



Hewlett Packard
Enterprise

HPE XP Storage Replication Adapter Software for VMware vCenter SRM version 2.5.x Administrative Guide

Abstract

This guide contains detailed instructions for installing, removing, configuring, and using the HPE Virtualization Adapter. The intended audience has independent knowledge of related OS software and of HPE disk arrays and software.

Part Number: P02067-003a
Published: February 2020
Edition: 13

© Copyright 2011-2020 Hewlett Packard Enterprise Development LP

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

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

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Contents

Overview.....	5
About HPE Storage Replication Adapter and Site Recovery Manager.....	5
VMware vCenter infrastructure.....	5
HPE storage and replication software products.....	5
RAID Manager.....	6
How the VMware® vCenter SRM™/SRA solution works.....	7
 Requirements, planning, and prerequisites.....	 8
Requirements.....	9
SRA/VMware® vCenter SRM™/RAID Manager location options.....	11
Test options.....	11
Using the S-VOL for testing.....	12
Using a copy of the S-VOL for testing.....	12
Configurations with protected and recovery VMs on the same site.....	13
Consistency groups and VM failover groups.....	13
Consistency groups and same-time split operations.....	13
About the Continuous Access Synchronous fence level “Never”.....	14
Prerequisites for High Availability configuration.....	14
 Deployment.....	 17
Supported SRM/SRA configurations.....	17
Deployment workflow.....	19
Installing RAID Manager.....	20
Creating and configuring a RAID Manager command device.....	21
Setting up HORCM configuration definition files.....	23
Editing HORCM.conf files.....	23
Starting HORCM instances, creating pairs.....	28
Starting HORCM instances, creating pairs (Windows).....	28
Starting HORCM instances, creating pairs (UNIX).....	29
Creating a copy for testing on the recovery site.....	30
Creating a copy for testing on the recovery site (Windows).....	30
Creating a copy for testing on the recovery site (UNIX).....	31
Setting environment variables.....	31
Defining environment variables using the GUI.....	33
Defining environment variables using the environmental setting file.....	34
About SSH.....	35
Configuring SRA for testing.....	36
Setting environment variables on the VMware® vCenter SRM™ host.....	37
Setting environment variables on a UNIX Host.....	37
SRA installation.....	38
Installing HPE SRA 2.x.....	38
Removing an earlier version of SRA.....	39
Checking the SRA version.....	40
Obtaining the latest rmsra20.....	41
Deploying rmsra20.....	41
Configuring SRM™ to communicate with RMXPSRA20 (SRM 5.x or earlier).....	42
Enabling array managers.....	46
Verifying devices.....	46

Configuring SRM to communicate with RMXPSRA20 (SRM 6.0 or later).....	47
Add array manager.....	48
Check devices.....	54
Configuring SRM to communicate with RMXPSRA20 (SRM 8.2 or later).....	55
Add array manager.....	56
Check devices.....	57
Performing reprotect and failback.....	57
Troubleshooting.....	59
Error messages on VMware® vCenter SRM™ log files.....	59
XML errors received from VMware® vCenter SRM™	59
Failure to launch scripts.....	65
Collecting information before contacting customer support.....	66
VMware® vCenter SRM™/SRA local configuration.....	66
VMware® vCenter SRM™/SRA remote configuration.....	67
VMware® vCenter SRM™/SRA Photon™ OS configuration.....	67
SRA Change Log.....	69
Change log for SRA.....	69
Configurations with both sites active.....	71
Protecting both sites.....	71
HORCM definition file setup.....	71
Websites.....	74
Support and other resources.....	75
Accessing Hewlett Packard Enterprise Support.....	75
Accessing updates.....	75
Customer self repair.....	76
Remote support.....	76
Warranty information.....	76
Regulatory information.....	77
Documentation feedback.....	77

Overview

This chapter describes HPE Storage Replication Adapter (SRA) 2.x and the VMware® vCenter Site Recovery Manager™ 5.x/6.x/8.x disaster recovery solution when used with HPE storage.

About HPE Storage Replication Adapter and Site Recovery Manager

The VMware® vCenter Site Recovery Manager™ 5.x/6.x/8.x (VMware® vCenter SRM™) software is a VMware application that automates the disaster recovery process using storage-based replication. HPE Storage Replication Adapter (SRA) is the interface that integrates HPE storage systems and replication software with VMware vCenter SRM processes.

Used together, VMware vCenter SRM and HPE storage and software provide an automated and seamless disaster recovery solution within the VMware vCenter infrastructure.

VMware vCenter infrastructure

The VMware® vCenter SRM™/HPE SRA solution on the VMware side consists of the following:

- VMware vSphere, the virtualization platform with data center infrastructure. vSphere includes:
 - VMware ESX/ESXi host, which is a virtualization platform that provides a data center infrastructure in which many virtual machines share hardware resources from a single physical machine. The ESX/ESXi host loads directly on a physical server.
 - vCenter Server, which provides management of one or multiple vSphere environments.

These vSphere elements are used at the protected and recovery sites.

- VMware® vCenter SRM™, which provides a disaster recovery solution that reduces planned and unplanned downtime of the vSphere infrastructure.

HPE storage and replication software products

The HPE Storage Replication Adapter (SRA) links VMware® vCenter SRM™ and HPE storage and replication software. The SRA/VMware® vCenter SRM™ solution supports:

- XP8 Storage (XP8)
- XP7 Storage (XP7)
- P9500 Storage (P9500)
- XP24000/XP20000 Disk Array (XP24000/XP20000 Disk Array)

NOTE: For the latest information about HPE storage systems supported by SRA, see the VMware Compatibility Guide on the VMware website.

HPE remote and in-system replication are key features of the solution. Remote replication is used to backup protected site data at the recovery site in a remote location. In-system replication is used on the remote site to create a clone volume for testing the VMware® vCenter SRM™-SRA solution.

The following remote replication products are supported:

- HPE Continuous Access Journal, which provides long-distance asynchronous replication across any distance without significant impact on host performance.
- HPE Continuous Access Synchronous Remote Replication, which provides synchronous remote replication.
- High Availability (HA), which provides synchronous remote replication.

The following in-system replication products are supported for creating a clone of the recovery site volume for testing.

- Business Copy (BC), which creates RAID-protected duplicate volumes within the storage system. With Business Copy, you create a clone of the remote backup volume in the remote storage system.
- Fast Snap (FS), which creates a virtual backup of a production volume from a point in time “snapshot”.

HPE users manage storage and data replication operations using the RAID Manager command line interface (CLI) software product.

The following figure shows the basic VMware® vCenter SRM™/SRA components.

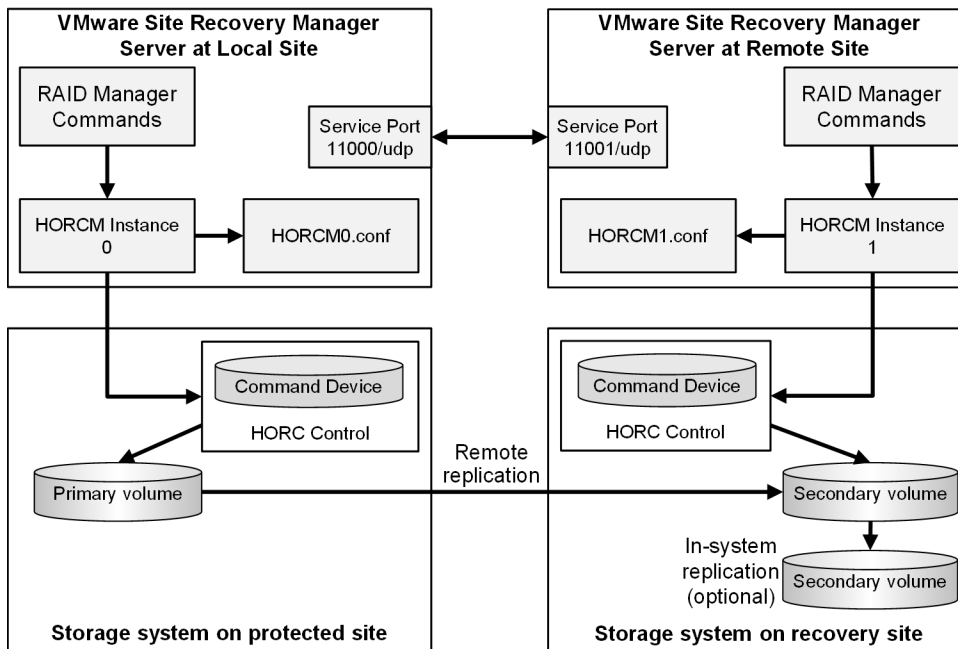


Figure 1: VMware® vCenter SRM™ and HPE components

RAID Manager

HPE's remote and in-system replication software require RAID Manager to manage the pairs. The adapter plug-in links RAID Manager with Site Recovery Manager (SRM).

There are two RAID Manager components:

- RAID Manager command devices, which reside on the storage systems. RAID Manager uses the command device as the interface to the storage system from the host. The command device accepts RAID Manager commands from the host and executes them on the storage system. The command device is a dedicated logical volume.

NOTE: The two methods for issuing RAID Manager commands from a host are the in-band method and the out-of-band method. In environments using SRM, the in-band method is recommended due to performance considerations.

- HORM Manager (HORCM), which resides on the RAID Manager server. HORCM operates as a daemon process. When activated, HORCM refers to the RAID Manager configuration definition files, also located on the server. The HORCM instance communicates with the storage system and remote servers.

HORCM definition files describe the storage systems, pair volumes, and data paths. When a user issues a command, RAID Manager uses the information in the HORCM files to identify which volumes are the targets of the command.

Two HORCM files are needed for each pair. One file describes the primary volumes (P-VOLs), which are also referred to as “protected volumes”, and the other file describes the secondary volumes (S-VOLs), which are also referred to as “recovery volumes”.

Figure 1: VMware vCenter SRM and HPE components on page 6 shows a two-server, two-HORCM-instance setup with optional in-system test copy.

How the VMware® vCenter SRM™/SRA solution works

The VMware® vCenter SRM™ software coordinates processing with HPE storage and replication so that in a recovery condition, the virtual machines at the protected site are shut down and the replicated virtual machines are powered up.

Recovery is guided by a recovery plan that specifies the order in which the virtual machines are to be started up.

After a recovery is performed, the running virtual machines are no longer protected. The VMware® vCenter SRM™ software provides a reprotect operation, which runs after the original protected site is back up. Reprotect activates RAID Manager operations that reverse-synchronize data in the storage systems from recovery site to protected site.

Finally, VMware® vCenter SRM™-supported failback (XP8, XP7, P9500, and XP24000/XP20000 Disk Array) and reprotect operations allow you to restore protection back to the original configuration, with data flow from the protected site to the recovery site.

VMware® vCenter SRM™ allows you to test recovery plans using an in-system copy of the replicated data without disrupting ongoing operations at either site.

Requirements, planning, and prerequisites

You share responsibilities for planning and deploying SRA 2.x with the HPE account team, which will assist you as needed throughout the process. The account team coordinates HPE resources to ensure a successful installation and deployment. Before you begin planning, please review the deployment workflow in **Deployment** on page 17.

Requirements

Table 1: Required hardware and software

Item	Description
HPE Storage Replication Adapter version	SRA 02.01.04—VMware® vCenter SRM™ 5.x/6.0/6.1: <ul style="list-style-type: none"> • Supports SSH connections. • Supports VMware® vCenter SRM™ on one array in loopback mode, for testing only in non-production environments. • Requires RMXPSRA_X64.exe.
	SRA 02.03.01—VMware® vCenter SRM™ 6.1 or later: <ul style="list-style-type: none"> • Supports RAID Manager version 01.36.03 or later. • Supports High Availability (HA). • Supports iSCSI for XP7. • Requires HPE_RMXPSRA_X64-02.03.01.exe.
	SRA 02.05.0x—VMware® vCenter SRM™ 6.1 or later: <ul style="list-style-type: none"> • Supports RAID Manager version 01-46-02 or later. • Supports High Availability (HA). • Supports iSCSI for XP8 and XP7. • Requires HPE_RMXPSRA_X64-02.05.00.exe or HPE_RMXPSRA_X64-02.05.00.gz or later.
Supported HPE storage systems	SRA 02.01.04—VMware® vCenter SRM™ 5.x/6.0/6.1: <ul style="list-style-type: none"> • XP7: 80-01-01 or later • P9500: 70-05-xx or later • XP24000/XP20000 Disk Array: 60-07-xx or later • XP12000 Disk Array/XP10000 Disk Array: 50-09-xx or later SRA 02.03.01—VMware® vCenter SRM™ 6.1 or later: <ul style="list-style-type: none"> • XP7: 80-01-01 or later When HA is used: 80-04-02 or later • P9500: 70-05-xx or later • XP24000/XP20000 Disk Array: 60-07-xx or later SRA 02.05.0x—VMware® vCenter SRM™ 6.1 or later:

Table Continued

Item	Description
	<ul style="list-style-type: none"> XP8: 90-01-02 or later XP7: 80-01-01 or later When HA is used: 80-04-02 or later P9500: 70-05-xx or later <p>NOTE: Refer to the VMware official website for supported storage.</p>
Supported operating systems	<ul style="list-style-type: none"> Windows Server 2003: SRA 2.1 and earlier Windows Server 2008 and later: SRA 2.2 and later Linux Solaris Solaris/x86 HP-UX AIX®
VMware infrastructure	<p>Environments:</p> <ul style="list-style-type: none"> SRM (can also be installed on a physical server). Use SRM 5.x, SRM 6.0, SRM 6.1, SRM 6.5, SRM 8.1, or SRM 8.2. <p>Protected site:</p> <ul style="list-style-type: none"> VMware vCenter Server ESX/ESXi host Datastore on the ESX/ESXi host <p>Recovery site:</p> <ul style="list-style-type: none"> VMware vCenter Server ESX/ESXi host Datastores: You do not need to create datastores in the recovery site. However, two volumes with the same capacity as the datastore of the primary ESX/ESXi host are required. The volumes must be mapped to the recovery ESX/ESXi host only when Cnt Ac-S or Cnt Ac-J is used. Do not install datastores on these volumes. In the case of HA, secondary volumes of HA pairs are recognized as datastores in the recovery site.

