAR StoreServ Storage system:
  - HPE 3PAR Remote Copy Software license on the HPE 3PAR storage system
  - HPE 3PAR Virtual Copy Software license on the HPE 3PAR storage system
  - For using Stretched storage in HPE 3PAR SRA, you must have Peer persistence license.
  - HPE 3PAR StoreServ Storage system user with edit permission

    NOTE: The HPE 3PAR SRA supports partial licensing facility to purchase licenses based on the capacity used on your storage system. The Remote Copy and Virtual Copy features are available with partial licenses. SRA 6.5.1 supports partial licensing only with`HPE 3PAR OS 3.1.2 MU2` or later.

  - All LUNs used by VMware Virtual Machines to form a protection group that are failed over together during test and recovery must be part of a single HPE 3PAR Remote Copy group. For more information about setting up and configuring Remote Copy groups, see the *HPE 3PAR Remote Copy Software User's Guide*.
  - All members of a virtual volume set must belong to the same Remote Copy group.
  - In the SLD configuration scenario, A is the Primary System, C the Asynchronous Periodic Backup System, and B the Synchronous Backup System. SRM and SRA is configured between 3PAR StoreServ Storage systems A and C, where site A is the protected site and site C is the recovery site.

    SLD configuration supports SRM recovery operation to site C only when both the arrays A and B are up and running (to perform any planned migration to site C) or when both the arrays A and B are down (to perform disaster recovery to site C). If either of the arrays A or B is down, SRM recovery operation to site C is not supported.

    Prior to planned migration operation to site C, ensure that the remote copy group is primary and VMs are up at site A.

    Prior to SRA reprotect operation from the recovery site to the protected site, the VVs at site A (configured in SRM protected site) must have the replication roles as primary. Use 3PAR `CLI` commands and 3PAR SSMC, for setting the roles as primary.
  - In the 3DC-PP configuration, A is the Primary System, C the Asynchronous Periodic Backup System, and B the Synchronous Backup System. Multi-Target Peer Persistence (MT_PP) configuration is set up for these SLD groups. The sites A and B can be configured in the VMware Metro Storage Cluster (vMSC) configuration where the remote copy groups are in Peer Persistence configuration between A and B. The ESX hosts in the sites A and B are in the VMware vSphere HA cluster and have uniform host access to the replicated Peer Persistence Remote Copy group volumes. SRM/SRA is configured between 3PAR StoreServ Storage systems A and C, where site A is the protected site and site C is the recovery site. SRM/SRA can also be configured between 3PAR StoreServ Storage systems B and C instead of systems A and C, where site B is the protected site and site C is the recovery site.

    SRM recovery operation including planned migration and disaster recovery to site C is supported in the 3DCPP configuration only when both the arrays A and B are up and running (to perform any planned migration to site C) or when both the arrays A and B are down (to perform disaster recovery to site C). When either of the arrays A or B is down, SRM recovery operation to site C is not supported.

Installing and configuring HPE 3PAR SRA

This chapter explains how to install and configure HPE 3PAR SRA.

> **NOTE:** The steps to install and configure HPE 3PAR SRA remains same for Stretched and Nonstretched storage.

Upgrade from an earlier version of the software to HPE 3PAR SRA 6.5.1 not supported.

This section describes how to:

- Remove an existing version of HPE 3PAR SRA
- Install the latest version of HPE 3PAR SRA
- Verify that the installation is successful

You cannot upgrade to HPE 3PAR SRA 6.5.1 from an earlier version. Therefore, you must remove the earlier version before installing HPE 3PAR SRA 6.5.1.

Removing HPE 3PAR SRA

To remove HPE 3PAR SRA, do the following:

Procedure

1. Log on as system administrator.
2. Click **Start** > **Control Panel** > **Programs and Features**.
3. Select **HPE 3PAR SRA Software Version <x.x>**.

   > **NOTE:** The installer name remains **HP 3PAR SRA Software Version <x.x>** for the earlier versions of SRA.

4. Click **Remove**.

   The **Program Maintenance** dialog box appears.
5. Select **Remove** and click **Next**.

   > **NOTE:** HPE 3PAR SRA configuration is not deleted in the Windows registry when the HPE 3PAR SRA package is uninstalled.

Installing HPE 3PAR SRA 6.5.1

To install HPE 3PAR SRA 6.5.1:

Procedure

1. To launch the installation wizard, double-click the installation executable file. Click **Next** to continue.

   > **NOTE:** HPE 3PAR SRA and SRM must be installed on the same host.

2. To acknowledge the User License Agreement, click **I Agree** , and click **Next** to continue.
3. To start installation at the default path, click **Next** .
4. After the installation is complete, restart the `VMware vCenter Site Recovery Manager` service to ensure that HPE 3PAR SRA is recognized by SRM.

NOTE: This package can only be installed under the existing VMware vCenter Site Recovery Manager installed path. No other installation location is provided as an option.

Verifying installation

To verify the installation of HPE 3PAR SRA 6.5.1:

Procedure

1. Click **Start** > **Control Panel** > **Programs and Features**.
2. Verify that **HPE 3PAR SRA Software Version 6.5.1** or any older versions appears under **Currently installed programs**.

NOTE: HPE 3PAR SRA installation adds the `SRA\3PARInServ` folder to VMware vCenter Site Recovery Manager storage folder (for example, `C:\Program Files (x64)\VMware\VMware vCenter Site Recovery Manager\storage`) and `TPDSrm.exe` is the adapter driver program that is invoked by SRM.

Configuring HPE 3PAR SRA

This section describes how to configure HPE 3PAR SRA.

- **Configuring HPE 3PAR StoreServ Storage system at protected and recovery sites** on page 15
- **Configuring HPE 3PAR StoreServ Storage system for Non-stretched storage** on page 16
- **Configuring HPE 3PAR StoreServ Storage system for Stretched storage** on page 16
- **Configuring VMware vCenter Server for hosts and clusters** on page 17

HPE 3PAR storage system setup

Any HPE 3PAR StoreServ storage system acting as an array manager (at the protected site or at the recovery site) in SRM setup must be configured with HPE 3PAR Remote Copy Software.

HPE 3PAR SRA supports synchronous and periodic replication modes in 1:1, 1:N, N:1, and M:N configurations as supported by HPE 3PAR Remote Copy Software, where M and N indicate the number of storage systems at primary and recovery sites respectively. HPE 3PAR SRA also supports synchronous long-distance configurations. For more information about Remote Copy configurations, see the *HPE 3PAR Remote Copy Software User's Guide*.

NOTE:

- HPE 3PAR SRA 6.5.1 supports SLD Remote Copy environment on:
  - `HPE 3PAR OS 3.1.2 MU3 P16` or later MUs
  - `HPE 3PAR OS 3.1.3, 3.2.1 P01` or later MUs
- HPE 3PAR SRAsupports both Periodic (RCIP) and Sync (RCFC) configurations.

NOTE:

When using Peer Motion to perform data migration, the Remote Copy configurations and SRM setup must be re-established with the new array after migration. For more information about re-establishing Remote Copy configurations, see the *HPE 3PAR Peer Motion Manager User Guide* or *HPE 3PAR Remote Copy Software User's Guide*.

Configuring HPE 3PAR StoreServ Storage system at protected and recovery sites

This section describes the HPE 3PAR StoreServ Storage configurations that you need to perform at the protected and recovery sites.

IMPORTANT:
Make sure that you do these configurations both at the protected and recovery sites.

Procedure

1. Make sure that the correct version of HPE 3PAR Operating System with the appropriate licensed features is available.
2. Create a user on the HPE 3PAR StoreServ Storage system.
3. Register ESXi hosts on the HPE 3PAR StoreServ Storage system.

   Before a LUN from the HPE 3PAR StoreServ storage system can be exported to the ESXi host, register the ESXi host WWNs/iSCSI names on the HPE 3PAR storage system by creating a host entry. Perform this operation on both the protected and recovery sites.

   NOTE: When you export LUNs to an ESXi host using `Persona 11` at the recovery site, the system stops responding while executing the **Rescan All** function. Therefore, you must remove all LUN exposures of the Remote Copy group member on the recovery site, except the Peer Persistence configuration to the host with `Persona 11`, to prevent any delayed response during ESXi rescan.
4. Create Common Provisioning Groups (CPGs) to use during the creation of virtual volume.
5. Create virtual volumes.

   Create the required number of virtual volumes to meet the replication requirement of the virtual infrastructure. For more information about creating virtual volumes, see the *HPE 3PAR OS CLI Administrator's Manual*.
6. Set up the HPE 3PAR Remote Copy Software.

   HPE 3PAR Remote Copy Software provides the capability to copy virtual volumes from a protected site to a recovery site.

   Set up a Remote Copy link between the protected and recovery site. Create a Remote Copy volume group at the protected site. A corresponding Remote Copy group is automatically created at the recovery site. Ensure that the HPE 3PAR storage system hardware is set up appropriately for creating a Remote Copy configuration between the protected site and recovery site. For more information about setting up HPE 3PAR Remote Copy Software, 3PAR SLD, and 3DC-PP configurations, see the *HPE 3PAR Remote Copy Software User Guide*.

   NOTE:

   - You can create a Remote Copy configuration between the protected and recovery sites using one of the following protocols:
     - RCIP
     - RCFC

     For information about implementing Remote Copy, see the *HPE 3PAR Remote Copy Software User's Guide*.
   - Remote Copy is supported on HPE 3PAR OS 2.3.1 or later.

Configuring HPE 3PAR StoreServ Storage system for Non-stretched storage

This section describes the HPE 3PAR StoreServ Storage configurations that you must perform only at the protected site.

Procedure

1. Create Remote Copy Group on the primary storage system.
2. Admit the virtual volume to the Remote Copy volume group.

   A virtual volume contains virtual infrastructure data (datastore, virtual disk, and RDM disk). Replication of virtual infrastructure data is enabled by admitting virtual volumes to the Remote Copy volume group. Each virtual volume at the protected site is mapped to a corresponding virtual volume at the recovery site. Data in each virtual volume at the protected site is synced with the data in the corresponding virtual volume at the recovery site whenever Remote Copy is active. For more information about adding virtual volumes to Remote Copy volume groups, see the *HPE 3PAR Remote Copy Software User Guide*.
3. Export the virtual volume to the ESXi host (create a VLUN).

   It is assumed that ESXi host(s) are already connected to the HPE 3PAR StoreServ storage system and configured per the recommendations in the *VMware ESX Servers Implementation Guide*. Create a VLUN for one or more ESXi hosts corresponding to the virtual volume. For more information, see the *HPE 3PAR OS VMware ESX Server Implementation Guide*.
4. In the SLD configuration scenario, A is the Primary System, C the Asynchronous Periodic Backup System, and B the Synchronous Backup System. SRM and SRA is configured between 3PAR StoreServ Storage systems A and C, where site A is the protected site and site C is the recovery site.
5. In the 3DC-PP configuration, A is the Primary System, C the Asynchronous Periodic Backup System, and B the Synchronous Backup System. Multi-Target Peer Persistence (MT_PP) configuration is set up for these SLD groups. The sites A and B can be configured in the VMware Metro Storage Cluster (vMSC) configuration where the remote copy groups are in Peer Persistence configuration between A and B. The ESX hosts, in the sites A and B are in the VMware vSphere HA cluster and have uniform host access to the replicated Peer Persistence Remote Copy group volumes. SRM/SRA is configured between 3PAR StoreServ Storage systems A and C, where site A is the protected site and site C is the recovery site. SRM/SRA can also be configured between 3PAR StoreServ Storage systems B and C instead of systems A and C, where site B is the protected site and site C is the recovery site.

Configuring HPE 3PAR StoreServ Storage system for Stretched storage

This section describes the HPE 3PAR StoreServ Storage configurations that you must perform on both the protected and recovery sites.

- Create Remote Copy Group from primary to recovery storage system.

  NOTE: Create Remote copy in Sync mode for stretched storage support.
- Admit the virtual volumes to the Remote Copy volume group.
- All associated hosts are connected to both the primary and secondary arrays.
- Set the same WWN for the replicated volumes which are admitted to the Remote Copy group in primary to recovery storage system.
- Set path management policy for Remote Copy volume group using the following command:

  ```
  setrcopygroup pol path_management
  ```
- Export the virtual volumes to the ESXi hosts on both sites (create a VLUN).

NOTE:

In stretched storage configuration, when VVs are exported to individual host, and later if that host becomes part of a hostset, then during disaster recovery workflow, on recovery site multiple exports are observed using host(s) and hostset(s).

Configuring VMware vCenter Server for hosts and clusters

This section describes how to configure the VMware vCenter Server for hosts and clusters.

Procedure

1. Discover LUNs on the ESXi hosts.
2. Rescan the HBA to verify if the VLUN is visible to the ESXi host. Perform rescan only after you export the VLUNs to the ESXi host.
3. Create a VMFS Datastore.
4. Deploy VMs as required on the protected site.

NOTE:

The steps to configure VMware vCenter Server for hosts and clusters remain same for stretched storage. Make sure that the datastore is visible on the recovery site also.

NOTE:

For SLD and 3DC-PP configuration, after the arrays are added in the SRM Array Manager successfully, if you select the primary array, two target arrays are listed. Configure SRM/SRA between HPE 3PAR StoreServ Storage systems A and C or B and C.

Only for SLD configuration, make sure that the remote copy group role, is primary at the array configured in the protected site before performing the planned migration to site C. In case, if both the arrays A and B are down (arrays in the synchronous replication mode), then perform the disaster recovery to site C. But before performing the reprotect operation from recovery site to the protected site, make sure that the remote copy group role is primary at the array configured in the protected site.

HPE 3PAR SRA Command Line Interface

HPE 3PAR SRA supports the `TPDSrm.exe` command-line interface. SRM requests are sent using a Perl script `command.pl` in the HPE 3PAR SRA installed directory. The Perl script internally processes the data to an XML file and spawns an instance of `TPDSrm.exe` to process the XML file. The XML file is removed once `TPDSrm.exe` returns to `command.pl`.

The HPE 3PAR SRA for VMware SRM 6.0 utility supports the following commands:

Commands

- `-v`

  To display version information.

  Syntax: `TPDSrm.exe <-v>`
- `cleansnaps`

  To remove any snapshots created for test failover on the HPE 3PAR Storage system.

  Syntax: `TPDSrm.exe cleansnaps <-sys StorageSystemName -user UserName -pass Password [-loglevel Num]>`

  - `-sys <StorageSystem>`

The HPE 3PAR storage system name or IP address to connect.

- `-user <UserName>`

  The HPE 3PAR storage system user name.

- `-pass <Password>`

  The HPE 3PAR storage system password.

- `-loglevel <Num>`

  Optional. Overrides the default output message level using a numeral from 1 to 5. The default value is 3 (1-error, 2-warning, 3-info, 4-verbose, 5-trivia).

- `viewstate`

  To view the local disaster recovery state cache information. Only `prepareFailover` and `failover` states are available.

  Syntax: `TPDSrm.exe viewstate`

- `cleanstate`

  To remove the local disaster recovery state cache created during the failover operation.

  Syntax: `TPDSrm.exe cleanstate <-sysid StorageSystemID> <-rcgroup RCGroupName>`

  - `-sysid <StorageSystemID>`

    The system ID of the HPE 3PAR storage system where the Remote Copy group name is found. Use the `viewstate` command to see currently cached information.

  - `-rcgroup <RCGroupName>`

    The Remote Copy group name.

- `viewcert`

  To view the currently accepted StoreServ certificate.

  Syntax: `TPDSrm.exe viewcert <-sysid StorageSystemID>`

  - sysid <StorageSystemID>

    Optional. System ID of the HPE 3PAR StoreServ. Displays all certificates if this option is not specified.

- `validatecert`

  To accept and save HPE 3PAR StoreServ certificate.

  This operation must be done prior to SRM configuration with HPE 3PAR Storage system.

  Syntax: `TPDSrm.exe validatecert <-sys StorageSystemIP -user UserName -pass Password>`

  - `-sys <StorageSystem>`

    HPE 3PAR StoreServ name or IP address to connect.

  - `-user <UserName>`

    HPE 3PAR StoreServ user name.

  - `-pass <Password>`

    HPE 3PAR StoreServ password.

- `removecert`

  To delete the accepted HPE 3PAR StoreServ certificate from cache.

  Syntax: `TPDSrm.exe removecert <-sysid StorageSystemID>`

  - `-sysid <StorageSystemID>`

    System ID of the HPE 3PAR StoreServ.

- `use_individual_vvs_to_export`

  Define virtual volume(s) export behavior for SRA operations

  if 'yes' then SRA uses individual virtual volume(s) for exporting to host(s) and/or hostset(s).

  if 'no' then SRA uses manually created vvset(s) to export to host(s) and/or hostset(s).

  Manually created vvset(s) are used to export only if the same Vvs exist in both the RC group in question. The vvset, and the number of Vvs in the RC group and Vvset are same. Otherwise, individual Vvs are used to export to the hosts. SRA will not use automatically created vvset for the RC group `[matched with 'RCP_<RC group name>']` to export to host(s) and/or hostset(s).

  If `use_individual_vvs_to_export` option is not configured by the user then value 'no' is set by default to this parameter.

  Once this option is configured, it is applicable for all the arrays at a particular SRM site (either protected or recovery site). Based on user preferred vv export behavior, this option needs to be set at protected and recovery sites.

  If user wants to configure this option at an array level then use below optional arguments.

  Optional arguments :

  - `-sys <StorageSystem>`

    HPE 3PAR StoreServ name or IP address to connect.
  - `-user <UserName>`

    HPE 3PAR StoreServ user name.
  - `-pass <Password>`

    HPE 3PAR StoreServ password.

  Eg: `TpdSrm use_individual_vvs_to_export no`

  `TpdSrm use_individual_vvs_to_export yes`

  `TpdSrm use_individual_vvs_to_export yes -sys <IP> -user sra -pass sra`

  `TpdSrm use_individual_vvs_to_export no -sys <IP> -user sra -pass sra`

  NOTE:

  This command is the new option available in SRA 6.5.1

- `log`

  To view or modify the current log size limit and the maximum number of log history files to maintain.

  Syntax: `TPDSrm.exe log [-size LogSize] [-cnt Num]`

  - `-size <LogSize>`

    Specify the log file size limit in MB. The default size is 2 MB.
  - `-cnt <Num>`

    Specify the maximum log history files besides the latest log file to maintain. The default is 20 histories.

Managing HPE 3PAR StoreServ Storage SSL Certificates

HPE 3PAR StoreServ Storage enables management and validation of SSL certificates by the host and client applications to establish a secure connection.

HPE 3PAR CLI and HPE 3PAR OS versions `2.3.1 MU5 P35`, `3.1.1 MU3 P27`, `3.1.2 MU3 P16`, or later, supports a self-signed 2048-bit RSA SSL certificate for HPE 3PAR StoreServ Storage system.

After upgrade, SRA requires that you accept and validate the HPE 3PAR StoreServ server SSL certificate to perform any operations related to HPE 3PAR StoreServ. Validate the HPE 3PAR StoreServ certificate using the SRA command-line interface (`TPDSrm.exe`) before you configure arrays from SRM. If you do not accept the specific HPE 3PAR StoreServ certificate, then the connection is not established with HPE 3PAR StoreServ and SRA returns an error message to SRM.

For nonstretched storage configuration, retrieve the respective array certificates for the protected and recovery sites at SRM.

For stretched storage configuration, retrieve the array certificates for both protected and recovery sites at the individual site before you proceed with stretched storage configuration at SRM.

Certificate validation is supported using the SRA command-line options. SRA supports the following commands to view, validate, and remove the HPE 3PAR StoreServ certificate:

- `TPDSrm.exe viewcert`—To view the currently accepted StoreServ certificate.
- `TPDSrm.exe validatecert`—To accept and save the HPE 3PAR StoreServ certificate.

  NOTE: Accept and validate the HPE 3PAR StoreServ certificate using the `TPDSrm` utility before you configure SRM with HPE 3PAR StoreServ Storage System. If you do not validate the certificate, connection to HPE 3PAR StoreServ is denied.

  To accept and validate HPE 3PAR StoreServ certificates, configure the remote copy between HPE 3PAR StoreServ storage systems on the Protected and Recovery sites.

  For more information on configuring remote copy, refer *HPE 3PAR Remote Copy User Guide*.

- `TPDSrm.exe removecert`—To delete the accepted HPE 3PAR StoreServ certificate from the cache memory.

If you have configured an SLD remote copy environment with three HPE 3PAR StoreServ Storage systems (A, B, and C), where A—B is configured in synchronous mode, A—C in asynchronous periodic mode, and B—C is the standby link in asynchronous periodic mode. SRM/SRA is configured between HPE 3PAR StoreServ Storage systems A and C, then HPE 3PAR SRA requires that you accept and validate the HPE 3PAR StoreServ Storage SSL certificate for the primary and secondary HPE 3PAR StoreServ Storage systems on both the Protected and Recovery sites.

NOTE: Accept the certificate when the link between A and C is UP.

For 3DC-PP configuration, the certificates of all 3PAR arrays must be accepted in both the protected and recovery site SRM servers.

For example, `HPE 3PAR StoreServ A` and `SRM Server 1` are part of the protected site. `HPE 3PAR StoreServ C` and `SRM Server 2` are part of the recovery site. `HPE 3PAR StoreServ B` is then, synchronous backup system, which is not configured in the SRM/SRA. In `SRM Server 1`, you must accept and validate the `HPE 3PAR StoreServ A`, `HPE 3PAR StoreServ B`, and `HPE 3PAR StoreServ C` certificates. As a mandatory step, perform similar procedure for `SRM Server 2`.

NOTE: Accept the certificate when all the 3PAR remote copy links are up, among all three arrays in the 3DC-PP configurations.

Steps to configure HPE 3PAR SRA in VMware vCenter Site Recovery Manager

This section describes how to configure VMware vCenter Site Recovery Manager and HPE 3PAR SRA.

Configuring VMware vCenter Site Recovery Manager

To launch SRM using VMware vSphere WebClient, click **Start** > **VMware** > **vCenterServer** > **VMware vSphere WebClient** .

NOTE:

For more information about configuring VMware vCenter SRM, see the *VMware vCenter Site Recovery Manager* documentation.

IMPORTANT:

Ensure that both vCenter Servers are configured with each other and can be accessed from the respective sites.

Configuring HPE 3PAR SRA

Perform the following HPE 3PAR SRA configurations in SRM.