Table Continued

Item	Description
RAID Manager	<p>RAID Manager must be installed on on Windows or UNIX systems at the protected site and recovery site. If Windows is used, RAID Manager and VMware® vCenter SRM™ must be installed on the same server.</p> <p>For more information, see <u>SRA/VMware® vCenter SRM™/RAID Manager location options</u> on page 11.</p> <p>Version 01.27.04 or later: Supports P9500, XP24000/XP20000 Disk Array, XP12000 Disk Array/XP10000 Disk Array.</p> <p>Version 01.30.03 or later: Adds support for XP7.</p> <p>Version 01.51.02 or later: Adds support for XP8.</p>
Remote replication	<p>For XP8, XP7, P9500, and XP24000/XP20000 Disk Array, use one of the following:</p> <ul style="list-style-type: none"> • Continuous Access Synchronous Remote Replication • Continuous Access Journal • High Availability
In-system replication	<p>Business Copy, Fast Snap, or Snapshot. Used for testing:</p> <p>Optional for XP8, XP7, P9500, and XP24000/XP20000 Disk Array</p>

SRA/VMware® vCenter SRM™/RAID Manager location options

The VMware® vCenter SRM™ array manager configuration for SRA 2.x varies depending on the location of RAID Manager.

- If the Windows version of RAID Manager is used, RAID Manager must be installed on both protection and recovery sites. This means that RAID Manager, VMware® vCenter SRM™, and SRA 2.x must be installed on the same servers. SRA 2.x will communicate locally with RAID Manager.
- If the UNIX version of RAID Manager is used, VMware® vCenter SRM™ array managers can be configured using SSH* to remotely communicate with RAID Manager instances. VMware® vCenter SRM™ and SRA must be installed on the same server, and RAID Manager can run on separate (remote) UNIX hosts. This allows you to run a centralized UNIX RAID Manager host instead of running UNIX RAID Manager hosts for each site (protection and recovery). HPE does not recommend running a centralized RAID Manager host for redundancy reasons.

* SRA 2.3.1 and later versions support only SSH and does not support telnet.

Test options

SRA/VMware® vCenter SRM™ recovery takes place automatically. To ensure that recovery occurs as expected, the recovery processes must be tested manually.

For XP8, XP7, P9500, and XP24000/XP20000 Disk Array, testing is done using either a copy of the S-VOL (recommended) or the remote S-VOL.

Note: The remote S-VOL for HA cannot be used.

Using the S-VOL for testing

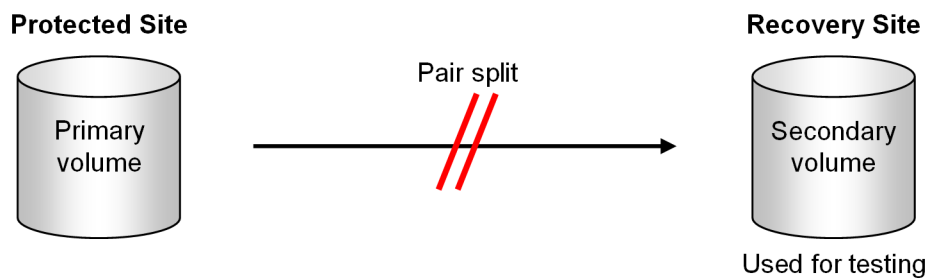
For XP8, XP7, P9500, or XP24000/XP20000 Disk Array, VMware® vCenter SRM™ can use the S-VOL on the remote site for test failover.

However, note the following important restrictions:

- Testing with the S-VOL disrupts replication from the primary to the secondary volumes.
You can avoid disruption to replication if you test during planned outages.
- The S-VOL is not available for an actual failover should the need arise.
- After testing, the pair is resynchronized with data that was stored in a bitmap. The updates are out of order, rendering the S-VOL unavailable for an actual failover should the need arise, until resynchronization is completed.

Required configuration for testing with S-VOL

The Continuous Access Synchronous or Continuous Access Journal pair must be split in order to test using the S-VOL. The following figure shows the VMware® vCenter SRM™ configuration during test failover using the S-VOL.



To enable SRA to allow the split and to test with the S-VOL, you must set two environment variables on the host. For instructions, see [Configuring SRA for testing](#) on page 36.

Using a copy of the S-VOL for testing

You can test failover with no disruption to replication between primary secondary systems using a point-in-time copy of the remote system S-VOL.

During test failover, the remote replication pair remains in PAIR status, and therefore protection continues uninterrupted.

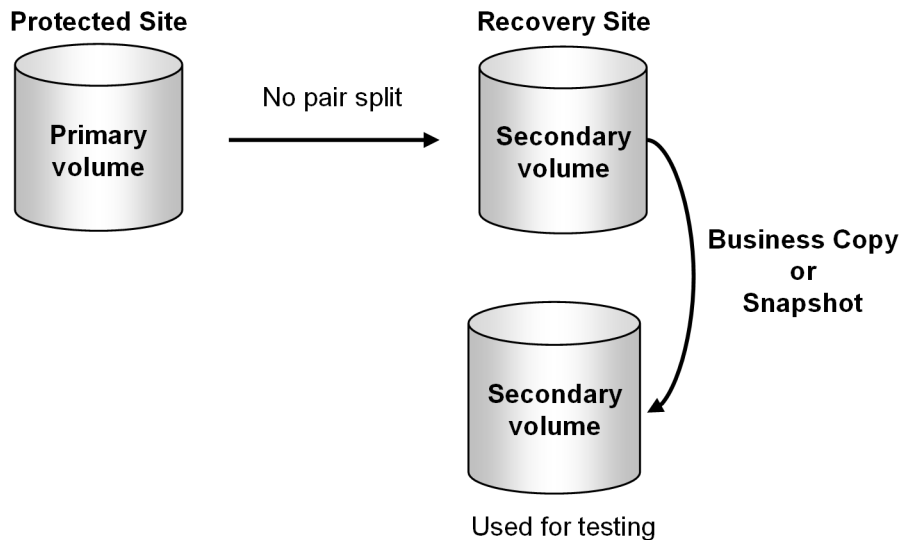
Business Copy, Fast Snap, and Snapshot are HPE in-system replication products for creating copies of the S-VOL on the remote site. These products are supported for the SRA/VMware® vCenter SRM™ solution on the XP8, XP7, P9500, and XP24000/XP20000 Disk Array storage systems.

Required configuration for testing with a copy of S-VOL

The in-system S-VOL must be assigned an MU#. By default, SRA looks for MU#0 to test with. When you use MU#0, then no further configuration is necessary for testing.

If you specify a different MU#, then you must set environment variables on the host to enable SRA to use it. For instructions, see [Configuring SRA for testing](#) on page 36.

The following figure shows an example of test failover using a Business Copy.



Business Copy port requirement

The Business Copy S-VOL must be presented on the same Fibre Channel or iSCSI port as the Business Copy P-VOL. Otherwise the UUID on the datastore changes. ESX/ESXi cannot attach the UUID to the shadow virtual machine for test failover unless the UUID matches.

Configurations with protected and recovery VMs on the same site

SRA/VMware® vCenter SRM™ supports a configuration in which both protected and recovery VMs are present on the local and remote sites, thus providing protection for each site. For more information, see [Configurations with both sites active](#) on page 71.

Consistency groups and VM failover groups

RAID Manager consistency groups are used to perform a single pair operation on a grouping of pairs with similar or the same kind of data. This ensures that all the pairs are managed in a consistent status. Consistency groups are defined in the HORCM definition files and are assigned when you create the pairs.

This is done before setting up your protection group. All virtual machines in a protection group store their files within the same datastore group, and all failover together.

Consistency groups must be aligned with the VM failover groups. This means that the LUNs associated with VMs that will be failed over as a group must be included in a single consistency group. Failure to do this can cause the recovery plan to fail.

Also, adding LUNs that are associated with different VMs or physical hosts to a consistency group not associated with those VMs or hosts can cause an outage on these additional VMs or hosts.

Consistency groups and same-time split operations

All P-VOLs in the same RAID Manager consistency group can be split at the same time. In addition, you can specify the time the split operation is to be performed on the consistency group. This RAID Manager operation is called At-Time Split. Data consistency is guaranteed across the consistency group when you perform the At-Time Split operation.

The At-Time Split can only be performed on the pairs in a RAID Manager consistency group.

HPE recommends assigning P-VOLs in a protected group to the same RAID Manager consistency group, and warns against placing a protected group's P-VOLs in multiple consistency groups.

See the Continuous Access Synchronous, Continuous Access Journal, or High Availability user guide for your storage system for information about using consistency groups and the At-Time Split operation.

About the Continuous Access Synchronous fence level “Never”

Using “Never” for the fence level for Continuous Access Synchronous pairs causes the internal horctakeover to fail; the command returns with EX_VOLCUR. This occurs because “Never” cannot completely guarantee data consistency.

However, the VMware® vCenter SRM™/VMware goal of Failover/ testFailover is booting the VMs. This makes the fence level “Never” acceptable despite the horctakeover return of EX_VOLCUR.

If you use “Never”, remember that the recovery will be on APP (SQL/ Exchange/Oracle/..).

Prerequisites for High Availability configuration

When you use High Availability (HA) for remote replication, each ESXi host must be connected to both primary and secondary volumes as shown in the figure. The connections are required because I/O to primary volumes might be momentarily blocked during planned migration, which results in failure of planned migration.

The connection must be managed by multipath software so that I/O from each ESXi host to the primary (or secondary) volumes can be transparently rerouted to the secondary (or primary) volumes in the case when the I/O to the primary (or secondary) volumes is blocked, as shown in [Figure 3: I/O rerouting by multipath software](#) on page 15.

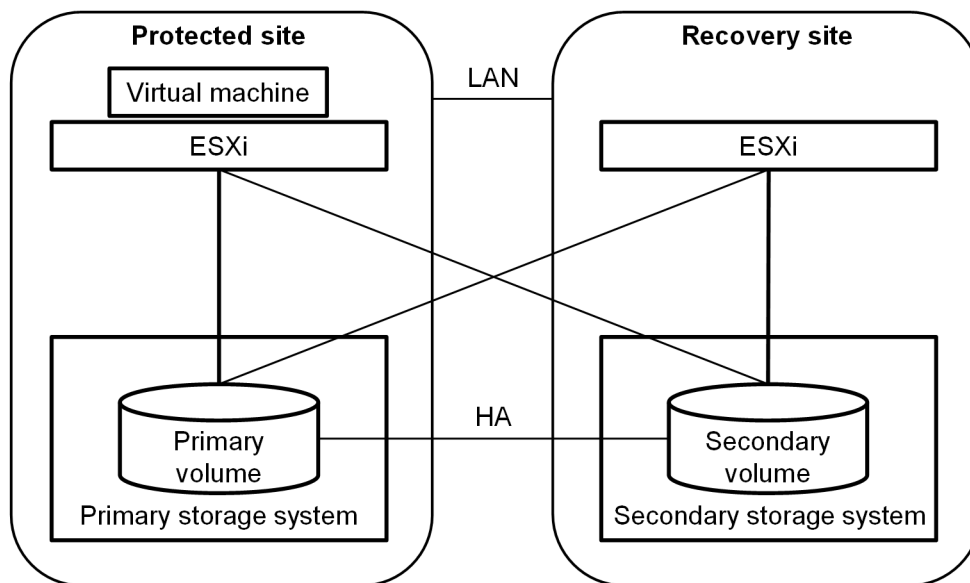


Figure 2: Connections when using HA

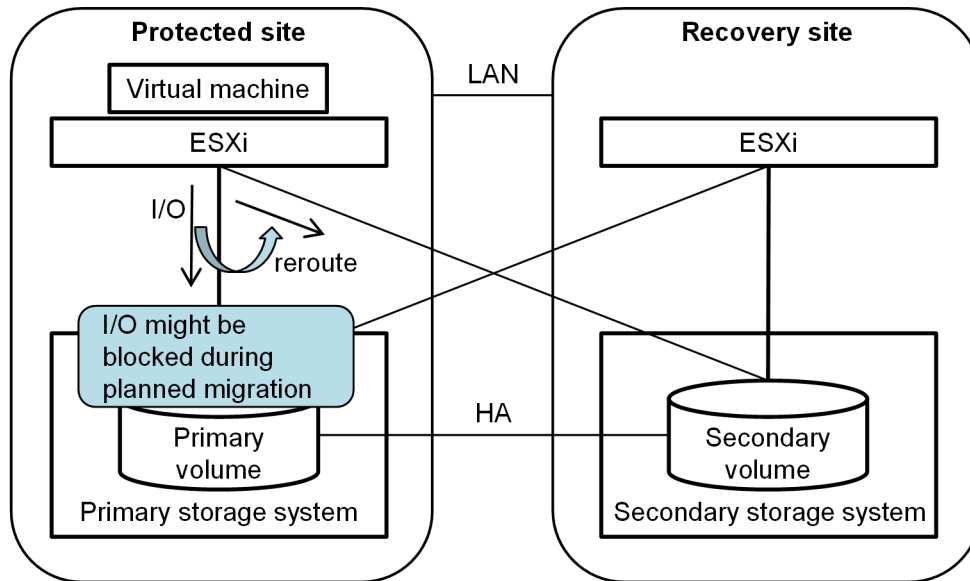


Figure 3: I/O rerouting by multipath software

Note the following when using HA:

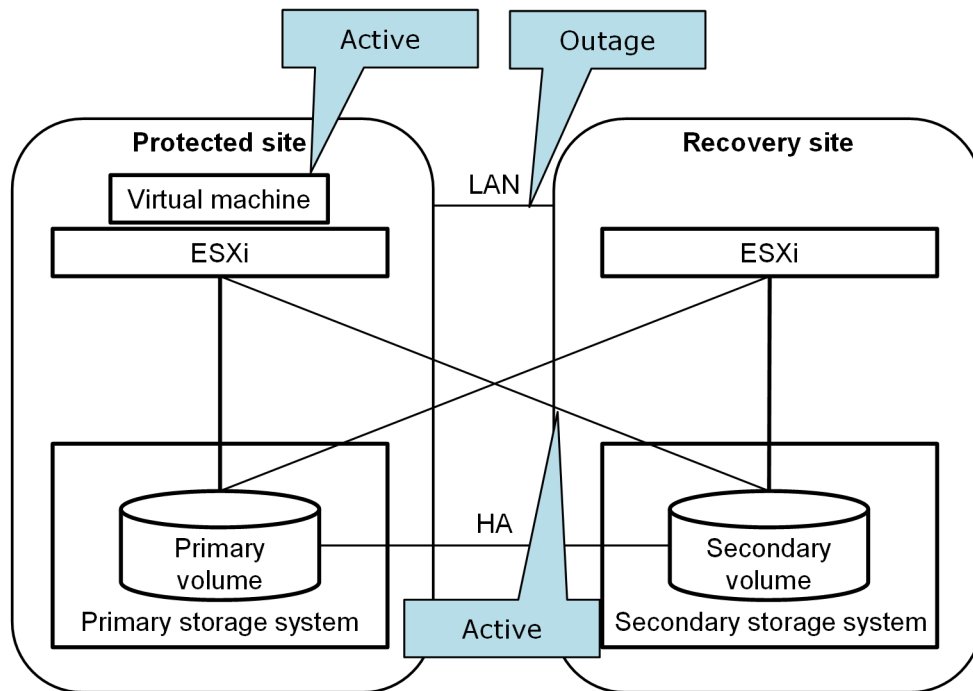
- Rerouting caused by I/O blockade on primary volumes shown in **Figure 3: I/O rerouting by multipath software** on page 15 might increase I/O latency. If you run latency-sensitive application software in virtual machines, it is recommended that you manually reroute I/O to secondary volumes before running planned migration.
- Latency of I/O from each ESXi in the protected site to the storage system in the recovery site can be larger than that of I/O from each ESXi in the protected site to the storage system in the protected site.

For example, the latency is generally larger when the recovery site is located far away from the protected site. If the latency is larger in your environment, reroute I/O back to the original volumes after planned migration has completed.

- Do not disconnect the connection by deleting LU.
- When all of the following conditions are satisfied, you cannot run planned migration nor disaster recovery:
 - The I/O mode of secondary volumes in the recovery site is “Block”.
 - The connections between each ESXi host in the recovery site and the storage system in the protected site are not active.
- If you run disaster recovery when all of the following conditions are satisfied, virtual machines might not be powered on in the recovery site after disaster recovery. In this case, shut down the virtual machines in the protected site or disconnect the connection between each ESXi in the protected site and the storage system in the recovery site, and then run disaster recovery.

Conditions:

1. The virtual machines in the protected site are active.
2. The LAN between the protected and recovery sites is in outage, vCenter in the protected site is in outage, or SRM in the protected site is in outage.
3. The connections between each ESXi in the protected site and the storage system in the recovery site are active.



Deployment

This chapter provides instructions for deploying HPE Storage Replication Adapter 2.0 and 2.5.

Supported SRM/SRA configurations

The deployment to use for each supported SRM/SRA configuration is unique.

The following table lists the supported SRM/SRA versions.

SRM Version	SRA Version	Supported configurations
SRM 8.1 (or earlier)	SRA 2.3.1 (or earlier)	Configurations 1 and 2
SRA 8.2	SRA 2.5	Configurations 1, 2, and 3

The following images illustrate the deployment examples for each configuration.

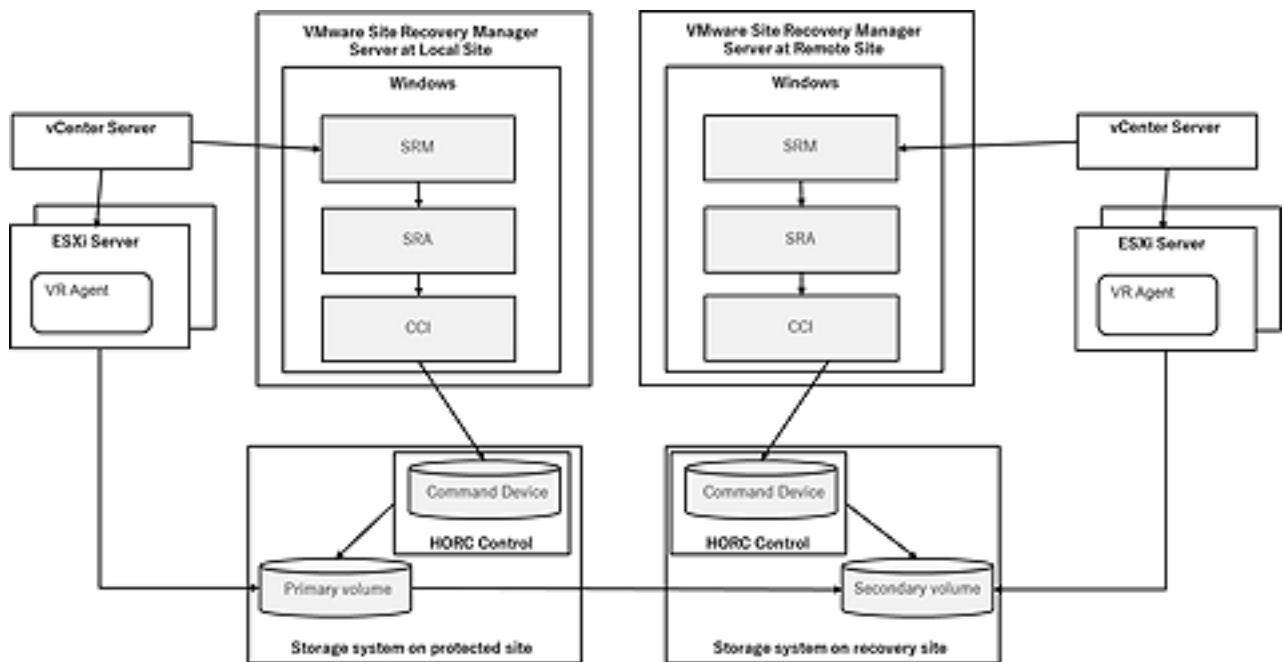


Figure 4: Configuration 1

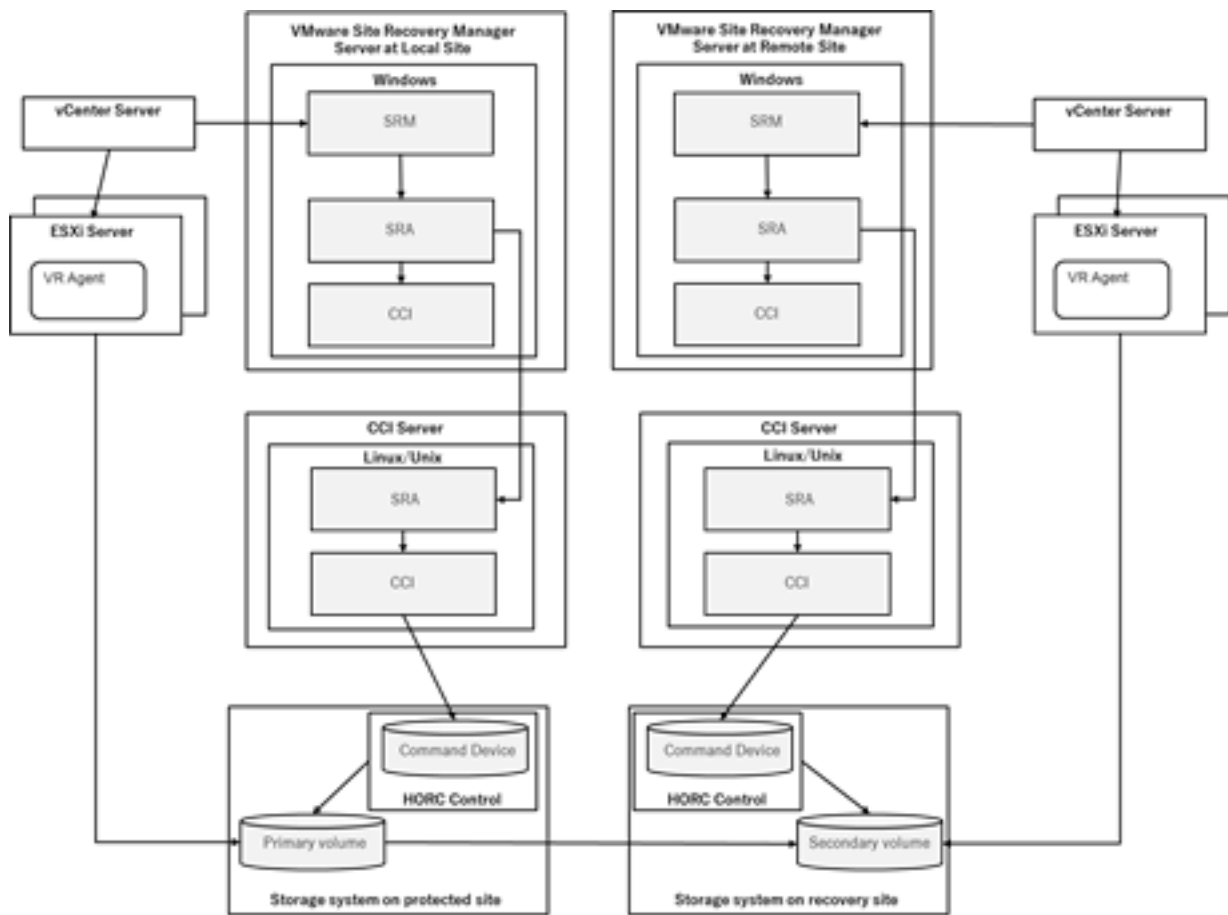


Figure 5: Configuration 2

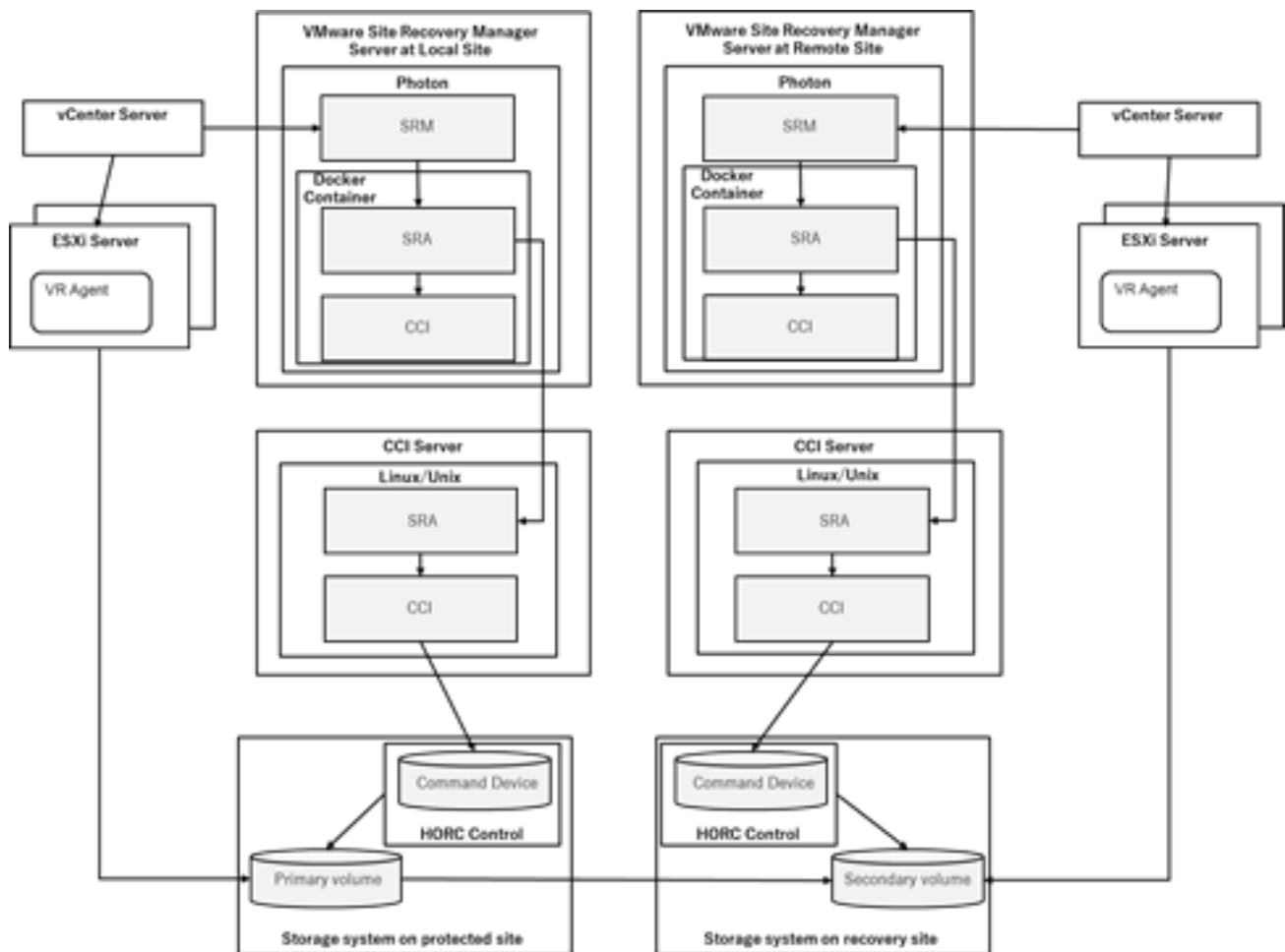


Figure 6: Configuration 3

Deployment workflow

The following workflow shows the basic order for setting up the SRA/ VMware® vCenter SRM™ solution. When a task is outside the scope of this document, a reference is provided to the appropriate documentation.

Table 2: Workflow for deploying

Task	How to
1. Review requirements and planning considerations.	See Requirements on page 9.
2. Configure the storage area network	-
3. Configure HPE remote replication using Remote Web Console. Includes storage, pair volume, port, logical path, and data path setup.	See the appropriate Continuous Access Synchronous, Continuous Access Journal, or High Availability user guide for instructions.

Table Continued

Task	How to
4. (Optional). Configure in-system replication for testing SRA/VMware® vCenter SRM™.	See the appropriate Business Copy or Fast Snap user guide for information.
5. Install RAID Manager to manage storage replication.	See Installing RAID Manager on page 20.
6. Create and map a command device.	See Creating and configuring a RAID Manager command device on page 21.
7. Set up RAID Manager HORCM files with pair and path information.	See Setting up HORCM configuration definition files on page 23.
8. Create pairs.	See Starting HORCM instances, creating pairs (Windows) on page 28.
9. Ensure VMware® vCenter SRM™ 2013 and VMware® vCenter SRM™ databases are installed.	See VMware vCenter Site Recovery Manager documentation.
10. Install SRA 2.x.	See SRA installation on page 38.
11. Connect protected and recovery sites.	See VMware vCenter Site Recovery Manager documentation.
12. Configure SRA in Site Recovery Manager.	See Configuring SRM™ to communicate with RMXPSRA20 (SRM 5.x or earlier) on page 42 or Configuring SRM to communicate with RMXPSRA20 (SRM 6.0 or later) on page 47 or Configuring SRM to communicate with RMXPSRA20 (SRM 8.2 or later) on page 55.
13. Set up inventory mappings, protection group, recovery plan, perform test recovery.	See VMware vCenter Site Recovery Manager documentation. Note: In an HA configuration, the protection groups are created with Storage Policy base.

Installing RAID Manager

RAID Manager is a collection of executable files that you use to manage replication and data protection operations. You run RAID Manager commands from a command line or use scripts consisting of a series of commands that automate several related processes.

- SRA 2.0 and SRA 2.1 require RAID Manager version 01.24.13 or later.
- SRA 2.2 and SRA 2.3.1 require RAID Manager version 01.36.03 or later.
- SRA 2.5 requires RAID Manager version 01.46.02 or later.

For installation and upgrade instructions, see the *HPE XP Storage RAID Manager Installation and Configuration User Guide*.

If RAID Manager is installed on the VMware® vCenter SRM™ host, HPE recommends that you run HORCM as a service. (HORCM is described in [Setting up HORCM configuration definition files](#) on page 23.)