Procedure

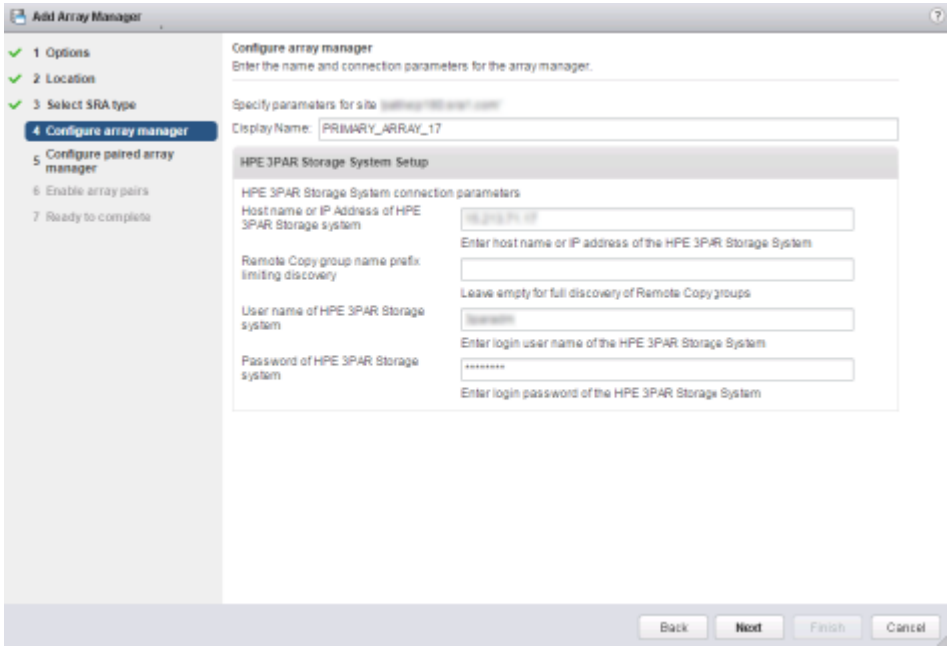
1. Click **VMware vSphere WebClient** > **Site Recovery**.

   The **Add Array Manager** window appears.
2. Enter the following information in the **Configure array manager** section.
   a. **Display Name**—Enter a display name for the HPE 3PAR StoreServ Storage System.
   b. **Host name or IP Address of HPE 3PAR Storage system**—Enter the host name or IP address of the storage system at the protected or recovery sites providing storage replication.
   c. **Remote Copy group name prefix limiting discovery**—The filtering condition to discover an RC group.

      NOTE:

      - You can use the asterisk (*) wildcard to search for an RC group in an array. Filtering reduces the time to discover the RC groups in an HPE 3PAR StoreServ Storage System.
      - If you do not specify any filtering conditions, then SRA discovers all Remote Copy groups in the HPE 3PAR StoreServ Storage System.

   d. **User name of the HPE 3PAR Storage system**—The user name that HPE 3PAR SRA uses to connect to the storage system.
   e. **Password of the HPE 3PAR Storage system**—The password that HPE 3PAR SRA uses to connect to the storage system.



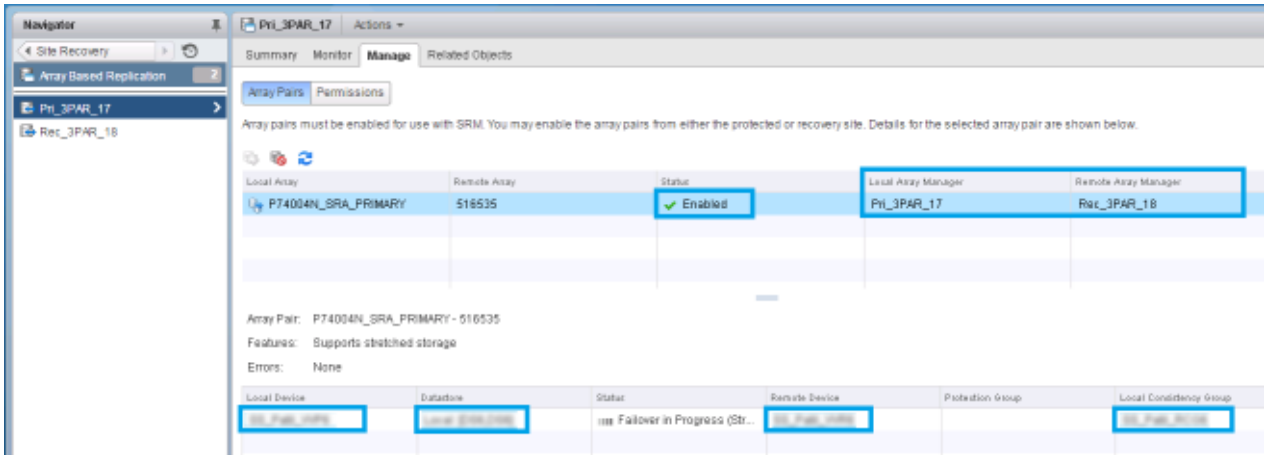
3. Click **Next**.

   The wizard displays the message `Ready to complete`.

4. Click **Finish**.

   After configuration, the wizard displays both HPE 3PAR StoreServ Storage System arrays in a paired state.

   The discovery of the devices starts automatically after the arrays are paired and they are displayed as shown in the figure:



   For an SLD configuration, after the Array Manager is added successfully, if you select the primary array, two target arrays are listed. Configure SRM/SRA between HPE 3PAR StoreServ Storage systems A and C.

   Figure 1 shows the SLD configuration of a primary and recovery array:

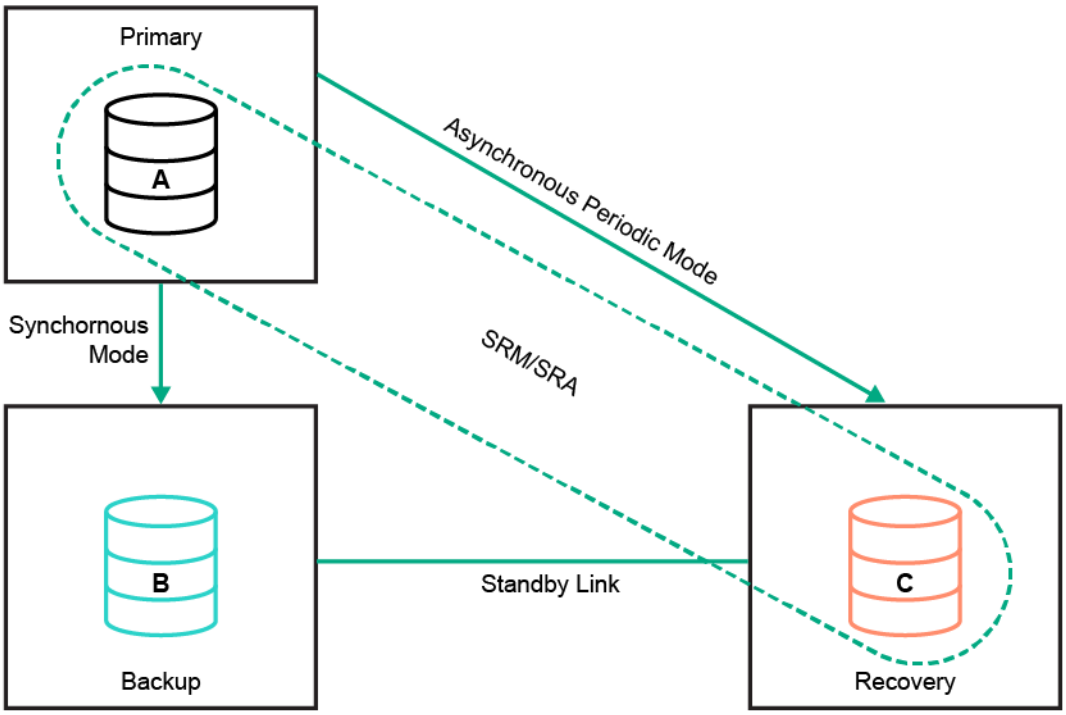


Figure 1: SLD configuration

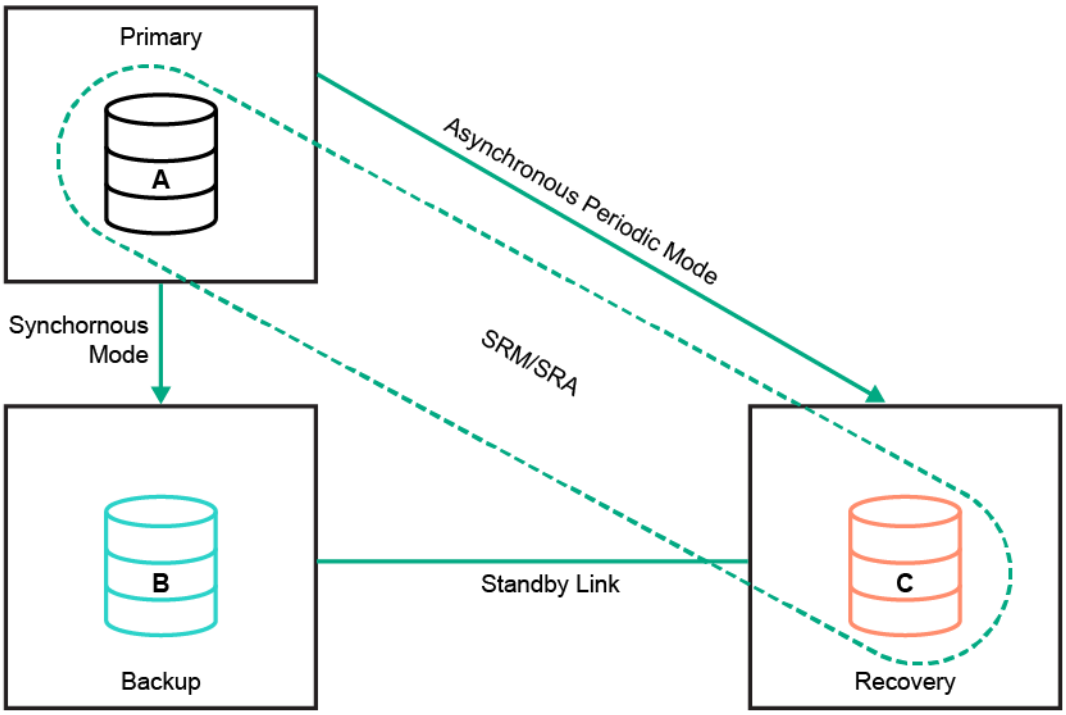


Figure 2:

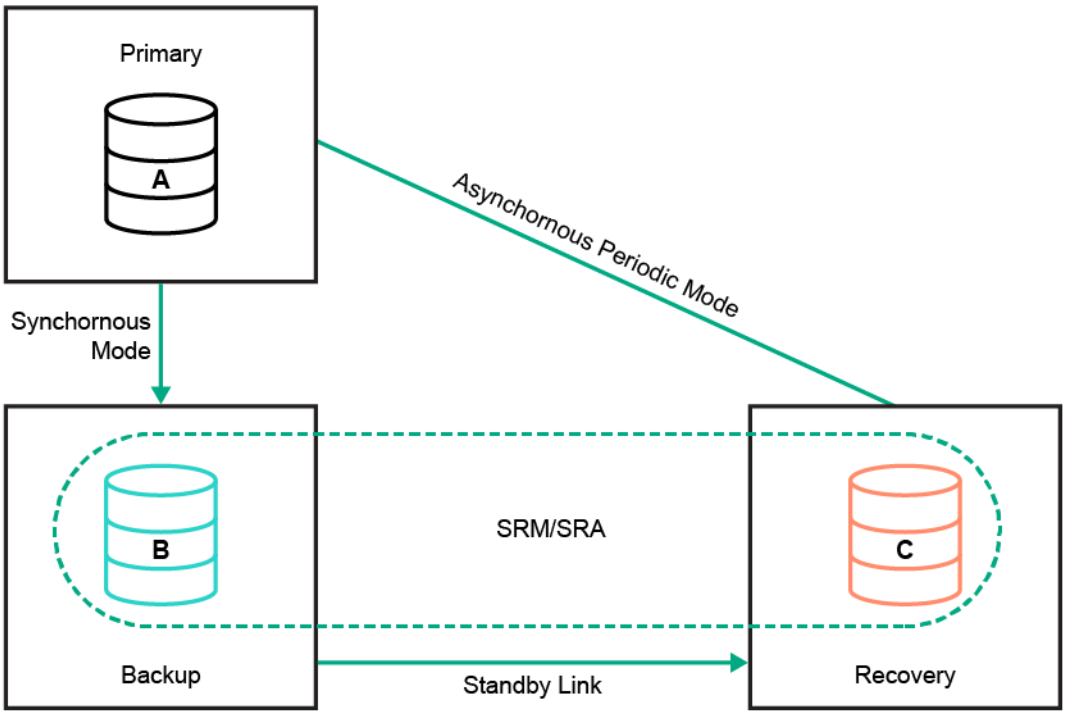


Figure 3: 3DC-PP configuration

3DC-PP configuration in SRM/SRA can be done either way as shown in Figure 2 and Figure 3.