Creating and configuring a RAID Manager command device

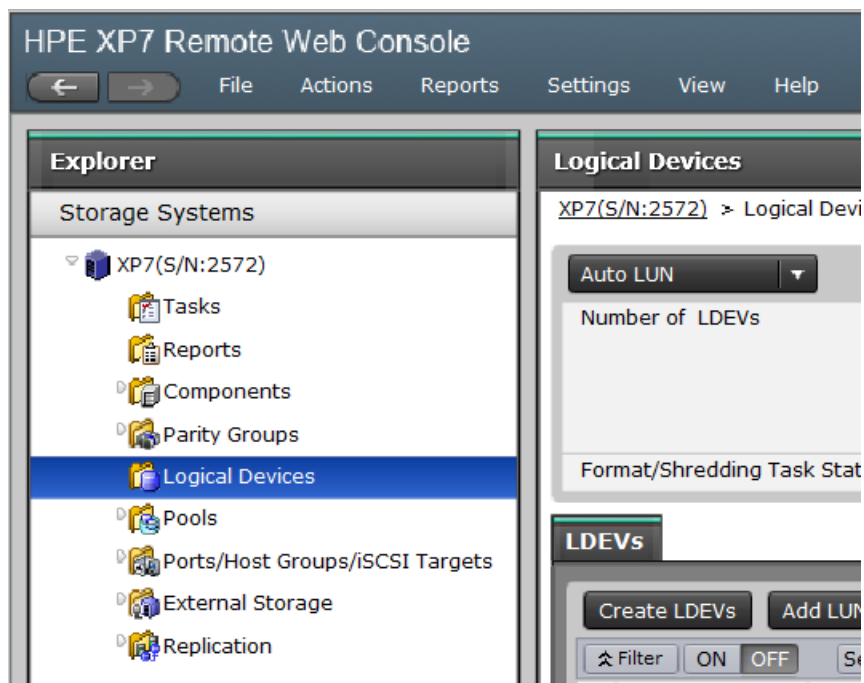
A RAID Manager command device (CMD) is a dedicated logical device on the storage system used by RAID Manager for communications between the host and the storage system. The CMD enables the RAID Manager software to send commands using in-band protocol to the storage system. One CMD per storage system is required.

Do not use the CMD to store user data. Define and configure the CMD as a raw device with no file system and no mount operation.

In the following procedure, you will create an LDEV, assign it as the CMD in the storage system, map it to a physical server or Windows virtual machine on the ESXi host—where VMware® vCenter SRM™ and RAID Manager are installed, and configure it.

Procedure

1. In the Remote Web Console **Explorer** pane, click **Storage Systems**, expand the target storage system, and then click **Logical Devices**.

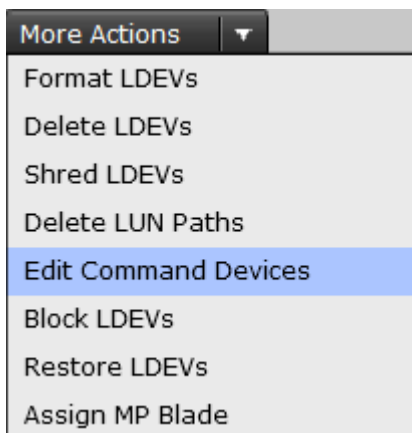


2. On the **LDEVs** tab-lower right, click **Create LDEVs** to create a new volume to be used as a command device.

The screenshot shows the 'LDEVs' tab in a management console. At the top, there are buttons for 'Create LDEVs', 'Add LUN Paths', 'Edit LDEVs', and 'More Actions'. Below these are filters for 'Filter' (ON/OFF), 'Select All Pages', and 'Column Settings'. The main table lists LDEVs with columns for selection, LDEV ID, LDEV Name, Status, Capacity, and Number of Paths.

	LDEV ID	LDEV Name	Status	Capacity	Number of Paths
<input type="checkbox"/>	1 ▲				
<input type="checkbox"/>	00:00:00	GADTEST	Normal	10.00 GB	
<input type="checkbox"/>	00:00:01		Normal	20.00 GB	
<input type="checkbox"/>	00:00:02		Normal	1.00 GB	

- Proceed through the **Create LDEVs** wizard, keeping the following in mind:
 - The CMD LDEV can be from a regular parity group or a THP pool.
 - The CMD LDEV can be small, but with a minimum of 47MB.
- On the **LDEVs** tab, select the newly created LDEV, then click **More Actions > Edit Command Devices**.



- In the **Edit Command Devices** wizard, select **Enable** for **Command Device**. Leave the Command Device Attributes disabled.

The screenshot shows the 'Edit Command Devices' wizard. The title bar says 'Edit Command Devices'. The progress bar shows '1.Edit Command Devices' and '2.Confirm'. The main text says: 'This wizard lets you edit one or more properties. Select the new value and click Finish to confirm.'

Command Device : ☒ Enable ☐ Disable

Command Device Attributes :

Command Device Security : ☐ Enable ☒ Disable

User Authentication : ☐ Enable ☒ Disable

Device Group Definition : ☐ Enable ☒ Disable

At the bottom, there are buttons: Back, Next, Finish, Cancel, and a help icon.

6. Click **Finish**.
7. Now map the CMD volume to the RAID Manager server (virtual or physical). If the RAID Manager server is a virtual server, map the CMD to the ESX/ESXi host where the VM resides.
8. From the VMware vSphere client, add the CMD LDEV to the VMware® vCenter SRM™ virtual machine as a physical RDM virtual disk.
9. Configure the command device in the guest operating system as follows:
 - a. In Microsoft Windows 2008, from the Server Manager menu, point to Storage and click **Disk Management**.
 - b. Right-click the RDM disk and click **Online**.
 - c. Right-click the RDM disk and click **Initialize Disk**.
 - d. Click **MBR** (Master Boot Record) as the partition style.
10. Present a CMD volume from the primary storage system to the primary ESX/ESXi server, and another CMD volume from the secondary storage system to the recovery ESX/ESXi server.

Setting up HORCM configuration definition files

You will need two HORCM configuration definition files to define the pair relationship: one file describes the primary volumes (P-VOLs), and the other file describes the secondary volumes (S-VOLs). A third HORCM configuration definition file is required if you use a Business Copy, Fast Snap, or Snapshot copy of the remote site S-VOL for testing.

Figure 1: VMware vCenter SRM and HPE components on page 6 provides a configuration example that shows the HORCM configuration definition files on the local and remote servers.

Editing HORCM.conf files

HORCM configuration definition files are used to identify the target volumes of a RAID Manager command.

Note the following when editing HORCM.conf files:

- Save a copy of the HORCM.conf files on the local and remote RAID Manager servers in the C:\Windows folder or /etc folder, according to the RAID Manager server's OS.
- HORCM files must be named **horcm#.conf**, where “#” represents the HORCM instance.
 - The instance on the primary site is usually **0**. In this case, the HORCM file on the primary site would be named, **horcm0.conf**.
 - The # of the secondary instance must be the primary instance number plus 1. Thus, if the primary instance is 0, the HORCM file on the secondary site would be named, **horcm1.conf**.

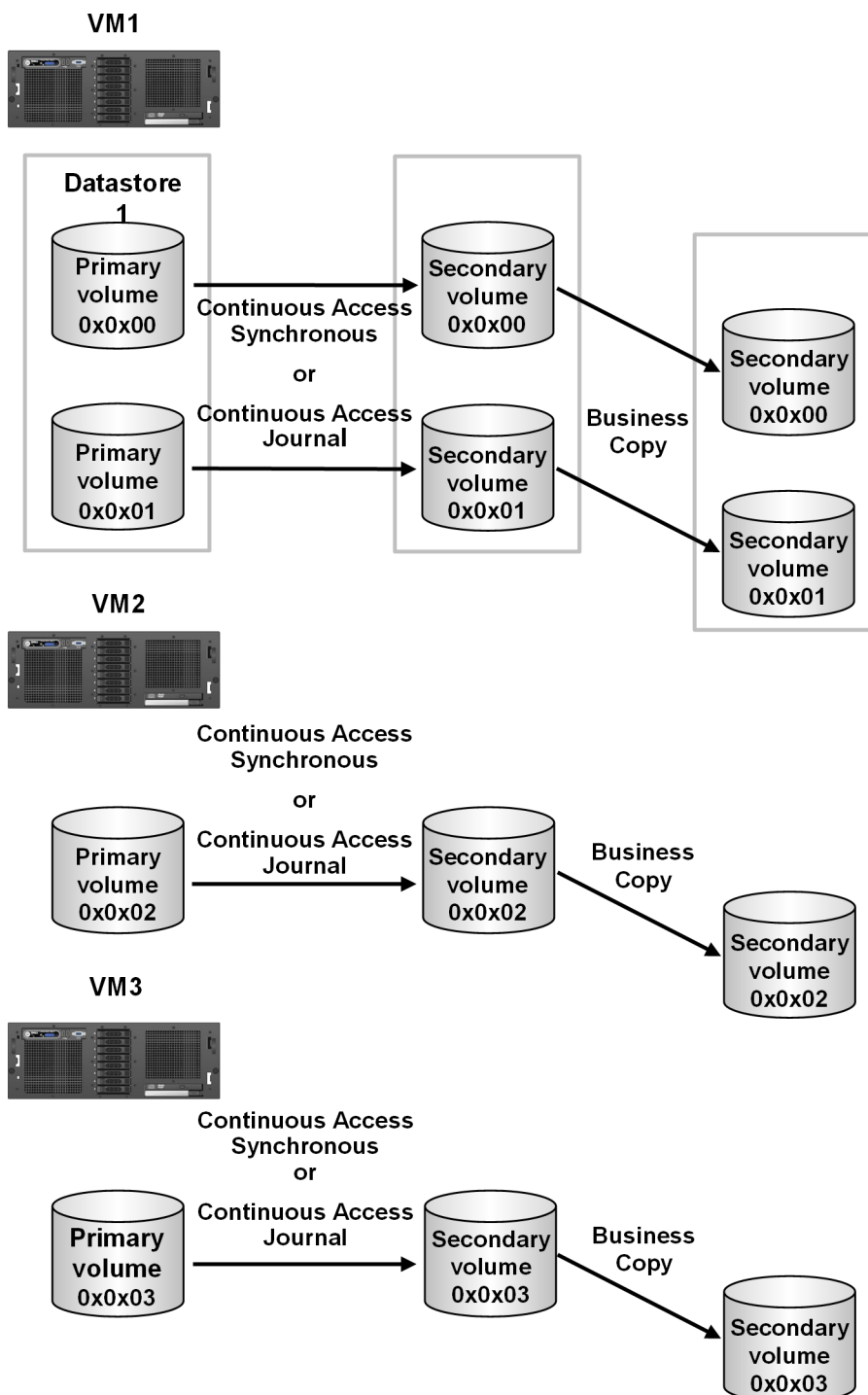
- Likewise, the # of Business Copy, Fast Snap, or Snapshot S-VOL instance must be the secondary instance number plus 1. Thus, if the secondary instance is 1, the HORCM file for the in-system S-VOL would be named **horcm2.conf**.
- It is best practice to name devices the same as the datastore contained in the LU. The following figure shows example device naming schemes.
- HORCM_LDEVG with SRM and the HPE SRA 2.1.4 and later is supported. The HORCM_LDEVG parameter defines the device group information that the RAID Manager instance reads. The following values are defined: Copy_Group, ldev_group, Serial#. For example:

```

HORCM_LDEVG
#Copy_Group    ldev_group    Serial#
ora            grp1         64034

```

For details, see the *HPE XP Storage RAID Manager User Guide*.



HORCM examples are provided in the following sections for the primary site, secondary site, and an optional secondary-site test pair.

Primary HORCM file

Example HORCM0.conf for primary site remote replication pair on page 26 shows an example of the HORCM file for the primary storage system.

Example HORCM0.conf for primary site remote replication pair

```
HORCM_MON
#ip_address      service      poll(10ms)      timeout(10ms)
172.17.46.38     horcm0             1000            3000

HORCM_CMD
#dev_name
\\.\CMD-64015

HORCM_LDEV
#dev_group      dev_name      Serial#      CU:LDEV(LDEV#)      MU#
CA_CAJ_SRM1     01A_01B        64015        00:1A

HORCM_INST
#dev_group      ip_address      service
CA_CAJ_SRM1     172.17.46.39   horcm1
```

The configuration files consist of the following sections:

- **HORCM_MON** — Information for monitoring the HORCM instance. Includes the IP address of the primary server, HORCM instance or service, polling interval for monitoring paired volumes, and timeout period for communication with the remote server.
- **HORCM_CMD** — Command device from the protected storage system. Replace the number with the serial number of the primary storage system.
- **HORCM_LDEV** — Consists of the following:
 - **#dev_group** is the group name for the pairs, which allows you to run a pair operation against the pairs in the group.
 - **dev_name** is the pair name (example uses P-VOL_S-VOL).
 - **Serial#** is the storage system's serial number.
 - **CU:LDEV(LDEV#)** is the LDEV ID of the P-VOL.
 - **MU#** is the mirror unit number. Use MU#0-2 for Business Copy, Fast Snap, and Snapshot. You do not need to specify MU# for Cnt Ac-S, Cnt Ac-J, and HA. If you want to specify MU# for Cnt Ac-S, Cnt Ac-J, and HA, use MU#h0 for Cnt Ac-S and MU#h0-h3 for Cnt Ac-J and HA.
- **HORCM_INST** — Consists of the following:
 - **#dev_group** is the group name for the pairs.
 - **ip address** is the network address of the remote server.
 - **service** is the remote HORCM instance.

Secondary HORCM file

Example HORCM1.conf for secondary site remote replication pair with in-system test pair on page 27 shows an example of the HORCM file for the secondary storage system.

Example HORCM1.conf for secondary site remote replication pair with in-system test pair

```
HORCM_MON
#ip_address      service      poll(10ms)      timeout(10ms)
172.17.46.39     horcm1      1000            3000

HORCM_CMD
#dev_name
\\.\CMD-64016

HORCM_LDEV
#dev_group      dev_name      Serial#      CU:LDEV(LDEV#)      MU#
CA_CAJ_SRM1     01A_01B      64016        00:1B
BC_SRM1         01B_01C      64016        00:1B                0

HORCM_INST
#dev_group      ip_address      service
CA_CAJ_SRM1     172.17.46.38   horcm0
BC_SRM1         172.17.46.39   horcm2
```

- **HORCM_MON** shows the IP address of the secondary server, HORCM instance or service, polling interval for monitoring paired volumes, and timeout period for communication with the remote server.
- **HORCM_CMD** shows the command device on the remote site. Note that the instance or service is increased from the primary instance by 1. Use the recovery storage system's serial number.
- **HORCM_LDEV** shows the same group and device name for the pair as used in the primary site HORCM file. The second entry in this section is a group for the Business Copy pair used for testing. The remote pair's S-VOL is the in-system pair's P-VOL. When using Business Copy for the in-system pair, make sure that the MU number is set for the P-VOL.
- **HORCM_INST** shows the pair's group name, and the IP address and service number of the primary host. The second entry for the in-system pair shows the secondary host IP address.

Notes:

- The Cnt Ac-S or Cnt Ac-J group must be defined before the BC group.
- The MU# (h0-h3) for Cnt Ac-J and HA devices must be specified.
- The MU# for Business Copy devices must be specified. If MU#1 or MU#2 are used, the environment variable RMSRATMU must be set. See **Configuring SRA for testing** on page 36 for instructions.

In-system test copy HORCM file

Example HORCM2.conf for secondary site in-system test pair on page 27 shows an example of the HORCM file for the test copy of the S-VOL. If you will not use a copy for testing, then you do not need to make an in-system copy HORCM file. For more information, see **Using a copy of the S-VOL for testing** on page 12.)

Example HORCM2.conf for secondary site in-system test pair

```
HORCM_MON
#ip_address      service      poll(10ms)      timeout(10ms)
172.17.46.39     horcm2      1000            3000

HORCM_CMD
#dev_name
\\.\CMD-64016
```

HORCM_LDEV				
#dev_group	dev_name	Serial#	CU:LDEV (LDEV#)	MU#
BC_SRM1	01B_01C	64016	00:1C	

HORCM_INST		
#dev_group	ip_address	service
BC_SRM1	172.17.46.39	horcm1

- **HORCM_MON** requires the IP address of the secondary server. The service is increased from the secondary HORCM instance by 1.
- **HORCM_CMD** requires the command device on the remote site. Use the recovery storage system's serial number.
- **HORCM_LDEV** requires the device group, device name, and serial number for the in-system pair, and must match the values in horcm1.conf for this pair. The LDEV ID is the only value that is changed from horcm1, and is the second volume mapped to the remote server. This is the in-system pair S-VOL, requiring no MU#.)
- **HORCM_INST** shows the IP address and service number of the secondary host. The service number must match the service number in the horcm1 HORCM_MON.

Starting HORCM instances, creating pairs

When the necessary HORCM files are edited and saved on the local and remote servers, start the HORCM instance on both servers and create the pair or pairs.

Use the following procedure to start HORCM instances and creating pairs for Windows or UNIX version of RAID Manager.

For additional information about RAID Manager commands and expected output, see the *HPE XP Storage RAID Manager Reference Guide*.

NOTE: If the Windows version of RAID Manager is used, RAID Manager is installed on the SRM server. If the UNIX version of RAID Manager is used, RAID Manager is installed on a location other than the SRM server.

Starting HORCM instances, creating pairs (Windows)

Procedure

1. On the primary and secondary vCenter servers, open a command prompt and enter the following:

```
cd c:\HORCM\etc
```

```
horcmstart.exe *
```

Substitute the HORCM instance number for the asterisk (*), for example, 0.

2. Verify the status of the pair volumes and systems. Initially, the volumes are in simplex (SMPL) status. Run the pairdisplay command on the primary server.

```
pairdisplay.exe -g <grp> -ICA<HORCM instance #> -fcx
```

3. On the primary server, create the Continuous Access Synchronous (Cnt Ac-S), Continuous Access Journal (Cnt Ac-J), or HA pair using the paircreate command:
 - For Cnt Ac-S, use: **paircreate.exe -g <grp> -vl -fg <fence> <CTGID> -ICA<HORCM instance #>**
 - For Cnt Ac-J, use: **paircreate.exe -g <grp> -vl -f async -jp <journal id> -js <journal id> -ICA<HORCM instance #>**
 - For HA, use: **paircreate.exe -g <grp> -vl -fg never -jq <quorum id> -ICA<HORCM instance #>**
4. Use the `pairdisplay` command to check pair status. When status is PAIR, the data on the primary site is copied to the recovery site. If the P-VOL contains a large amount of data, completion may take longer than expected (the `pairdisplay` command shows the copy percentage).
5. Shut down the HORCM instance on both sites. VMware® vCenter SRM™ will start the instances again, but HORCM processes must be stopped for this. For example:
 - On the primary server, run **horcmshutdown.exe 0**.
 - On the recovery server, run **horcmshutdown.exe 1**.

Starting HORCM instances, creating pairs (UNIX)

Procedure

1. On the primary and secondary UNIX hosts, open a command prompt and enter the following:


```
cd /HORCM/usr/bin
horcmstart.sh *
```

 Substitute the HORCM instance number for the asterisk (*), for example, 0.
2. Verify the status of the pair volumes and systems. Initially, the volumes are in simplex (SMPL) status. Run the `pairdisplay` command on the primary UNIX host.


```
pairdisplay -g <grp> -ICA<HORCM instance #> -fcx
```
3. On the primary UNIX host, create the Continuous Access Synchronous (Cnt Ac-S), Continuous Access Journal (Cnt Ac-J), or HA pair using the paircreate command:
 - For Cnt Ac-S, use: **paircreate -g <grp> -vl -fg <fence> <CTGID> -ICA<HORCM instance#>**
 - For Cnt Ac-J, use: **paircreate -g <grp> -vl -f async -jp <journal id> -js <journal id> -ICA<HORCM instance #>**
 - For HA, use: **paircreate -g <grp> -vl -fg never -jq <quorum id> -ICA<HORCM instance #>**
4. Use the `pairdisplay` command to check pair status. When status is PAIR, the data on the primary site is copied to the recovery site. If the P-VOL contains a large amount of data, completion may take longer than expected (the `pairdisplay` command shows the copy percentage).

NOTE: The HORCM instances of RAID Manager are installed on the primary and secondary UNIX hosts must be running.

Creating a copy for testing on the recovery site

If you are using a copy of the remote replication S-VOL for testing, use the following procedure to start the HORCM instance and create the pair.

If you are not using a copy for testing, skip this section.

Creating a copy for testing on the recovery site (Windows)

Prerequisites

- For Business Copy, assign the pair to a consistency group by using the **-m grp** option.
- For Split mode, you must set to **quick** by using the command option **-fq quick**.
- For Business Copy, S-VOLs and P-VOLs must be mapped on the same Fibre Channel or iSCSI port.

Procedure

1. On the remote site vCenter server, open a command prompt and enter the following to start the in-system HORCM instance:

```
cd c:\HORCM\etc
```

```
horcmstart.exe *
```

Substitute the HORCM instance number for the asterisk (*). For example, 2.

2. Verify the status of the pair volume and system by using the pairdisplay command.

```
pairdisplay.exe -g <grp> -IBC<HORCM instance #> -fcx
```

Initially, the volumes are in simplex (SMPL) status.

3. Create the pair by using the following:

```
paircreate -g <grp> -vl -m grp -fq quick
```

- **-m grp** creates a consistency group for all LUNs in the pair group.
 - **-fq quick** allows for Business Copy quick split.
 - For Fast Snap or Snapshot, do not use the **-fq quick** option.
4. Use the `pairdisplay` command to check the in-system pair's status. When status is PAIR, the data in the P-VOL (remote S-VOL) is copied to the in-system S-VOL.
 5. Shut down the HORCM instance. VMware® vCenter SRM™ will start the instance at a later time, but HORCM processes must be stopped for this. Run **horcmshutdown.exe 1 2**.

Creating a copy for testing on the recovery site (UNIX)

Prerequisites

- For Business Copy, assign the pair to a consistency group by using the **-m grp** option.
- For Split mode, you must set to **quick** by using the command option **-fq quick**.
- For Business Copy, S-VOLs and P-VOLs must be mapped on the same Fibre Channel or iSCSI port.

Procedure

1. On the remote site vCenter server, open a command prompt and enter the following to start the in-system HORCM instance:

```
cd /HORCM/usr/bin
```

```
horcmstart.sh *
```

Substitute the HORCM instance number for the asterisk (*). For example, 2.

2. Verify the status of the pair volume and system by using the `pairedisplay` command.

```
pairedisplay -g <grp> -IBC<HORCM instance #> -fcx
```

Initially, the volumes are in simplex (SMPL) status.

3. Create the pair by using the following:

```
paircreate -g <grp> -vl -m grp -fq quick
```

- **-m grp** creates a consistency group for all LUNs in the pair group.
- **-fq quick** allows for Business Copy quick split.
- For Fast Snap or Snapshot, do not use the **-fq quick** option.

4. Use the `pairedisplay` command to check the in-system pair's status. When status is PAIR, the data in the P-VOL (remote S-VOL) is copied to the in-system S-VOL.

NOTE: The HORCM instances of RAID Manager are installed on the primary and secondary UNIX hosts must be running.

Setting environment variables

RMXPSRA20 requires that the following system environment variables be defined in order to make certain parameters available. The following table lists the environment variables that are required for each configuration. Command line examples are included.

To define the variables using the GUI, see [Defining environment variables using the GUI](#).

Configuration 3 uses the environmental setting file. For information, see [Defining environment variables using the environmental setting file](#).

Table 3: Environment Variables

Variable	Description	Command line example	Configuration
HORCMROOT	Used to specify the installed HORCM directory if RAID Manager is on Windows. If RAID Manager is not used on either the local or remote system, the C: drive is used. If RAID Manager is used on UNIX, HORCMROOT is not required.	To set the directory to the E: drive: C:\>setx HORCMROOT E: /m	1
RMSRATOV	Used to specify the timeout value for failover using Universal Replicator. If not specified on either the local or remote system, 60 seconds is the default.	Configuration 1 and 2: To the set timeout value to 30 seconds: C:\>setx RMSRATOV 30 /m Configuration 3: Cannot set the RMSRAFNGPTCHK by using the command line. See <u>Defining environment variables using the environmental setting file.</u>	1, 2, and 3
RMSRATMU	Used to specify the MU# of the in-system replication volume for testFailover. If not specified, then MU#0 is the default and this variable is not specified on the remote.	Configuration 1 and 2: To specify MU#1 C:\>setx RMSRATMU 1 /m Configuration 3: Cannot set the RMSRAFNGPTCHK by command line. See <u>Defining environment variables using the environmental setting file.</u>	1, 2, and 3

Table Continued

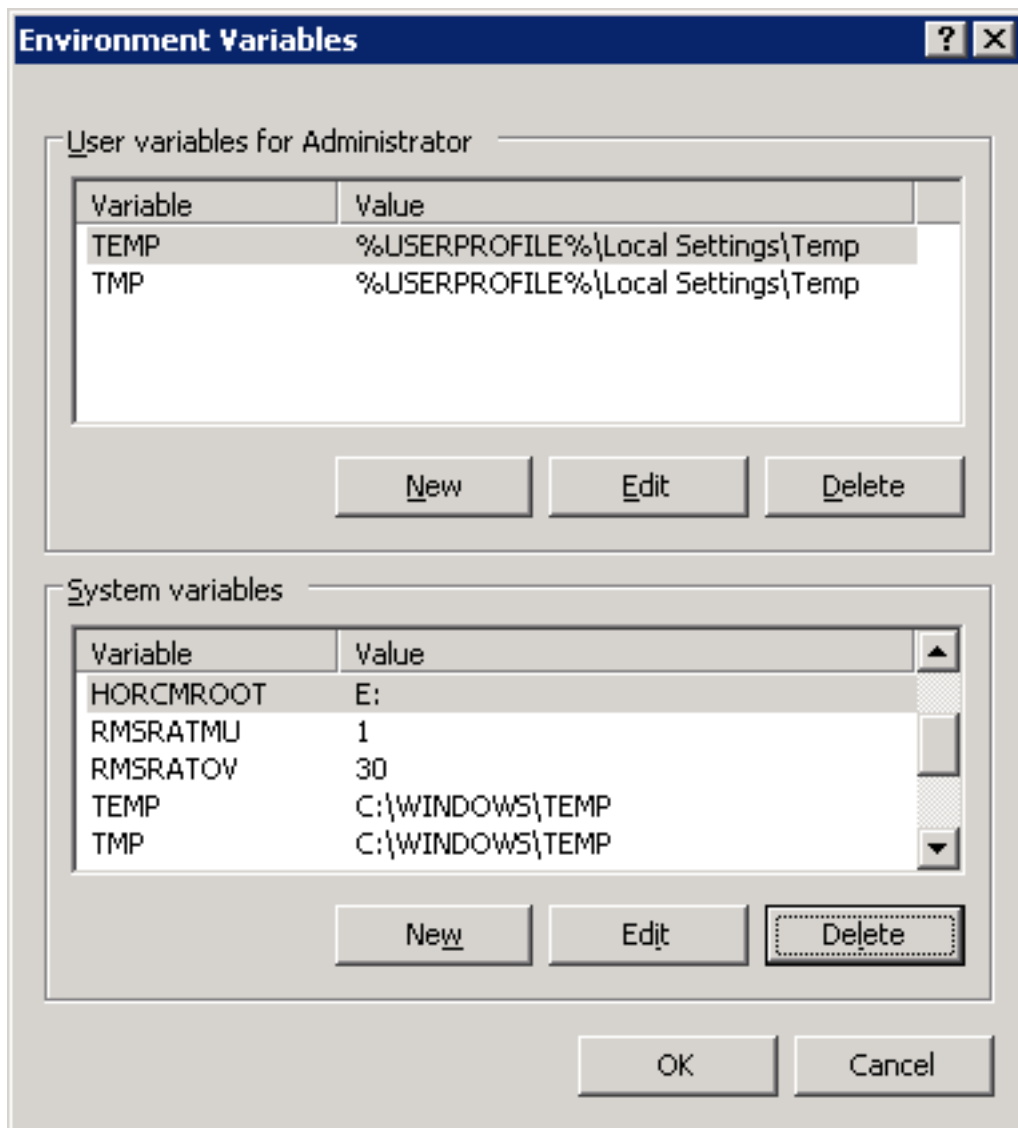
Variable	Description	Command line example	Configuration
RMSRA_MULT_CAP	Used to report support for SRM "Multiple Array".	C:\>setx RMSRA_MULT_CAP 1 /m Note: This is set on a RAID Manager Server not on WindosOS or Photon™ OS.	1, 2, and 3
RMSRA_USE_SSH	Used to specify an SSH connection instead of Telnet.	C:\>setx RMSRA_USE_SSH 1 /m	2
RMSRAFNGPTCHK	Used to specify whither to check the FingerPrint of RAID Manager servers or not. "yes" is the default that means to check the FingerPrint. "no" means not to check the FingerPrint. If not specified, then set to check the FingerPrint of RAID Manager servers.	Cannot set the RMSRAFNGPTCHK by command line. See <u>Defining environment variables using the environmental setting file.</u>	3

Defining environment variables using the GUI

Define the variables using the GUI as follows.