> **NOTE:** In the 3DCPP configuration, some remote copy groups can be in Primary at A, Secondary at B and vice versa. You can configure, either A and C or B and C in the SRM protected and recovery site respectively.

The array pair between HPE 3PAR StoreServ Storage systems A and C is automatically enabled and paired as shown here:

NOTE:

Linked mode is not a prerequisite for using Site recovery manager. However, with SRM 5.1, linked mode has a new prerequisite. That is, if you want to use SRM 5.1 ensure that you install SSO at both sites. Also, install SRM specifically in Multisite mode.

For more information on configuring SRA in Linked mode, see **http://blogs.vmware.com/vsphere/2013/02/linked-mode-with-sso-for-srm.html.**

NOTE:

For both SLD and 3DC-PP configurations, refresh the devices for enabled array pairs in **Devices** tab, under **Array Managers** of SRM GUI, when all the remote copy links are up, among all the 3PAR arrays.

SRA behavior during SRM operations

This chapter describes the SRA behavior during SRM operations, such as test, failover, and failback.

Test

Use the test option to perform nondisruptive recovery operations. SRM communicates with HPE 3PAR SRA using the remote storage information obtained during the discovery process. SRA creates snapshots of the remote virtual volumes and presents them to the recovery ESXi server. During this recovery process, the VMs continue to run at the production site (protected site). You can verify that the VMs are running at the recovery site.

Clean Up

Perform the Cleanup operation after verifying that the VMs are running at the recovery site using the Test operation. SRA does a cleanup (unpresent and delete) of the previously created snapshots.

Recovery Operation from Protected Site to Recovery Site

2 Data Center Configurations

2 Data Centers (2DC) are configured with either of the following:

- SRM Standard storage feature with either Synchronous or asynchronous periodic or asynchronous streaming replication modes
- SRM stretched storage feature with synchronous replication mode

Planned Migration

During, the planned migration SRM shuts down the VMs at the protected site and unmounts the datastores. If the volumes are not already replicated yet, SRA replicates the data from the protected site volumes to the recovery site volumes, reverses the replication direction, changes the status of the replicated virtual volumes as read-only at protected site and read/write at the recovery site. After this operation, SRM rescans the datastores at the recovery site and restarts the VMs. Snapshots are created for the replicated virtual volumes in the arrays at both protected and recovery sites for the local backup purposes.

If the 3PAR remote copy links between the 3PAR arrays are up and running, the SRA initiates the planned migration operation successfully, else, SRA fails the planned migration operation.

SRA initiates the replication operation between the replicated volumes, one time before the VMs are shut down and, one time after the VMs are shut down.

NOTE: During planned migration, for stretched storage feature, the replicated VVs are not unexported to the ESXi hosts, they remain exported to the ESX hosts.

Disaster Recovery

When the protected datacenter is unavailable due to any disasters or failures and the datacenters remote copy links are down and SRM is still available in the protected site, user has to run the SRM recovery plan with disaster recovery option to start the VMs at the recovery site.

The SRA recovery process is similar to planned migration, except that planned migration would fail when remote copy link between SRM protected, and recovery site is down and disaster recovery tries to accomplish the task. If the remote copy links are down between the 3PAR arrays at the protected site, and recovery site,

then the replication operation is not performed between the replicated volumes. If the remote copy links are up and running, and if user chooses this option, then disaster recovery behaves like a planned migration.

Disaster Recovery with Forced Recovery

When the protected datacenter is offline and the SRM is not able to perform its usual tasks or is unavailable, user can run the disaster recovery with the forced recovery option. Forced recovery starts the virtual machines on the recovery site without performing any operations on the protected site.

NOTE: After the recovery operation, the replicated VVs are unexported to the ESX hosts in the protected site. Whereas in forced recovery, if both the arrays are down, the replicated VVs cannot be unexported to the ESXi hosts at the protected site. Prior to the reprotect operation, recovery required option has to be executed through SRM during which the replicated VVs are unexported to the ESX hosts in the protected site. The replicated VVs are exported to the ESX hosts in the recovery site and VMs are online after the recovery operation.

3 Data Center Configurations with 3PAR Synchronous Long Distance (SLD)

In the following SLD configuration scenario, A is the Primary System, C the Asynchronous Periodic Backup System, and B the Synchronous Backup System. SRM and SRA is configured between 3PAR StoreServ Storage systems A and C, where site A is the protected site and site C is the recovery site.

SLD configuration supports SRM recovery operation to site C only when both the arrays A and B are up and running (to perform any planned migration to site C) or when both the arrays A and B are down (to perform disaster recovery to site C). If either of the arrays A or B is down, SRM recovery operation to site C is not supported.

Planned Migration

During planned migration, SRM shuts down the VMs at protected site and unmounts the datastores. If the volumes are not replicated, SRA replicates the data from the protected site volumes to the recovery site volumes, reverses the replication direction, changes the status of the replicated virtual volumes as read-only at protected site and read/write at the recovery site. After this operation, SRM rescans the datastores at the recovery site and restarts the VMs. Snapshots are created for the replicated virtual volumes in the arrays at both protected and recovery sites for the local backup purposes.

SRA initiates the replication operation between the replicated volumes, one time before the VMs are shut down and, one time after the VMs are shut down.

If the 3PAR remote copy links between the 3PAR arrays at site A and site C that are configured with SRM and SRA are up and running, SRA initiates the planned migration operation successfully, else, the SRA fails the planned migration operation. Prior to planned migration operation to site C, ensure that the remote copy group is primary and VMs are up at site A.

When the **Remote Copy links between A and C are up**, SRM and SRA functions in the following ways for different Remote Copy link states:

- **All links are up:** SRM initiates data transfer from A–C and also between A and B through HPE 3PAR SRA. Once the sync is complete, SRA stops the RC groups between A–B and between A–C. SRA initiates failover at C, C becomes the Failover System and takes the role of the Primary System. C will have the latest data.
- **A–B link is down and B–C links is either up or down:** SRM initiates data transfer from A to C through HPE 3PAR SRA. Once the sync is complete, SRA stops the RC groups between A–C. SRA initiates a failover at C, C becomes the Failover System and takes the role of the Primary System. C will have the consistent and latest data.
- **B–C link is down:**

  When A-B link is up:

SRM initiates data transfer from A–C and also between A and B through HPE 3PAR SRA. Once the sync is complete, SRA stops the RC groups between A–B and between A–C. SRA initiates failover at C, C becomes the failover system and takes the role of the primary system. C will have the consistent and latest data.

Disaster Recovery

When the protected datacenter is unavailable due to any disasters or failures and the remote copy links between the datacenters are down and SRM is still available in the protected site, the user has to run the SRM recovery plan with disaster recovery option to start the VMs at the recovery site. The SRA recovery process is similar to planned migration, except that planned migration would fail when remote copy link between SRM protected, and recovery site is down and disaster recovery tries to accomplish the task. If the remote copy links are down between the 3PAR arrays at the protected site and recovery site, the replication operation is not performed between the replicated volumes. If the remote copy links are up and running and if the user chooses the disaster recovery option, then this option behaves like a planned migration.

NOTE: When both the arrays A and B are up and running, prior to performing the SRM recovery operation to site C, ensure that the remote copy group is primary at site A.

SRM/SRA functions in the following ways for different Remote Copy link states:

- **All links are up:** In case, where user performs disaster recovery instead of planned migration, SRM initiates data transfer from A to C and between A and B through HPE 3PAR SRA. Once the sync is complete, SRA stops the RC groups between A–B and between A–C and initiates failover at C. C becomes the Failover System and takes the role of the Primary System. C will have the consistent and latest data.
- **All links are down:**

  In a situation, where either A or B will have the most current data between the two arrays, HPE 3PAR SRA does not initiate any data transfer from either A or B to C. With the available data, C becomes the failover system and takes the role of the primary system.
- **A–C link is down and other two links are up:** HPE 3PAR SRA initiates the data transfer from A to B. Once the sync is complete, SRA stops the RC groups between A–B and initiates failover at C. C becomes the Failover System and takes the role of the Primary System. Before the failover operation at C, C gets the latest data from B. For more information, see section **Limitations of SLD configuration**.
- **A-B link is down and other two links are up:** SRM initiates data transfer from A to C through HPE 3PAR SRA. Once the sync is complete, SRA stops the RC groups between A–C and initiates a failover at C. C becomes the Failover System and takes the role of the Primary System. C gets the latest data from A.
- **B-C link is down and other two links are up:** SRM initiates data transfer from A to C and also A and B through HPE 3PAR SRA. Once the sync is complete, SRA stops the RC groups between A–B and between A–C and initiates failover at C. C becomes the Failover System and takes the role of the Primary System. C will have the consistent and latest data from A.
- **A-C and A-B links are down and other link (B-C) is up:** In a situation, where between the two arrays, either A or B will have the most current data, HPE 3PAR SRA does not initiate any data transfer from either A or B to C. With the available data, C becomes the failover system and takes the role of the primary system.
- **A-C and B-C links are down and other link (A-B) is up:** In a situation, where between the two arrays, either A or B will have the most current data, HPE 3PAR SRA does not initiate any data transfer from either A or B to C. With the available data, C becomes the failover system and takes the role of the primary system.
- **A-B and B-C links are down and other link (A-C) is up:** SRM initiates data transfer from A-C through HPE 3PAR SRA. Once the sync is complete, SRA stops the RC groups between A–C and initiates failover at C. C becomes the Failover System and takes the role of the Primary System. C will have the consistent and latest data from A.

CAUTION:
If C does not contain the most current data, any data which is in A and is replicated to B that is not replicated to C is discarded after SRM reprotect operation.

Disaster recovery with forced recovery

When the protected datacenter is offline and SRM is not able to perform its usual tasks or is unavailable, user can run the disaster recovery with the forced recovery option. Forced recovery starts the virtual machines on the recovery site without performing any operations on the protected site. This operation behaves exactly like the operation mentioned in the disaster recovery section except that there is no sync operation initiated between the sites and the recovery site volumes are made read/write and VMs are brought online in the recovery site.