Procedure

1. In Windows Control Panel, open **System Properties**.
2. On the **Advanced** tab, select **Environment Variables**.
3. In the **Environment Variables** dialog, **System Variables** box, click **New** to add the desired variables.



4. Reboot Windows.

Defining environment variables using the environmental setting file

Environment variables should be defined after installing HPE Storage Replication Adapter (SRA) version 2.5.

Procedure

1. Use SSH to log in to SRM (Photon™ OS). The password to use for the login is the admin password which was set at the time SRM was installed:

User: admin (Initial admin user)

Password: (Initial admin user password)

2. Move to root user: `admin@photon []$ su`

The password to use for the login is the root password which was set at the time SRM was installed.

Password: Initial root user password

3. Deploy "env.conf":

```
root@photon [ ]$cd /var/lib/docker/volumes/"[Docker Image ID]"-v/_data/
root@photon [ ]$vi env.conf
```

Set the environment variables in the format of "environment variable name"="environment variable value". If "env.conf" does not exist or the environment variables are not set, the default value is set as described in the following table.

Environment variable name	Default	Description
RMSRATOV	60	The timeout value 60[s] is set.
RMSRATMU	0	The MU number 0[number] is set.
RMSRAFNGPTCHK	yes	If "no" is set, SRA does not check the FingerPrint of RAID Manager Server at SSH connection (not recommended).

4. Save the env.conf file.

5. Change the env.conf file:

```
root@photon [ ]$chmod a+r env.conf
```

About SSH

SRM/SRA Configuration 1 and 2

If your site has implemented the SRM/SRA configuration 1 or 2,

The environment variable for SSH secure protocol must be defined for SRM/ SRA because the SSH library and command are not provided by Windows Server 2008/2012.

The variable **RMSRA_USE_SSH** is used to specify an SSH connection. For example: C:\>setx RMSRA_USE_SSH 1 /m

Install PuTTY (version 0.62 or later, 32-bit) using \Program Files (x86)\PuTTY\plink.exe or by downloading it from <http://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>.

You can register using the fingerprint for executing the SSH command with the remote host, or by executing the following command one time for authentication: SRA install drive: \Program Files (x86)\PuTTY\plink.exe -ssh -l root -pw PASS HOST ls

where:

- PASS: password
- HOST: hostname for HORCM server

SRM/SRA Configuration 3

If your site has implemented the SRM/SRA configuration 3, deploy the FingerPrint information of RAID Manager servers in the specified directory for SSH connection:

```
/var/lib/docker/volumes/"[Docker Image ID]"-v/_data/known_hosts
```

The Docker Image ID is assigned to each SRA. Refer to the following table and confirm the Docker Image ID corresponding to SRA.

SRA version	Docker Image ID
02.05.00	0f9d59dbe59e8c9ecd6c21664a88eb1a191de059fc47c88c76cb88de2027fabd

NOTE: The format of FingerPrint information (known_hosts) should follow the format of **OpenSSH_7.4p1**. The 'known_hosts' must be readable.

Example deployment of known_hosts:

1. Use SSH to log in to SRM (Photon™ OS).

2. Move to root user.

3. Run the Docker container:

```
root@photon [ ]$docker run -i -d --name get_fngpnt self/sra:RMCMD
```

4. Log in to the Docker container:

```
root@photon [ ]$docker exec -it get_fngpnt bash
```

5. Get information from **known_hosts**:

```
root@photon [ ]$ssh-keyscan -t rsa [IP Address of RAID Manager Server] >
known_hosts_file
```

6. Copy the contents of known_hosts_file into the local tmp file of your PC.

7. Press Ctrl+D to log out of the Docker Container.

8. Delete the Docker container:

```
root@photon [ ]$docker stop get_fngpnt
```

```
root@photon [ ]$docker rm get_fngpnt
```

9. Confirm whether the get_fngpnt of the Docker container exists:

```
root@photon [ ]$docker ps -a
```

10. Deploy **known_hosts**:

```
root@photon [ ]$cd /var/lib/docker/volumes/"[Docker Image ID]"-v/_data/
```

```
root@photon [ ]$vi known_hosts
```

11. Copy the content of **known_hosts_file** into **known_hosts**, then save the file.

12. Change the mode of **known_hosts**:

```
root@photon [ ]$chmod a+r known_hosts
```

Configuring SRA for testing

Business Copy (BC), Fast Snap (FS), and Snapshot are supported on the respective HPE Storage platform for this use case.

- SRA automatically searches MU#0 to test with. If you have created the BC, FS, or Snapshot pair and set the S-VOL at MU#0, no further configuration is necessary.
- If you test using the remote replication pair, the pair must be split first. This requires the following environment variables on the host to be set:

- **SplitReplication=true** (gives permission to use Cnt Ac-S/Cnt Ac-J S-VOL)

Note: SplitReplication=true is not supported for HA pairs.

- **RMSRATMU=MUX**, where x is an unused MU number other than 0.

With these variables set, SRA would search for the BC, FS, or Snapshot S-VOL at MU#0, fail, and then continue the operation using the Cnt Ac-S or Cnt Ac-J S-VOL.

The RAID Manager location determines where you set the environment variable when you have an MU# other than 0:

- If RAID Manager is installed on the VMware® vCenter SRM™ host, then you set the environment variables on the VMware® vCenter SRM™ host.
- If RAID Manager is installed on a UNIX host, then you set the environment variables on the UNIX host.

Setting environment variables on the VMware® vCenter SRM™ host

Procedure

1. On the VMware® vCenter SRM™ host, issue the following command to set the **SplitReplication** parameter to true:
setx SplitReplication true /m
2. Issue the following command to set the RMSRATMU parameter to 1:
setx RMSRATMU 1 /m
3. Reboot the VMware® vCenter SRM™ host.
4. Verify that the variables are set correctly using the **Set** command.
5. Optional: If RAID Manager is installed on another drive (e.g. E:), then use the HORCMROOTD variable:
setx HORCMROOT E: /m
6. Optional: The default timeout value for failover using Cnt Ac-J/Async is 60sec. This can be changed using RMSRATOV variable:
setx RMSRATOV 120 /m

Setting environment variables on a UNIX Host

Use the root user profile to set these variables; that is, **/root/.bash_profile** for Linux or **/.profile** for HP-UX. Use the appropriate root user profile for your default shell. Insert the following lines in this file.

- **SplitReplication=true**
- **export SplitReplication**
- **RMSRATMU=1**
- **export RMSRATMU**

Log out and back in and use the **env** command to verify that these variables are set correctly.

Configuration is now complete. When testFailover is executed on virtual machine 1, the Continuous Access Synchronous pairs are suspended and utilized for testing. When testFailover is done on virtual machine 2, the Business Copy pairs at MU#1 are suspended and used for testing.

SRA installation

This section discusses both options.

- If you are installing a new version of SRA 2.x, continue to **Installing HPE SRA 2.x** on page 38.
- If you are upgrading an existing version of SRA 2.x, you must remove it before continuing. See **To remove an earlier version of SRA (Configuration 1, 2)** on page 39 for instructions.
- To check your SRA version, see **Checking the SRA version** on page 40.

Installing HPE SRA 2.x

Read the following conditions before performing the installation.

- Site Recovery Manager 2013 must be installed on both protected and recovery sites.
- Download one of the following versions of SRA 2.x from the VMware website:
 - For VMware® vCenter SRM™ 5.x/6.0, download RMXPSRA_X64.exe.
 - For VMware® vCenter SRM™ 6.1, 6.5 or 8.1, download HPE_RMXPSRA_X64-02.03.01.exe.
 - For VMware® vCenter SRM™ 8.2, download HPE_RMXPSRA_X64-02.05.00.exe or HPE_RMXPSRA_X64-02.05.00.gz or later.
- If a previous version of SRA is installed, it must be removed before installing SRA 2.x. See **To remove an earlier version of SRA (Configuration 1, 2)** on page 39 for instructions.
- Install SRA on the VMware® vCenter SRM™ servers on the protected and recovery sites.
- Make sure the RMXPSRA20 executable in the RAID Manager installation is the latest version. If you site has implemented Configuration 3, you can obtain the latest RMXPSRA20 version from the SRM (Photon™ OS) directory.

Installation for Configuration 1 or 2

The following installation procedure applies if your site has implemented SRA Configuration 1 or 2.

Procedure

1. Double-click the executable file in the download folder.
2. Accept the terms of the license agreement and click **Next**.
3. Either accept or change the default installation path. The default location is C:\Program Files\VMware\VMware vCenter Site Recovery Manager.
4. Click **Install** and proceed through the wizard.
5. After the SRA installation, restart the VMware® vCenter SRM™ service.

- a. Right click **My Computer** and select **Manage**.
- b. Click **Services and Application**, then select **Services**.
- c. Locate **VMware Site Recover Manager**, then click **Restart**.

Installation for Configuration 3

Use the following installation procedure if your site has implemented SRA Configuration 3.

NOTE: Before you begin, verify that the CONFIGURE APPLIANCE setting has been configured.

Procedure

1. Log in to **SRM Appliance Management**.
2. Click **Storage Replication >New Adapter**.
3. Click **UPLOAD**, and then select HPE_RMXP_SRA_X64-02.xx.xx.gz.
4. Confirm the SRA version.

Removing an earlier version of SRA

If an earlier version of SRA is installed, it must be removed in order to upgrade to SRA 2.x.

There are two options for removing an earlier version of SRA, depending on the type of configuration your site has implemented. The uninstall instructions pertain to Configuration 1 or 2 and Configuration 3 scenarios.

If needed, you can check the installed version. For information, see [Checking the SRA version](#) on page 40.

To remove an earlier version of SRA (Configuration 1, 2)

Refer to the following instructions for removing an earlier version of SRA if your site has implemented Configuration 1 or 2.

Procedure

1. Open Windows **Control Panel**.
2. Click **Add or Remove Programs**.
3. Select **HPE Storage Replication Adapter** from the list of currently installed programs.
4. Click **Remove**.
5. Open an Explorer window.
6. Navigate to C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\RMXP
7. Right-click the HPE Storage Replication Adapter folder and click **Delete**.
SRA is removed.

To remove an earlier version of SRA (Configuration 3)

Refer to the following instructions for removing an earlier version of SRA if your site has implemented Configuration 3.

Procedure

1. Log in to **SRM Appliance Management**.
2. Click **Storage Replication** then select **SRA** and click **Delete**.
3. Check all boxes then click **Delete**.

Checking the SRA version

You can check your existing version of HPE SRA on the following three machines:

- Windows server
- Linux server
- Docker container on Photon

To check the SRA version on a Windows server

Procedure

1. On the Windows server that is running VMware® vCenter SRM™ and RAID Manager, log in as an administrator.
2. Open a command prompt window.
3. Navigate to `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\RMXP.`
4. Issue the following command:

```
rmsra20 -h
```

Note the version number information that is displayed, for example:

```
Ver&rev: 02.01.03
```

5. To display the RMXPSRA20 version number installed with SRA, issue the following command:

```
./rmsra20 -h
```

To check the SRA version on a Linux server

Procedure

1. On the Linux RAID Manager server, log in as root.
2. Navigate to the `/HORCM/usr/bin` directory.
3. Using FTP, copy the `rmsra20.linux` file from the SRA installation folder on the Windows VMware® vCenter SRM™ server to the `/HORCM/usr/bin` directory on the Linux server that is running RAID Manager.

4. Issue the following commands to make the `rmsra20.linux` file executable:

```
chmod +x rmsra20.linux
mv rmsra20.linux rmsra20
```

5. Issue the following command to display the version number of RMXPSRA20 installed with the SRA:

```
./rmsra20 -h
```

Note the version number information that is displayed, for example:

```
Ver&Rev: 02.05.0x or later
```

To check the SRA version on a Docker Container on Photon

You can check the SRA version on a Docker Container on Photon from the SRM Appliance Management.

Procedure

1. Login to **SRM Appliance Management**.
2. Click **Storage Replication**.

Obtaining the latest rmsra20

If your site has implemented Configuration 3, then install HPE Storage Replication Adapter (SRA) 2.5 before completing the instructions to obtain rmsra20.

Procedure

1. Use SSH to log in to SRM (Photon OS).
2. Move to root user.
3. Locate rmsra20:

```
root@photon [ ]$cd /opt/vmware/support/logs/srm/SRAs/sha256_"[Docker Image ID]"/
```

Refer to the table for the SRA Docker Image ID.

4. Obtain rmsra20 using the scp command, for example:

```
scp rmsra20* "[username]"@"[IP Address]":
```

Deploying rmsra20

After obtaining rmsra20 (see [Obtaining the latest rmsra20](#) on page 41), you can deploy the latest rmsra20 to the RAID Manager Server.

Procedure

1. Deploy rmsra20 using the scp command. For example:

```
scp rmsra20.linux64 "[RAID Manager Server's username]"@"[RAID Manager Server's IP Address]":/HORCM/usr/bin
```

2. Replace the original rmsra20 with the latest rmsra20.

```
cp /HORCM/usr/bin/rmsra20 /HORCM/usr/bin/rmsra20_bak
```

Configuring SRM™ to communicate with RMXPSRA20 (SRM 5.x or earlier)

After the remote replication pair is created, SRA is installed, and the protected and recovery sites are connected, you configure VMware® vCenter SRM™ to discover the replicated volumes and to manage recovery and testing. This is done by configuring the array managers on the local and remote sites.

Configuring array managers is typically done once. If connection information or credentials change, or different storage systems (arrays) are used, then the VMware® vCenter SRM™ array managers must be reconfigured.

Prerequisites

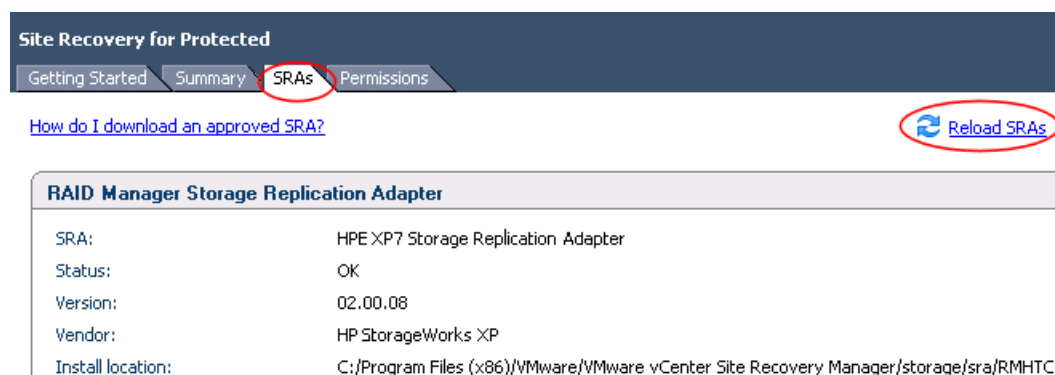
- RAID Manager must be installed.
- All HORCM files must be defined.
- The remote replication pair must be created.
- VMware® vCenter SRM™ must be installed on the vSphere local and remote servers.
- HPE SRA must be installed on both servers.
- The local and remote sites must be paired in VMware® vCenter SRM™.

Procedure

NOTE: The image examples in the procedure may differ depending on your environment.

1. Open the vSphere client and connect to the vCenter server at the protected site.
2. Click the **Site Recovery** icon on the home page.
3. On the Summary tab, click the **Array Managers** line, and then click the protected site in the top-left frame.
4. On the **SRAs** tab, make sure that the desired SRA displays.

If no SRA is listed, click **Reload SRAs** at the top of the screen. If a SRA is still not listed, then no SRA has been installed on the VMware® vCenter SRM™ host. See the procedure in **Installing HPE SRA 2.x** on page 38 for information.



5. In the **Array Manager Information** box, for **Display Name**, enter a specific name for the array manager being added to the site.

Add Array Manager

Array Manager Information

Specify a display name and an installed SRA for this array manager.

Display Name:

SRA Type:

Additional information about available SRA types and versions is available on the SRAs tab of the array manager folder for each site.

[Help](#) [< Back](#) [Next >](#) [Cancel](#)

6. For **SRA Type**, select **HPE XP Storage Replication Adapter**.
7. Click **Next**.
8. In the **Connection to remote HORCM Server** window for Site A, for **HORCMINST** and **IP Address of HORCM(RAID Manager) Server**, enter one of the following:
 - If RAID Manager and the HORCM instance are located on the VMware® vCenter SRM™ server, enter HORCMINST=X, where “X” is the instance number. For example, for HORCM0, enter HORCMINST=0.

When adding array manager for the recovery site, this is the only option.

Add Array Manager

HPE XP7 Storage Replication Adapter

Connection to remote HORCM Server

HORCM Server connection parameters

HORCMINST and IP Address of HORCM(CCI) Server:
 Enter 'HORCMINST=X@IP_Address' to Remote or 'HORCMINST=X' to Local for HORCM(CCI) Server

Username:
 Enter 'username' to Remote 'dummy' to Local for HORCM(CCI) Server

Password:
 Enter 'password' to Remote 'dummy' to Local for HORCM(CCI) Server

- If RAID Manager and the HORCM instance are located on a remote UNIX server, enter one of the following:
 - If connecting to HORCMINST=X on the remote UNIX host, enter HORCMINST=X@Host-name.
 - If connecting to the \$HORCMINST environment variable setting (Remote Login Environment) on a UNIX host, enter \$HORCMINST@Host-name.

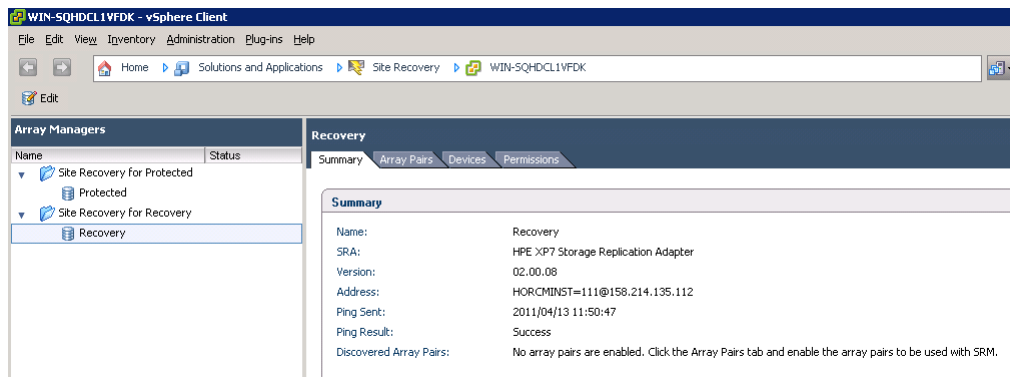
9. Enter a **Username** and **Password** as follows:

- If RAID Manager and the command device are located on the VMware® vCenter SRM™ server and user authentication is not configured on the command device, type any Username and Password.
If user authentication is configured on the command device, enter the required authentication Username and Password.
- If RAID Manager and the command device are located on a remote UNIX server and no root user is needed, then you must have permission for using RAID Manager commands. See the section on changing the RAID Manager user in *HPE XP Storage RAID Manager User Guide*.
If the remote host is Suse Linux that does not know “network” as terminal type, then the following variables must be set:

```
setx RMSRA_TEL_WAITS "/terminal type\? /i" /m
setx RMSRA_TEL_RESPS vt100 /m
```

10. Click **Next**.

11. On the **Summary** tab, verify the connected SRA is HPE XP Storage Replication Adapter.



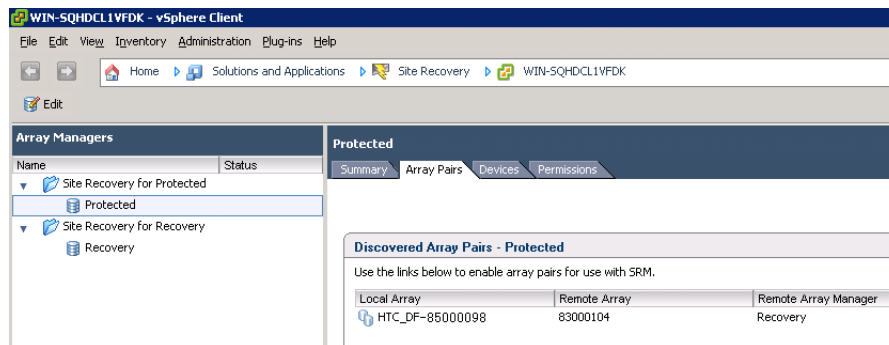
12. Repeat this procedure to configure an array adapter for the recovery site.

Enabling array managers

After you add protected and recovery site array managers, you must enable them.

Procedure

1. Select the protected site array manager then click the **Array Pairs** tab.



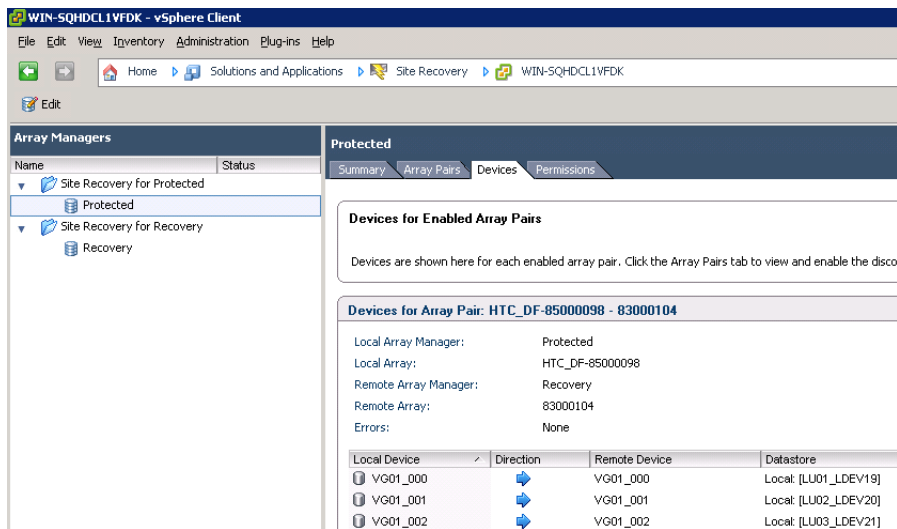
2. Verify that the **Local Array** ID and **Remote Array** ID are discovered on the array manager.
3. Click **Enable**.
4. Repeat this procedure for the recovery site array manager.

Verifying devices

After enabling array managers, you must verify that the local and remote devices are discovered on VMware® vCenter SRM™.

Procedure

1. Select the protected site array manager then click the **Devices** tab.

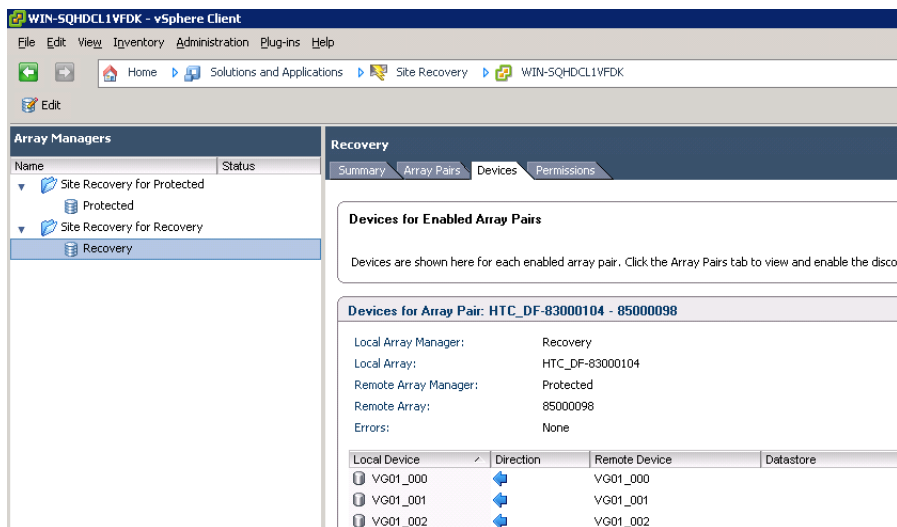


2. Verify discovered devices for the protected site as follows:

- The **Local Device** and **Remote Device** are the dev_name on horcm*.conf.
- The **Direction** is from **Local Device** to **Remote Device**.
- The **Datastore** maps to the P-VOLs.

3. Select the recovery site array manager and verify the discovered devices as follows:

- The **Local Device** and **Remote Device** are the dev_name on horcm*.conf.
- The **Direction** is from **Remote Device** to **Local Device**.
- The **Datastore** maps to the P-VOLs.



Configuring SRM to communicate with RMXPSRA20 (SRM 6.0 or later)

To configure SRM 6.0 or later to communicate with RMXPSRA20, complete the following tasks:

- **Add array manager** on page 48
- **Check devices** on page 54

Add array manager

Configuring array managers is typically done once. If connection information or credentials change, or different storage systems (arrays) are used, then the array managers must be reconfigured.

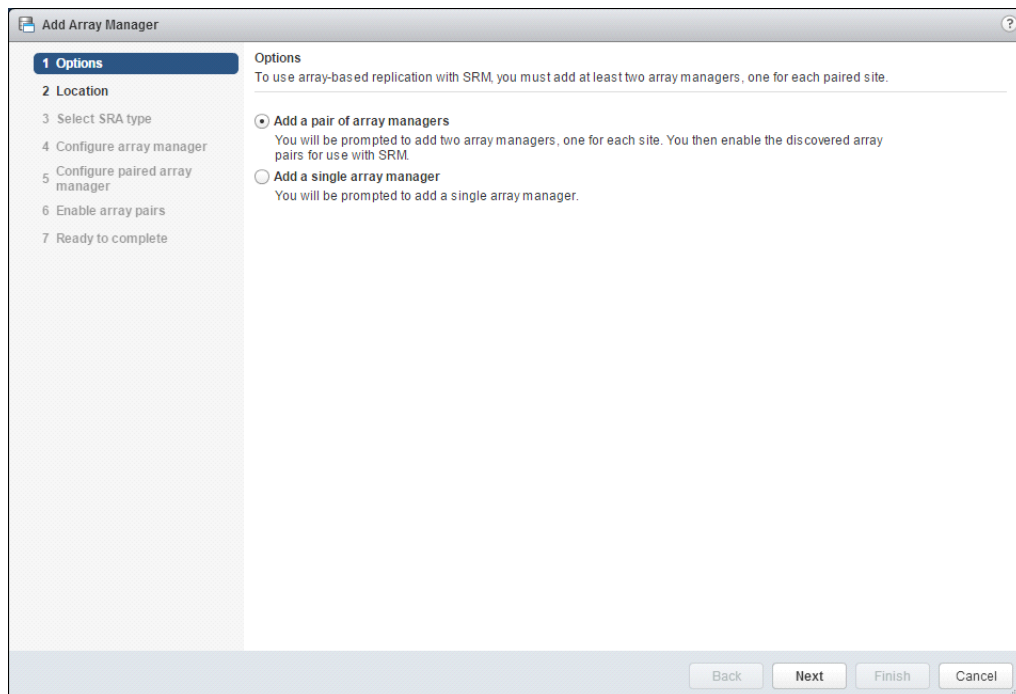
Prerequisites

- SRM is installed at the protected site and the recovery site.
- RMXPSRA20 is installed in the same server as SRM at both sites.
- The protected site and the recovery site must be paired in SRM.
- RAID Manager is installed in a correct configuration.
- All HORCM configuration definition files are defined, and HORCM instances are started.
- Remote replication has been configured.

Procedure

NOTE: The image examples in the procedure may differ depending on your environment.

1. Connect to the vCenter server at the protected site via vSphere Web Client.
2. Click **Site Recovery > Array Based Replication**.
3. Click **Add new Array Manager** in the **Objects** tab.
4. In **Options**, select **Add a pair of array managers**, and click **Next**.



5. In **Location**, select a pair of sites and click **Next**.

Add Array Manager

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

Location
Specify a pair of sites for the two array managers.

Sites	SRM ID
10.213.0 - 10.213.1	com.vmware.vcDr

1 items

Site: 10.213.0
SRM Server: 10.213.0
vCenter Server: 10.213.0
SRM ID: com.vmware.vcDr

Site: 10.213.1
SRM Server: 10.213.1
vCenter Server: 10.213.1
SRM ID: com.vmware.vcDr

Back Next Finish Cancel

6. In **Select SRA type**, select SRA type from the menu. To use an HPE storage system, select **HPE XP Storage Replication Adapter**. After selecting it, click **Next**.

Add Array Manager

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

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

SRA Type	Status
HPE XP7 Storage Replication Adapter	OK

1 items

SRA Type: HPE XP7 Storage Replication Adapter
Version: 02.01.04
Vendor: HP StorageWorks XP
Supported Array Models: HP StorageWorks XP P9000/ XP/ XP7
Supported Software: P9000 RAID Manager XP 01.24.16 or later

Back Next Finish Cancel

If HPE XP Storage Replication Adapter is not displayed, check if RMXPSRA20 is installed in the SRM server correctly, and click **Rescan SRAs**. For SRA rescan, refer to the SRM manual provided by VMware.