NOTE: After the recovery operation, the replicated VVs are not unexported to the ESX hosts in the protected site. In case of forced recovery, if both the arrays are down, then at the protected site, the replicated VVs cannot be unexported to the ESXi hosts. Prior to reprotect operation, the recovery required option has to be executed through SRM during which the replicated VVs are unexported to the ESX hosts in the protected site. The replicated VVs are exported to the ESX hosts in the recovery site and VMs are online after the recovery operation.

Before doing the SRA reprotect operation, make sure that the VVs at site A (configured in SRM protected site) have the replication roles as primary. Use 3PAR `CLI` commands and 3PAR SSMC to view and get the roles as primary.

3 Data Center Configurations with Peer Persistence (3DC-PP)

In the following scenarios for 3DC-PP configuration, A is the Primary System, C the Asynchronous Periodic Backup System, and B the Synchronous Backup System. Multi-Target Peer Persistence (MT_PP) configuration is set up for these SLD groups. The sites A and B can be configured in the VMware Metro Storage Cluster (vMSC) configuration where the remote copy groups are in Peer Persistence configuration between A and B. The ESX hosts in the sites A and B are in the VMware vSphere HA cluster and have uniform host access to the replicated Peer Persistence Remote Copy group volumes. SRM/SRA is configured between 3PAR StoreServ Storage systems A and C, where site A is the protected site and site C is the recovery site. SRM/SRA can also be configured between 3PAR StoreServ Storage systems B and C instead of systems A and C, where site B is the protected site and site C is the recovery site.

The following scenarios for planned migration, disaster recovery, forced recovery and reprotect are mentioned, considering that A is the protected site, C is the recovery site and remote copy group role is Primary (Source) at A and Secondary at B. If the remote copy group role is Primary (Source) at B and Secondary at A irrespective of sites configured in SRM, then replace A with B for all the following scenarios.

If the remote copy group role is Primary-Rev at one side and Primary at another side, between A and B, then Primary-Rev is considered as Source.

SRM recovery operation including planned migration and disaster recovery to site C is supported in the 3DCPP configuration only when both the arrays A and B are up and running (to perform any planned migration to site C) or when both the arrays A and B are down (to perform disaster recovery to site C). When either of the arrays A or B is down, SRM recovery operation to site C is not supported.

3PAR 3DC-PP configuration comes with both quorum and non quorum configuration.

Planned Migration

In the following scenario, A is the protected site and C is the recovery site.

SRM shuts down the VMs at protected site and unmounts the Datastores. If the volumes are not already replicated SRA replicates the data from the protected site volumes to the recovery site volumes, reverses the replication direction, changes the status of the replicated virtual volumes as read-only at protected site and read/write at the recovery site. SRM rescans the Datastores at the recovery site and restarts the VMs.

Snapshots are created for the replicated virtual volumes in the arrays at both protected and recovery sites for the local backup purposes.

SRA initiates the replication operation between the replicated volumes, one time before the VMs are shut down and, one time after the VMs are shut down.

If the 3PAR remote copy links between the 3PAR arrays at sites A and C which are configured with SRM/SRA are up and running, SRA initiates planned migration operation successfully, else, the SRA fails the planned migration operation.

When the Remote Copy links between A and C are up, SRM and SRA functions in the following ways for different Remote Copy link states:

- **All links are up:** SRM initiates the data transfer from A to C and between A and B through HPE 3PAR SRA. Once the sync is complete, SRA stops the RC groups between A–B and between A–C and initiates failover at C. C becomes the Failover System and takes the role of the Primary System. C will have the consistent and latest data.
- **A–B link is down and B-C links is either up or down:** SRM initiates data transfer from A to C through HPE 3PAR SRA. Once the sync is complete, SRA stops the RC groups between A–C and initiates a failover at C. C becomes the Failover System and takes the role of the Primary System. C will have the consistent and latest data compared to site A.
- **B–C link is down:**

  When A-B link is up:

  SRM initiates data transfer from A to C and between A and B through HPE 3PAR SRA. Once the sync is complete, SRA stops the RC groups between A–B and between A–C and initiates failover at C. C becomes the failover system and takes the role of the primary system. C has the consistent and latest data compared to site A.

Disaster Recovery

When the protected datacenter is unavailable due to any disasters or failures and the remote copy links between the datacenters are down and SRM is still available in the protected site, the user has to run the SRM recovery plan with disaster recovery option to start the VMs at the recovery site. The SRA recovery process is similar to planned migration, except that planned migration would fail when remote copy link between SRM protected, and recovery site is down and disaster recovery tries to accomplish the task. If the remote copy links are down between the 3PAR arrays at the protected site and recovery site, then the replication operation is not performed between the replicated volumes. If the remote copy links are up and running and if the user chooses the disaster recovery option, then this option behaves like a planned migration.

SRM/SRA functions in the following ways for different Remote Copy link states:

- **All links are up:** In case, where the user performs disaster recovery instead of planned migration, SRM initiates data transfer from A to C and between A and B through HPE 3PAR SRA. Once the sync is complete, SRA stops the RC groups between A–B and between A–C and initiates failover at C. C becomes the Failover System and takes the role of the Primary System. C will have the consistent and latest data compared to site A.
- **All links are down:** In a situation, where either A or B will have the most current data between the two arrays, HPE 3PAR SRA does not initiate any data transfer from either A or B to C. With the available data, C becomes the failover system and takes the role of the primary system.
- **A–C link is down and other two links are up:**

  HPE 3PAR SRA initiates the data transfer from A to B. Once the sync is complete, SRA stops the RC groups between A–B and initiates failover at C. C becomes the Failover System and takes the role of the Primary System. Prior to failover operation at C, C gets the latest data from B. For more information, see **Limitations of SLD configuration**.
- **A-B link is down and other two links are up:**

SRM initiates data transfer from A to C through HPE 3PAR SRA. Once the sync is complete, SRA stops the RC groups between A–C and initiates a failover at C. C becomes the Failover System and takes the role of the Primary System. C will have the consistent and latest data compared to site A.

- **B-C link is down and other two links are up:** SRM initiates data transfer from A to C and also between A and B through HPE 3PAR SRA. Once the sync is complete, SRA stops the RC groups between A–B and between A–C and initiates failover at C. C becomes the Failover System and takes the role of the Primary System. C will have the consistent and latest data compared to site A.
- **A-C and A-B links are down and other link (B-C) is up:** In a situation, where either A or B will have the most current data between the two arrays, HPE 3PAR SRA does not initiate any data transfer from either A or B to C. With the available data, C becomes the failover system and takes the role of the primary system.
- **A-C and B-C links are down and other link (A-B) is up:**

  In a situation, where either A or B will have the most current data between the two arrays, HPE 3PAR SRA does not initiate any data transfer from either A or B to C. With the available data, C becomes the failover system and takes the role of the primary system.
- **A-B and B-C links are down and other link (A-C) is up:**

  SRM initiates data transfer from A to C through HPE 3PAR SRA. Once the sync is complete, SRA stops the RC groups between A–C and initiates failover at C. C becomes the Failover System and takes the role of the Primary System. C will have the consistent and latest data compared to site A.

> △ **CAUTION:**
> If C does not contain the most current data, any data replicated to B that is not replicated to C is discarded after SRM reprotect operation.

Disaster Recovery with Forced Recovery

When the protected data center is offline and the SRM cannot perform its usual tasks or is unavailable, the user can run the recovery with the forced recovery option. Forced recovery starts the virtual machines on the recovery site without performing any operations on the protected site. This operation behaves same as the operation mentioned in the disaster recovery, but there is no sync operation initiated between the sites. The recovery site volumes are made read/write and VMs are brought online in the recovery site.

> **NOTE:**
>
> After the recovery operation, the replicated VVs are unexported to the ESX hosts in the protected site, where the ESX hosts present in the sites A and B are in a HA cluster and the VVs are unexported to all the ESX hosts in both A and B. In case of forced recovery, if both the arrays are down, then at the protected site, the replicated VVs cannot be unexported to the ESXi hosts. Prior to reprotect operation, recovery required option has to be executed through SRM during which the replicated VVs are unexported to the ESX hosts in the protected site. The replicated VVs are exported to the ESX hosts in the recovery site and VMs are online after the recovery operation.

> **NOTE:** At the end of the SRM recovery operation, the replicated volumes at array A are unexported to the ESX hosts.
>
> The above statement is applicable for planned migration, disaster recovery and disaster recovery with forced recovery for 2DC, SLD and 3DC-PP configurations.

Reprotect Operation (after SRM recovery of VMs from protected site to recovery site).

Reprotect operation is performed to configure protection in the reverse direction (from Site B to Site A) as a preparation for failback to the original state. Reprotect operation allows SRA to perform the replication from the recovery site where VMs are running after the failover to the protected site, which means for the 2DC

configurations, remote copy links between the arrays has to be up and running before performing the reprotect operation.

For SLD and 3DC-PP configurations, the reprotect operation requires that the remote copy links between the new primary and both the targets to be up. If array C is the new primary system and if the links between C–A and C–B are up, then SRA starts the remote replication from C–A and C–B and waits until the sync is complete. During the reprotect operation, SRA triggers delta resync operation from C–A and C–B where C is the new primary system after failover. If the SRM recovery operation was performed when either A–B or B–C or both the remote copy links are down, as per the remote copy behavior, reprotect operation triggered by SRM through SRA will initiate a full copy from C–B only (from C–A, delta resync will be initiated).

NOTE: In SLD configuration, before performing reprotect operation, ensure that the C-A and C-B remote copy links are up and the replication role of the remote copy group at array A is primary and at array B is secondary using the 3PAR CLI commands.

The following steps must be followed before reprotect operation:

- Check the replication roles of the remote copy group at array A and array B by executing the following 3PAR CLI command.

  showrcopy groups
- If the replication role of the remote copy group at array A is primary and replication role of the remote copy group at array B is secondary, then no need of any manual operation. Here the assumption is that, array A is configured in the protected site.
- If the replication role of the remote copy group at array A is secondary and replication role of the remote copy group at array B is primary, then execute the following 3PAR CLI command at both array A and array B for this remote copy group, sequentially (order of execution does not matter).

  ```
  setrcopygroup reverse -current -local -t <sync target name> <Remote Copy Group Name>
  ```

  After executing the previous command, at both array A and array B successfully, execute the following 3PAR CLI command on array A or array B.

  ```
  setrcopygroup reverse -natural -t <sync target name> <Remote Copy Group Name>
  ```
- If the replication role of the remote copy group at array A is primary and replication role of the remote copy group at array B is primary-rev, then execute the following 3PAR CLI commands, for this remote copy group at array B, sequentially.

  ```
  setrcopygroup recover -t <sync target name> <Remote Copy Group Name>
  ```

  ```
  setrcopygroup reverse -natural -t <sync target name> <Remote Copy Group Name>
  ```

  Now the replication role of the remote copy group at array A is secondary and replication role of the remote copy group at array B is primary. Execute the following 3PAR CLI command at both array A and array B for this remote copy group sequentially (order of execution does not matter).

  ```
  setrcopygroup reverse -current -local -t <sync target name> <Remote Copy Group Name>
  ```

  After the previous command is executed at both array A and array B successfully, execute the following 3PAR CLI command on array A or array B.

  ```
  setrcopygroup reverse -natural -t <sync target name> <Remote Copy Group Name>
  ```
- If the replication role of the remote copy group at array A is primary-rev and replication role of the remote copy group at array B is primary, then execute the following 3PAR CLI commands, for this remote copy group at array A, sequentially.

  ```
  setrcopygroup recover -t <sync target name> <Remote Copy Group Name>
  ```

  ```
  setrcopygroup reverse -natural -t <sync target name> <Remote Copy Group Name>
  ```
- If the replication role of the remote copy group at array A is secondary-rev and replication role of the remote copy group at array B is primary-rev, then execute the following 3PAR CLI command, for this remote copy group at array A and array B, sequentially.

  ```
  setrcopygroup reverse -current -local -t <sync target name> <Remote Copy Group Name>
  ```
- If the replication role of the remote copy group at array A is primary-rev and replication role of the remote copy group at array B is secondary-rev, then execute the following 3PAR CLI commands for this remote copy group at array A.

```
setrcopygroup reverse -natural -t <sync target name> <Remote Copy Group
Name>
```

NOTE:

Check if the replication role of the remote copy group at array A is primary, and replication role of the remote copy group at array B is secondary, using showrcopy groups command, after performing the steps mentioned above.

Recovery Operation from Recovery Site to Protected Site (Failback)

Failback is a process that sets the replication environment to its original state at the protected site (local site).

For 2DC configuration, see section **Recovery Operation from Protected Site to Recovery Site** .

For SLD and 3DC-PP configurations, ensure that both the arrays A and B are up before performing the failback operations.

For SLD configuration, before performing failback operation, ensure that the C-A and C-B remote copy links are up, SRA first performs the sync operation from C-A and C-B if links are up, makes the virtual volumes at site A (configured in SRM as protected site) as read-write and mounts the datastore and VMs are brought online.

For 3DC-PP configuration, SRA first performs the sync operation from C-A and C-B if links are up, makes the virtual volumes at either site A or site B (sites that were primary previously) as read-write and mounts the datastore and VMs are brought online.

Snapshots are created for the replicated virtual volumes in the arrays at both protected and recovery sites for the local backup purposes.

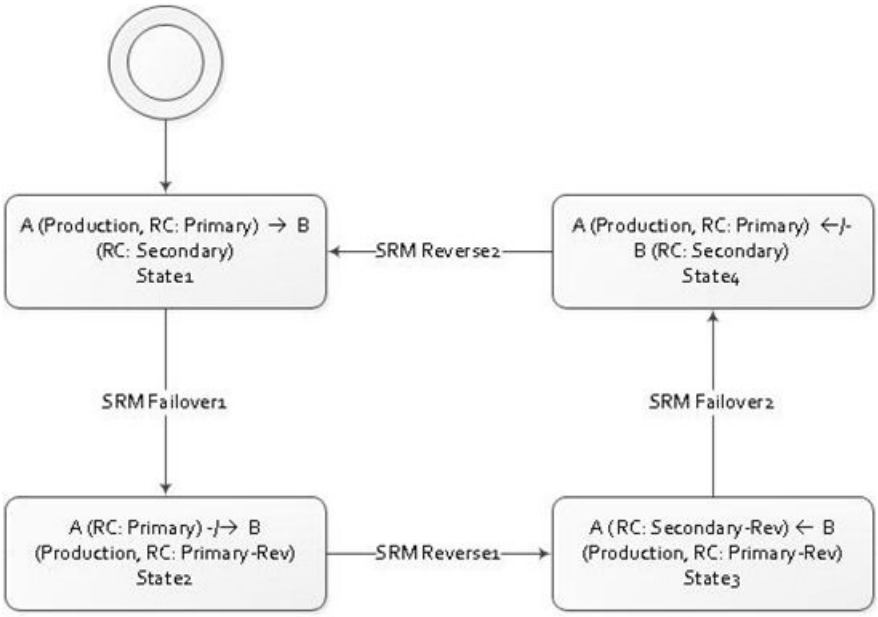
NOTE: After the recovery operation, the replicated VVs are unexported to the ESX hosts in the recovery site. In case of forced recovery and if the array C is down, then at the recovery site, the replicated VVs cannot be unexported to the ESXi hosts. Prior to reprotect operation, recovery required option has to be executed through SRM during which the replicated VVs are unexported to the ESX hosts in the recovery site. The replicated VVs are exported to the ESX hosts in the protected site and VMs are online after the recovery operation.

NOTE: At the end of the SRM recovery operation, the replicated volumes at array A are unexported to the ESX hosts.

Reprotect Operation (after SRM recovery of VMs from recovery site to protected site)

Reprotect operation allows SRA to perform the replication from the protected site where VMs are running after the failback to the recovery site, which means for the 2DC configurations, remote copy links between the arrays has to be up and running before performing the reprotect operation. For SLD configuration, the remote copy links between the sites configured in the SRM (A and C) has to be up and running before performing the reprotect operation. For 3DC-PP configuration, the remote copy links between the array where the replicated virtual volumes are primary and VMs are running, the array C has to be up and running before performing the reprotect operation.

State diagram for SRM and HPE 3PAR Remote Copy environment



Websites

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

www.hpe.com/storage/spock

Storage white papers and analyst reports

www.hpe.com/storage/whitepapers

For additional websites, see **Support and other resources**.

XP websites

XP7 documentation (Storage Information Library)

http://www.hpe.com/info/xp7-docs

XP7 documentation (HPESC)

http://www.hpe.com/info/XP7manuals

XP7 Command View Advanced Edition documentation (Storage Information Library)

http://www.hpe.com/info/cvae-docs

XP7 Command View Advanced Edition documentation (HPESC)

http://www.hpe.com/support/CVAE7/manuals

Related documents and terminology

For information about:	See:
Locating HPE 3PAR documents	**http://www.hpe.com/support/hpesc** Search on the product name "HPE 3PAR StoreServ Storage." Click the link for your product, and then click **Manuals**.
HPE 3PAR storage system software	
Storage concepts and terminology	**HPE 3PAR StoreServ Storage Concepts Guide**
Using the HPE 3PAR Management Console (GUI) to configure and administer 3PAR storage systems	**HPE 3PAR Management Console User's Guide**
Using the HPE 3PAR CLI to configure and administer storage systems	**HPE 3PAR Command Line Interface Administrator's Manual**
CLI commands	**HPE 3PAR Command Line Interface Reference**
Analyzing system performance	**HPE 3PAR System Reporter Software User's Guide**
Installing and maintaining the Host Explorer agent to manage host configuration and connectivity information	**HPE 3PAR Host Explorer User's Guide**
Creating applications compliant with the Common Information Model (CIM) to manage HPE 3PAR storage systems	**HPE 3PAR CIM API Programming Reference**
Migrating data from one HPE 3PAR storage system to another	**HPE 3PAR-to-3PAR Storage Peer Motion Guide**
Configuring the Secure Service Custodian server to monitor and control 3PAR storage systems	**HPE 3PAR Secure Service Custodian Configuration Utility Reference**
Using the CLI to configure and manage HPE 3PAR Remote Copy	**HPE 3PAR Remote Copy Software User's Guide**
Updating HPE 3PAR operating systems	**HPE 3PAR Upgrade Pre-Planning Guide**
Identifying storage system components, troubleshooting information, and detailed alert information	**HPE 3PAR F-Class, T-Class, and StoreServ 10000 Storage Troubleshooting Guide**
Installing, configuring, and maintaining the HPE 3PAR Policy Server	**HPE 3PAR Policy Server Installation and Setup Guide** **HPE 3PAR Policy Server Administration Guide**

Table Continued

For information about:	See:
Planning for HPE 3PAR storage system setup, including hardware specifications, installation considerations, power requirements, networking options, and cabling information for HPE 3PAR storage systems	
HPE 3PAR 7200 and 7400 storage systems	**HPE 3PAR StoreServ 7000 Storage Site Planning Manual**
HPE 3PAR 8000 storage systems	**HPE 3PAR StoreServ 8000 Storage Site Planning Manual**
HPE 3PAR 10000 storage systems	**HPE 3PAR StoreServ 10000 Storage Physical Planning Manual** **HPE 3PAR StoreServ 10000 Storage Third-Party Rack Physical Planning Manual**
HPE 3PAR 20000 storage systems	**HPE 3PAR StoreServ 20000 Storage Site Planning Manual**
Installing and maintaining HPE 3PAR storage systems	
Installing 7200 and 7400 storage systems and initializing the Service Processor	**HPE 3PAR StoreServ 7000 Storage Installation Guide** **HPE 3PAR StoreServ 7000 Storage SmartStart Software User's Guide**
Installing 8000 storage systems and initializing the Service Processor	**HPE 3PAR StoreServ 8000 Storage Installation Guide**
Maintaining, servicing, and upgrading 7200 and 7400 storage systems	**HPE 3PAR StoreServ 7000 Storage Service Guide**
Servicing and upgrading 8000 storage systems	**HPE 3PAR StoreServ 8000 Storage Service and Upgrade Guide**
Servicing 20000 storage systems	**HPE 3PAR StoreServ 20000 Storage Drive Servicing Guide**
Troubleshooting 7200 and 7400 storage systems	**HPE 3PAR StoreServ 7000 Storage Troubleshooting Guide**
Maintaining the Service Processor	**HPE 3PAR Service Processor Software User Guide** **HPE 3PAR Service Processor Onsite Customer Care (SPOCC) User's Guide**
HPE 3PAR host application solutions	
Backing up Oracle databases and using backups for disaster recovery	**HPE 3PAR Recovery Manager Software for Oracle User's Guide**
Backing up Exchange databases and using backups for disaster recovery	**HPE 3PAR Recovery Manager Software for Microsoft Exchange 2007 and 2010 User's Guide**

Table Continued

For information about:	See:
Backing up SQL databases and using backups for disaster recovery	**HPE 3PAR Recovery Manager Software for Microsoft SQL Server User’s Guide**
Backing up VMware databases and using backups for disaster recovery	**HPE 3PAR Management Plug-in and Recovery Manager Software for VMware vSphere User's Guide**
Installing and using the HPE 3PAR VSS (Volume Shadow Copy Service) Provider software for Microsoft Windows	**HPE 3PAR VSS Provider Software for Microsoft Windows User's Guide**
Best practices for setting up the Storage Replication Adapter for VMware vCenter	**HPE 3PAR Storage Replication Adapter for VMware vCenter Site Recovery Manager User Guide**
Troubleshooting the Storage Replication Adapter for VMware vCenter Site Recovery Manager	**HPE 3PAR Storage Replication Adapter for VMware vCenter Site Recovery Manager Troubleshooting Guide**
Installing and using vSphere Storage APIs for Array Integration (VAAI) plug-in software for VMware vSphere	**HPE 3PAR VAAI Plug-in Software for VMware vSphere User's Guide**

HPE 3PAR terminology updates

- The server previously known as the "InServ" is now called "HPE 3PAR StoreServ Storage system."
- The operating system previously known as the "InForm OS" is now called "HPE 3PAR OS."
- The user interface previously known as the "InForm Management Console (IMC)" is now called "HPE 3PAR Management Console."
- All products previously known as “3PAR” products are now called "HPE 3PAR" products.

Typographic conventions

Table 1: Document conventions

Convention	Element
Bold text	• Keys that you press • Text you typed into a GUI element, such as a text box • GUI elements that you click or select, such as menu items, buttons, and so on
`Monospace text`	• File and directory names • System output • Code • Commands, their arguments, and argument values
`<Monospace text in angle brackets>`	• Code variables • Command variables
`Bold monospace text`	• Commands you enter into a command line interface • System output emphasized for scannability

WARNING:

Indicates that failure to follow directions could result in bodily harm or death, or in irreversible damage to data or to the operating system.

CAUTION:

Indicates that failure to follow directions could result in damage to equipment or data.

NOTE:

Provides additional information.

Required

Indicates that a procedure must be followed as directed to achieve a functional and supported implementation based on testing at Hewlett Packard Enetrprise.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  http://www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  http://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

  www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  www.hpe.com/support/downloads

  Software Depot

  www.hpe.com/support/softwaredepot
- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience.

Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty for your product or to view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* reference document, go to the Enterprise Safety and Compliance website:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Important notes

SRM

SRM configuration

- It is strongly recommended to configure one protected group per Remote Copy group.
- If multiple Remote Copy groups are included in one protected group, it is recommended to set the same sync time on all the periodic Remote Copy groups.
- Support for Dynamic Access Groups. The concept of Dynamic Access Group support is to expose LUNs only to the specified HBA initiators provided by SRM. Any exposure of the participating LUNs made to other initiators not on the requested list is removed. This feature is always enabled.
- Multiple Remote Copy groups in one protected group is not recommended. HPE 3PAR SRA logs a warning to user if multiple instances of such configurations are detected during the Test or Recovery operation since this might be an indication that VMs are using virtual volumes from different Remote Copy groups.

SRM behavior

SRM might potentially time-out if multiple test failover or recovery operations are run simultaneously. Rerun the operation if the time-out error occurs. Alternatively, if the operations are run sequentially, the time-out error can be avoided.

SRA behavior

- The reserved virtual volume naming conventions for HPE 3PAR SRA are as follows:
  - `SRM_RO_<VVID>`
  - `SRM_RW_<VVID>`
  - `SRM_RECOVER_RO_<VVID>`
  - `SRM_TARGETBK_RO_<VVID>`
- If SRM runs into a virtual volume promote operation during reprotect, you must retry the reprotect operation.
- If needed, devices on the protected storage system must be read-only after `prepareFailover` and optionally take snapshots of the source devices for restoration. The way to make a device read-only to meet SRM's specification before failover is to remove VLUN exposure so that no one has access to it. If something goes wrong during the failover process, Remote Copy will internally manage taking the snapshots. HPE 3PAR SRA also takes a snapshot of the devices on the protected site of SRM (Remote Copy role `Primary` or `Primary-Rev`) for restore purposes since the user might activate the Remote Copy sync after failback (`setrcopygroup restore`) that might destroy the data content. The snapshot name must have the `SRM_RECOVER_RO_<VVID>` prefix.
- After failover, the devices on the protected storage system must be read-only. This is same for `prepareFailover`. The only difference is that, if the failover is part of the failback workflow, the protected storage system becomes `secondary` after failback using the `setrcopygroup restore` command. Devices under the secondary Remote Copy group will automatically have read-only access.
- More protection to the data on the recovery storage system. HPE 3PAR SRA takes a snapshot of the devices on the recovery storage system of the SRM before failover for optional restore purpose. The snapshot name will have the following prefix: `SRM_TARGETBK_RO_<VVID>`.
- If a failover operation is unsuccessful, be sure to clean up the local disaster state cache. Otherwise, the subsequent SRM operations will fail.

On both protected and recovery sites where HPE 3PAR SRA is installed, run the following commands:

- `TPDSrm viewstate`
- `TPDSrm cleanstate -sysid <StorageSystemID> -rcgroup <RCGroupName>`

- Primary Array is down or is taken offline.

  When the primary array is down or the remote copy link between the primary and secondary array is down, and if you must run the recovery operation, do the following:

  1. To execute the recovery, click **Disaster Recovery with Forced Recovery**.

     After completing this step, SRM displays the `Recovery Required` prompt. This operation implies that after bringing up the storage array or link, you must run recovery again.
  2. After bringing up the storage array or link, navigate to the **Devices** tab in SRM and click **Refresh** to rediscover the devices.

     Make sure that the devices are discovered again in SRM.
  3. Execute the **Recovery** and **Reprotect** operations.

     For more information about Disaster Recovery—Forced Recovery option, see the *VMware vCenter Site Recovery Manager* documentation.

- **Snapshots Management**

  SRA creates snapshots during Test and Recovery operation as described previously.

  - **Test**

    During Test, SRA creates snapshots of the remote virtual volumes and presents them to the recovery ESXi server. Naming conventions for these snapshots are `SRM_RO_<VVID>` and `SRM_RW_<VVID>`. Snapshots created during **Test** operation is deleted during `Cleanup` operation.
  - **Recovery**

    During SRM recovery from protected site to recovery site (failover operation), HPE 3PAR SRA takes a snapshot of the devices on the protected site of SRM during `preparefailover` for restoration if needed. Naming conventions for these snapshots are `SRM_RECOVER_RO_<VVID>`. HPE 3PAR SRA also takes a snapshot of the devices on the recovery storage system of the SRM before failover for optional restore purpose. The snapshot name has the prefix `SRM_TARGETBK_RO_<VVID>`. These snapshots will be deleted in the next SRM recovery from protected site to recovery site.

    During SRM recovery from recovery site to protected site (failback operation), similar logic is followed in SRA. But the names of the snapshot in the protected site 3PAR will be `SRM_TARGETBK_RO_<VVID>` (already `SRM_RECOVER_RO_<VVID>`snapshots exist during the first failover) and the names of the snapshot in the recovery site will be `SRM_RECOVER_RO_<VVID>`(already `SRM_TARGETBK_RO_VVID` snapshots exist during the first failover). These snapshots will be deleted in the next SRM recovery from recovery site to protected site.

    Therefore, there will be maximum of two snapshots existing for each VV of the RC groups in the 3PAR arrays at any time.

    SRA does not have any automatic function to delete these snapshots. User can decide to delete these snapshots manually after a successful failover. When a failover or failback operations is executed next time, SRA deletes the snapshots and create snapshots.

CAUTION:
When the remote copy links are up and running between the HPE 3PAR arrays, do not execute the SRM forced recovery operation during the failback scenario. That is, when you want to move VM workloads from recovery site to the protected site. If you perform the forced recovery operation during failback scenario, then subsequent recovery required operation fails.

- If you see, following warning during reprotect operation, you can ignore this message since the reprotect operation goes through successfully. This warning is because, the previous reprotect operation might have failed, and then the subsequent reprotect operation succeeds with the following warning message.

Warning: Unable to find source consistency group with target name.

- If the reprotect operation fails due to the SRM timeout, before the second reprotect operation is initiated, ensure to refresh the devices for enabled array pairs in **Devices** tab under **Array Managers** of SRM GUI.
- In a single SRM recovery plan, user must not create protection groups with a combination of 3DC-PP, SLD and sync, periodic and async streaming remote copy groups.
- Do not perform simultaneous execution of reprotect operation for the multiple recovery plans. If the execution of reprotect operation for the multiple recovery plans is performed, then you can see some unexpected behaviors.
- During the creation of virtual volume, which will be part of remote copy group, do not put "\", at the end of the comments field.
- In 3DC-PP configuration, If the SRM reprotect operation fails, and if get following error, follow the following steps to make the reprotect operations work successfully.
  - **Error code 1142**: Changing the replication role for the remote copy group `<RC group name>` in the array `<system id>` has failed.

    Manual intervention is required, to correct this error. Follow steps mentioned in the *HPE SRA user guide* for this error.

  For 3DC-PP configuration, If A is the Primary System, C is the Asynchronous Periodic Backup System, and B is the Synchronous Backup System. Multi-Target Peer Persistence (MT_PP) configuration is set up for these SLD groups. The sites A and B can be configured in the VMware Metro Storage Cluster (vMSC) configuration, where the remote copy groups are in Peer Persistence configuration between A and B. The ESX hosts in the sites A and B are in the VMware vSphere HA cluster and have uniform host access to the replicated Peer Persistence Remote Copy group volumes. SRM/SRA is configured between 3PAR StoreServ Storage systems A and C, where site A is the protected site and site C is the recovery site. SRM/SRA, can also be configured between 3PAR StoreServ Storage systems B and C, instead of systems A and C, where site B is the protected site, and site C is the recovery site.

  - Run the showrcopy groups `<RC group name>` command on both the arrays A and B.
  - If the group role is Primary-Rev or Secondary-Rev, run the `setrcopygroup reverse –local –natural <RC group name>` command to change the remote copy role to Primary or Secondary. Perform this step in both the arrays A and B. Perform this step only if the role is either primary-rev or secondary-rev. Ensure that the roles of the remote copy group at A and B are Primary and Secondary or vice versa, using `showrcopy` command before retrying the SRM reprotect operation.
- If the required devices are missing in the SRM GUI, check the SRA logs. If you see following warning in the 3DC-PP configuration, and not able to proceed with any of the SRM configurations, perform following steps.
  - **Warning**: Unable to fetch the information for the remote copy group which is part of SLD configuration (3DCPP).

    This warning could be due to one of the following reasons:

    – Unable to connect to the 3PAR array, which is in synchronous link and not configured in SRM.
    – Synchronous link of the SLD configuration could be down.

    Navigate to the **Devices** tab in SRM and click **Refresh** to rediscover the **Devices**. If the required devices are missing in the SRM GUI, then ensure that all the remote copy links are up and validation of the certificates is done using `tpdsrm.exe` for all the 3PAR arrays in the 3DC-PP configuration. After this step, again navigate to the **Devices** tab in SRM and click **Refresh** to rediscover the devices and you must see the required devices.

Host configuration

If an ESXi host has both FC and iSCSI definitions created on the 3PAR storage system and the vCenter Server also has both FC and iSCSI software adapter configured, per the vCenter Server's request, LUNs will be exposed to both host definitions in the event of a failover. However, if only one host definition is presented

on the HPE 3PAR storage system (either FC or iSCSI), HPE 3PAR SRA will only expose LUNs to whichever is defined on the HPE 3PAR Storage system.

3PAR Remote Copy

Remote Copy Behavior

In a disaster recovery scenario, when the Remote Copy links are down, the Remote Copy group status might still be `Started`. A failover attempt is successful only when the Remote Group status becomes `Stopped`.

SRA Support for virtual volume sets and host sets

HPE 3PAR SRA supports virtual volume set (vvset) and host set features of HPE 3PAR StoreServ Storage system.

The following are the HPE 3PAR SRA prerequisites for HPE 3PAR virtual volume set and HPE 3PAR host set features:

- To use the vv set feature for presenting the primary LUNs to a host, you must manually create the vv set and map the remote copy group virtual volumes to the created vv set in the primary HPE 3PAR StoreServ Storage system. Hewlett Packard Enterprise recommends that you create the vv set manually in the secondary HPE 3PAR StoreServ Storage system and map the RC group virtual volumes to the created vv set. In the event of a failover, HPE 3PAR SRA uses the manually created vv set to present LUNs to the host and HPE 3PAR SRA does not create the vv set by itself.

  All virtual volumes exposed using the same HPE 3PAR virtual volume set and protected by SRM must belong to the same remote copy group.

  If virtual volumes are from a virtual volume set with multiple VMs created, be sure to include all virtual volumes in a single remote copy group and in the same protection group. Otherwise, there is a potential of losing connectivity to the VMs if virtual volumes are included in more than one remote copy group and all remote copy groups are not included in the same protection group.
- User can also choose to use individual vvs, Instead of vvset, to export to the host during SRM recovery operation. User can use `TPDSrm.exe` command line options, to choose between individual vvs and vvset for the export operation.

  SRA does not use remote copy auto-created vvset (name starts with `RCP_`) for the remote copy group during the export operation.
- Ensure that the vvset name contains `RCP_<RC group name>`. If not, SRA will treat auto-created vvset, as manually created vvset during SRM recovery operation, resulting in multiple exports to the hosts/hostsets. This means that the remote copy group must not exceed the maximum character limit.

  Multiple exports to the hosts/hostsets can also happen, If there are multiple manually created vvsets for the remote copy group, during the SRM recovery operation.

  Do not create vvset manually starting with `RCP_`.

NOTE:

- **IMPORTANT:**
  If a remote copy group has virtual volumes that are not participating in datastore creation and if these virtual volumes are exposed to a different host, then the data might get corrupted.

- You must make sure that all virtual volumes in a remote copy group are participating in datastore. The virtual volumes in a remote copy group that are not participating in datastore creation must not be presented to a host.
- If the virtual volumes participating in an SRM configuration are exposed using a virtual volume set, any virtual volume member in this set, not used by SRM in the same protected group loses connectivity to the LUN after a failover.
- In the event of a failover, if the participating virtual volumes and hosts are part of vv set and host set respectively, then the LUNs are exposed using vv set and host set features, if the option to use individual vvs for export is not set through `TPDSrm` command line option.
- If the participating virtual volumes and hosts are not part of vv set and host set features, then the LUNs are individually exposed to the ESXi hosts.
- If a manually created VVSet contains volumes which are part of Remote Copy group, and also other volumes , then during failover SRA would unexport the vvset , hence all volumes contained in the Manually created VVSet will be unexported.

  NOTE:

  The user cannot individually unexport VV from an exported VVset.

- If a host is part of multiple hostsets, then SRA exports 3PAR virtual volumes multiple times to this host, where VMs are getting migrated using multiple hostsets, during SRM recovery operation.

Support for SLD and 3DC-PP

- HPE 3PAR SRA supports synchronous long-distance remote copy groups on HPE 3PAR OS 3.1.2 MU3 P16 or later MUs, and HPE 3PAR OS 3.1.3 or later.
- HPE 3PAR SRA can coexist with a synchronous long-distance remote copy group on HPE 3PAR OS version 3.1.1 to HPE 3PAR OS 3.1.2 MU2.
- For HPE 3PAR OS versions up to 3.1.2 MU2:
  - SRM supports only one-to-one replication. If one of the pairs in an SLD setup is selected for an SRM configuration, only the selected pair is started after reprotect in the failover workflow.
  - Before failback, all the pairs in the SLD setup must be started as a requirement for `setrcopygroup` restore operation. You can run the `showrcopy groups <groupname>` command to see the status of the SLD groups. All virtual volume members in the SLD setup must be in **Synced** status for the failback operation to be successful.

  NOTE:

  You cannot use Stretched storage feature in HPE 3PAR SLD and 3DC-PP configuration.

- SRA supports 3DC-PP configuration from 3PAR OS 3.3.1 onwards
- In the following SLD/3DC-PP configuration scenario, A is the Primary System, C is the Asynchronous Periodic Backup System, and B the Synchronous Backup System. SRM and SRA is configured between 3PAR StoreServ Storage systems A and C, where site A is the protected site and site C is the recovery site.

  In 3DC-PP and SLD configurations, if the switchover/failover is done for the first time from array A to B, before the sync operation to the periodic target, C gets triggered from the new primary volume B, as part of the periodic time interval, if B-C link goes down, VMs continue to run at B. At this moment, VMs

continue to run on array B. But if you trigger the planned migration/disaster recovery to site C, then SRA tries to sync data from array A volume to array C volume and then performs the storage failover operation after the sync operation is complete. In this situation, the sync operation from array A volume to array C volume goes to full sync. Due to this operation, the SRM recovery operation may time out. If you retry the SRM recovery operation, after the full sync is complete, this operation completes successfully.

If all the remote copy links are up, after moving the VMs to array B for the first time, do not perform the planned migration to array C until the first sync operation gets initiated and completed from B to C, based on periodic interval set. If B to C remote copy links go down, VMs continue to be online in array B. But if you want to migrate the VMs from array B to array C, during this situation (B to C link down), expect the full sync to be initiated from array A to array C volumes.

In 3DC-PP and SLD configurations, when the synchronization to the periodic target is in progress, and if the remote copy link goes down then synchronization will fail. At this stage if the SRM recovery operation is initiated at C, sometimes it fails with the error message, **Error**: StoreServ failover command has failed. Additional information: {**Error**: Volume `<volume name>` of group `<remote copy group name>` is currently the target of a copy or promote}.

If the user notices the previous error, retry the SRM operation after some time.

Workarounds for SLD and 3DC-PP error codes

This section describes workaround for the following SLD error codes:

- **Error code 1110**: One of the failure reasons might be remote copy replication role of the RC Group <`RC group name`> in target storeserv system `<target name>` is not secondary. Manually issue the HPE 3PAR remote copy setrcopygroup CLI command with reverse option to change the role.

  To resolve this:

  1. Run the `showrcopy groups <RC group name>` command on the original protected storage system.
  2. Run the `setrcopygroup reverse –local –current <RC group name>` command to change remote copy role, if the group role is `Primary-Rev`.
- **Error code 1112**: HPE 3PAR SRA is unable to connect to target storeserv system `<target name>` to execute the failover operation with restore option. HPE 3PAR SRA fails to connect to target HPE 3PAR storeserv system with the available credentials. Try the following options:

  1. Try accepting target HPE 3PAR SSL certificate again.
  2. Verify the connectivity to target 3PAR array from SRM host and retry the operation.

  If above options do not resolve the issue, manually issue the HPE 3PAR `remote copy setrcopygroup` CLI command with restore option to change the replication roles.

  To resolve this:

  1. Run the `showrcopy groups <RC group name>` command on the protected storage system.
  2. Run the `showrcopy groups <RC group name>` the command on the recovery storage system.
  3. Run the `setrcopygroup restore -t <targetname> <RC group name>` command on the protected storage system to change the remote copy roles, if the group role is `Primary-Rev` on the protected storage system, and `Secondary-Rev` on the recovery storage system.

Limitations of SLD and 3DC-PP configuration

In an SLD remote copy environment with three HPE 3PAR StoreServ Storage systems (A, B, and C), where A—B is configured in synchronous mode, A—C in asynchronous periodic mode, and B—C is the standby link in asynchronous periodic mode. SRM/SRA is configured between HPE 3PAR StoreServ Storage systems A and C.

- During the reprotect operation, SRA triggers a delta resync operation from C—A and C—B, where C is the new primary system after failover. If the SRM recovery operation was performed when either A—B or B—

C or both the remote copy links were down, then as per the remote copy behavior, the reprotect operation triggered by SRM through SRA will initiate a full copy from C—B only (from C—A delta resync will be initiated).

- SRM recovery operation initiated at C does a delta sync from B to C and then initiate the failover operation at C. If the A—C link is down, as per the remote copy behavior, the data transfer from B—C becomes full-sync mode during SRM recovery operation at C.

  Workaround: When all the remote copy links are UP, run the SRM *Test* operation at least once before executing the disaster recovery at 'C' when the A—C link is down, to avoid B—C going to FULL SYNC.

  NOTE:

  In a single recovery plan, 3DCPP groups must not be mixed with other RCGs like 2DC, stretched storage, and SLD as these are not supported configuration.

Support for Stretched Storage

CAUTION:
3PAR Remote Copy links down, Storage arrays and all IO paths operational

Do not perform SRM Failover/Failback operation whenever the recovery plan includes VMs residing on stretched devices and when Remote Copy links are down between two 3PAR storage arrays and both the arrays and all IO paths are operational to avoid any potential data corruption issues.

- In stretched storage, if the reprotect operation is performed after a disaster recovery from protected site to recovery site, then reprotect is completed successfully, with **Error message**: Error-Failed to sync data on replica devices. A specified parameter is not correct: deviceGroup.
- In case of an inoperable protected array, when you execute recovery (failover) (disaster recovery with forced recovery) to migrate VMs to the recovery site in SRM, the recovery operation succeeds and prompts you to execute recovery once again.

  The protected storage array and links between storage arrays must be functional before executing recovery again. After performing these steps, run `Discover Devices` for the selected array pair in SRM GUI to complete the recovery operation.
- In case of an inoperable recovery array, when you execute recovery (failback) (disaster recovery with forced recovery) to migrate VMs back to the protected site in SRM, the recovery operation succeeds and prompts you to execute recovery once again.

  The recovery storage array and links between storage arrays must be functional before executing recovery again. After performing these steps, run `Discover Devices` for the selected array pair in SRM GUI to complete the recovery operation.
- For the previous two bullet points, after refreshing the devices (Discover Devices) in the SRM GUI, you may get the following error:

  Internal error: `std::exception 'class Dr::Xml::XmlValidateException` "Unexpected element 'Identity' found"

  Ignore this error and continue with "Recovery Required" and further SRM operations.
- Error in recovery plan when you shut down the protected VMs.

  Error:*`Operation timed out`* : 900 seconds during Shutdown of VMs at Protected Site.

  If you use SRM to protect datastores on arrays that support dynamic swap, then running a disaster recovery when the protected site is partially operable or running a force recovery might cause errors when rerunning the recovery plan to complete protected site operations. One such error occurs when the protected site becomes operational, but SRM is unable to shut down the protected virtual machines. This error usually occurs when 3PAR array enables the protected LUNs as read-only, which renders ESXi unable to complete I/O for powered on protected virtual machines.

To complete the recovery workflow, reboot ESXi hosts on the protected site that affects read-only LUNs.

- In the protected and recovery sites, if both the 3PAR arrays are up and running, remote copy links are up and only the ESX servers and SRM server in the protected site go down, follow the following steps to perform SRM recovery operation:

  Before performing SRM recovery operation, execute the following 3PAR CLI commands:

  1. Perform showrcopy on both the protected and recovery site arrays. Ensure that the remote copy group roles are Primary and Secondary respectively, and group status is **Started** and volumes status is in **Synced** state.
  2. Execute, following `setrcopygroup` command in the protected site array where the remote copy group role is Primary:

     ```
     setrcopygroup switchover <remotecopygroupname>
     ```
  3. Perform showrcopy on both the protected and recovery site arrays. Ensure that the remote copy group roles are Secondary and Primary respectively, on protected and recovery site arrays and group status is **Started** and volumes status is in **Synced** state.
  4. After executing the previous steps, perform the SRM recovery operation.

  NOTE: In this scenario, if only SRM server in the protected site is down and ESX servers are up and running, it is suggested not to perform SRM recovery operation. As you know, VMs are still running in the protected site ESX servers.

  If you still want to perform SRM recovery, then follow the previous steps.

  If you do not follow the previous steps and perform SRM recovery operation, then recovery operation may fail with the following error:

  Error: Cannot failover Peer Persistence group `<remote copy group name>` as target `<target name>` is still accessible.

- When you execute **Recovery** > **Planned Migration without vMotion** in SRM, the recovery operation might fail due to *SyncFailed*.

  SyncFailed: Failed to sync data for group or Cannot process consistency group <groupname> with role 'target' when expected consistency group with role 'source'.

  To complete the recovery workflow, run **Discover Devices** operation manually for the selected array pair in SRM GUI and execute **Recovery** > **Planned Migration without vMotion**.