7. In **Configure array manager**, enter appropriate values in the following fields.

- **Display Name:** Enter (name) the array name. For example, enter "Protected".
- **HORCMINST and IP Address of HORCM(RAID Manager) Server:** The value that should be entered depends on the configuration. Enter it as follows:
 - When Windows version of RAID Manager is used (RAID Manager is installed in the SRM server): Enter "HORCMINST=X". Enter the HORCM instance number that is used for remote replication running on the SRM server at the recovery site for X. For example, when the HORCM instance number is 300, enter "HORCMINST=300".
 - When UNIX version of RAID Manager is used (RAID Manager is installed in other than the SRM server): Enter "HORCMINST=X@Host-name". Enter the HORCM instance number that is used for remote replication running on the RAID Manager server at the recovery site for X. Enter the host name or the IP address of the RAID Manager server at the recovery site for Host-name. (To enter the host name, DNS needs to be set correctly, and the host name can be resolved in the environment.) For example, when the HORCM instance number is 300 and the IP address of the RAID Manager host is 192.168.1.10, enter HORCMINST=300@192.168.1.10.
- **Username and Password:** The value that should be entered depends on the configuration. Enter it as follows:
 - Windows version of RAID Manager is used: The value that should be entered depends on whether the command device authentication is set.

Command device authentication is not set: The values of username and password are not used in RMXPSRA20. Enter an arbitrary character string as a dummy one. For example, enter "dummy".

Command device authentication is set: In **Username** and **Password**, enter username and password that are used for command device authentication.
 - UNIX version of RAID Manager is used:

Enter the login information of the RAID Manager server.

To set information of a user who does not have the root permission, you need to give the permission to perform RAID Manager.

To use command device authentication, command device authentication needs to succeed in the RAID Manager server in advance. For more information, see **Command device authentication** on page 53.

When the RAID Manager host is Suse Linux, and "network" is not determined as the terminal type, set the following environmental variables in the SRM server.

```
> setx RMSRA_TEL_WAITS "/terminal type\? /i" /m
> setx RMSRA_TEL_RESPS vt100 /m
```

Add Array Manager

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

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

Specify parameters for site '10.213.0'

Display Name: Protected

Connection to HORCM Server

HORCM Server connection parameters
HORCMINST and IP Address of HORCM(CCI) Server: HORCMINST=100
Enter 'HORCMINST=X@IP_Address' to Remote or 'HORCMINST=X' to Local for HORCM(CCI) Server

Username: maintenance
Enter 'username' to Remote 'dummy' or 'array username' to Local for HORCM(CCI) Server

Password: *****
Enter 'password' to Remote 'dummy' or 'array password' to Local for HORCM(CCI) Server

Back Next Finish Cancel

8. Click **Next**. In the event of an error, check the configuration and the entered values.
9. In **Configure paired array manager**, enter appropriate values in the following fields.
 - **Display Name:** Enter (name) the array name. For example, enter "Recovery".
 - **HORCMINST and IP Address of HORCM(RAID Manager) Server:** The value that should be entered depends on the configuration. Enter it as follows:
 - When Windows version of RAID Manager is used (RAID Manager is installed in the SRM server): Enter "HORCMINST=X". Enter the HORCM instance number that is used for remote replication running on the SRM server at the recovery site for X. For example, when the HORCM instance number is 300, enter "HORCMINST=300".
 - When UNIX version of RAID Manager is used (RAID Manager is installed in other than the SRM server): Enter "HORCMINST=X@Host-name". Enter the HORCM instance number that is used for remote replication running on the RAID Manager server at the recovery site for X. Enter the host name or the IP address of the RAID Manager server at the recovery site for Host-name. (To enter the host name, DNS needs to be set correctly, and the host name can be resolved in the environment.) For example, when the HORCM instance number is 300 and the IP address of the RAID Manager host is 192.168.1.10, enter HORCMINST=300@192.168.1.10.
 - **Username and Password:** The value that should be entered depends on the configuration. Enter it as follows:
 - Windows version of RAID Manager is used: The value that should be entered depends on whether the command device authentication is set.
 Command device authentication is not set: The values of username and password are not used in RMXPSRA20. Enter an arbitrary character string as a dummy one. For example, enter "dummy".
 Command device authentication is set: In **Username** and **Password**, enter username and password that are used for command device authentication.
 - UNIX version of RAID Manager is used:

Enter the login information of the RAID Manager server.

To set information of a user who does not have the root permission, you need to give the permission to perform RAID Manager.

To use command device authentication, command device authentication needs to succeed in the RAID Manager server in advance. For more information, see **Command device authentication** on page 53.

When the RAID Manager host is Suse Linux and "network" is not determined as the terminal type, set the following environmental variables in the SRM server:

```
> setx RMSRA_TEL_WAITS "/terminal type\? /i" /m
```

```
> setx RMSRA_TEL_RESPS vt100 /m
```

Add Array Manager

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

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

Specify parameters for site "10.213.111.1"

Display Name: Recovery

Connection to HORCM Server

HORCM Server connection parameters

HORCMINST and IP Address of HORCM(CCI) Server: HORCMINST=300
Enter 'HORCMINST=X@IP_Address' to Remote or 'HORCMINST=X' to Local for HORCM(CCI) Server

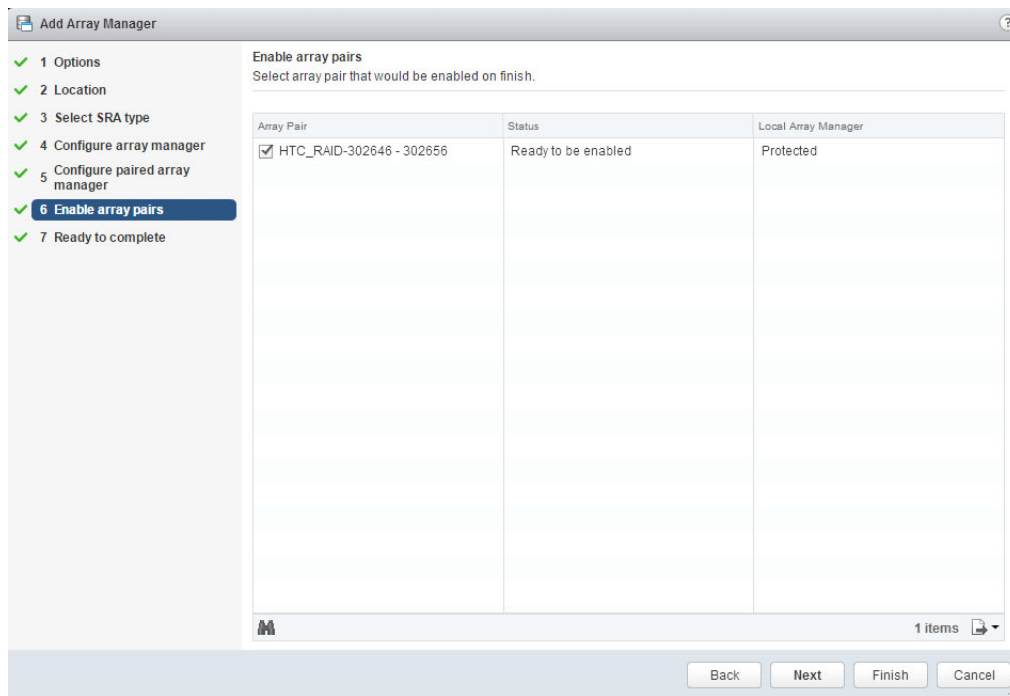
Username: maintenance
Enter 'username' to Remote 'dummy' or 'array username' to Local for HORCM(CCI) Server

Password: *****
Enter 'password' to Remote 'dummy' or 'array password' to Local for HORCM(CCI) Server

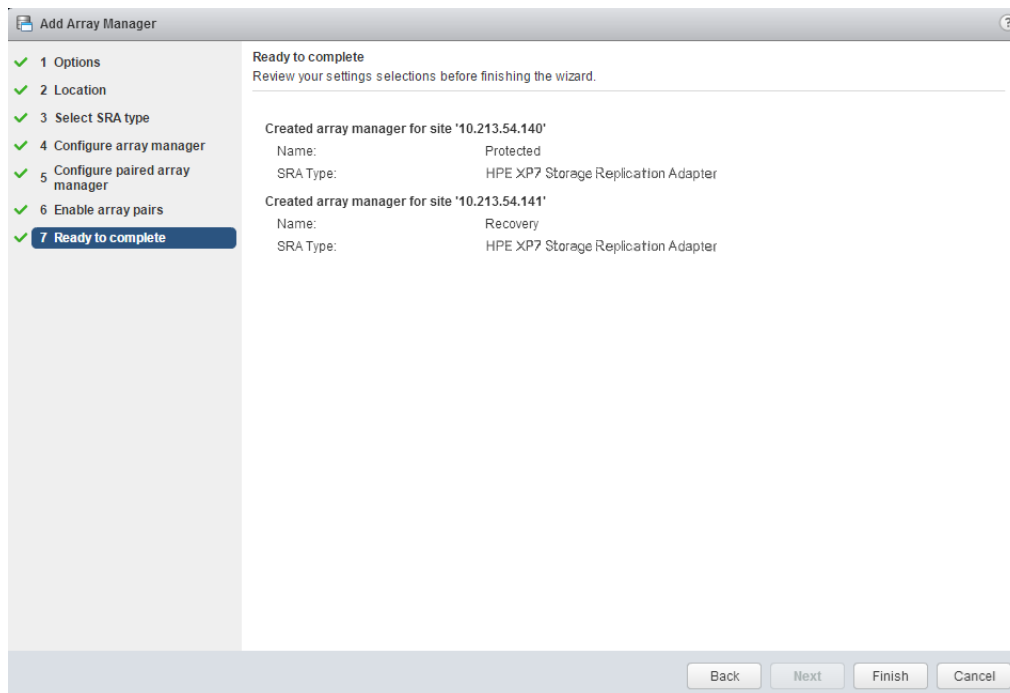
Back Next Finish Cancel

10. Click **Next**. In the event of an error, check the configuration and the entered values.

11. In **Enable array pairs**, select an array pair from the list and click **Next**.



12. In **Ready to complete**, check the configuration at the end, and click **Finish**. In the event of an error, check the configuration.



Command device authentication

Use the following procedure for the command device authentication on UNIX systems.

Procedure

1. Set the "HORCC_AUTH_UID" environmental variable to "HTSRA".

```
# export HORCC_AUTH_UID=HTSRA
```

2. Execute a RAID Manager command and enter login credentials for the storage system.

```
# raidqry -g
```

```
User for Serial#[64016] :
```

```
Password :
```

NOTE: "64016" above is the serial number of the storage system.

3. If the command device authentication succeeds, the following file is created. Verify the file exists.

```
# ls -l /HORCM/usr/var
```

```
-rw----- 1 root root 464 May 20 16:10 RMSVR_root_HTSRA_64016
```

NOTE: "RMSVR" is the server name of Unix, "root" is the user name who logs in to Unix, and "64016" is the serial number of the storage system.

Check devices

Check if the protected volumes are recognized by SRM by completing the following procedure. In the event of an unintended result or an error, check the configuration.

Procedure

1. Connect to vCenter server at the protected site from vSphere Web Client.
2. Click **Site Recovery > Array Based Replication**, and click the site name in the left pane.
3. Click the **Manage** tab.

Protected
Actions

Summary
Monitor
Manage
Related Objects

Array Pairs
Permissions

Array pairs must be enabled for use with SRM. You may enable the array pairs from either the protected or recovery site. Details for the selected array pair are shown below.

Local Array	Remote Array	Status	Local Array Manager	Remote Array Manager
HTC_RAID-30...	302656	✓ Enabled	Protected	Recovery

Array Pair: HTC_RAID-302646 - 302656

Errors: None

Local Device	Status	Remote Device	Datastore	Protection Group	Local Consistency ...
srm0	➔ Outgoing R...	srm0	Local: [snap-5...		srm_pair0
srm1	➔ Outgoing R...	srm1	Local: [snap-0f...		srm_pair0

2 items

4. Check the following items at the protected site:

- Do **Local Device** and **Remote Device** match dev_name in the HORCM configuration definition file?
- Does **Status** show Outgoing?
- Does **Datastore** show Local?

5. Check the following items at the recovery site.

- Do **Local Device** and **Remote Device** match dev_name in the HORCM configuration definition file?
- Does **Status** show Incoming?
- Does **Datastore** show Remote?

Configuring SRM to communicate with RMXPSRA20 (SRM 8.2 or later)

To configure SRM 8.2 or later to communicate with RMXPSRA20, complete the following tasks:

- **Add array manager** on page 56
- **Check devices** on page 57

Add array manager

Configuring array managers is typically done once. If connection information or credentials change, or different storage systems (arrays) are used, then the array managers must be reconfigured.

Prerequisites

- SRM is installed at the protected site and the recovery site.
- RMXPSRA20 is installed in the same server as SRM at both sites.
- The protected site and the recovery site are paired in SRM.
- RAID Manager is installed in a correct configuration.
- All HORCM configuration definition files are defined, and HORCM instances are started.
- Remote replication has been configured.

Procedure

1. Connect to the vCenter server at the protected site using vSphere Web Client.
2. Click **Site Recovery** then click **VIEW DETAILS**.
3. Click **Configure > Array Based Replication > Storage Replication Adapters**.
4. Make sure that the version of SRA is the one that you installed:
 - If not on display, Click **RESCAN ADAPTERS** on both the protected site and the recovery site.
 - If the version on display differs from the one that you installed, re-install SRA. See **Installing HPE SRA 2.x** on page 38.
5. Click **Configure > Array Based Replication > Array Pairs** then click **+ADD**.
6. In Storage replication adapter, confirm whether **Status** is **OK**. If it is, click **NEXT**.
7. In **Local array manager**, enter appropriate values and verify information:
 Enter a name for the array manager. In the following example, X is the HORCM instance number on the RAID Manager Server: HORCMINST=X@Host-name

 Enter a Username and Password for the RAID Manager Server.

 Confirm that all HORCM configuration definition files are defined, and HORCM instances are started.

 Confirm that remote replication has been configured.
8. Click **NEXT**.
 In the event of an error, check the configuration and the entered values.
9. In **Remote array manager**, enter appropriate values and verify information:
 Enter a name for the array manager. In the following example, X is the HORCM instance number on the RAID Manager Server: HORCMINST=X@Host-name

Enter a Username and Password for the RAID Manager Server.

Confirm that all HORCM configuration definition files are defined, and HORCM instances are started.

Confirm that remote replication has been configured.

10. Click NEXT.

In the event of an error, check the configuration and the entered values.

11. In Array pairs, select the array pairs to enable then click NEXT.

12. In Ready to complete, check the configuration at the end, then click FINISH.

In the event of an error, check the configuration.

NOTE: For information about command device authentication on UNIX systems of the RAID Manager Server, refer to the topic, **Configuring SRM to communicate with RMXPSRA20 (SRM 6.0 or later)** on page 47.

Check devices

Check if the protected volumes are recognized by SRM by completing the following procedure. In the event of an unintended result or an error, check the configuration.

Procedure

1. Click Configure > Array Based Replication > Array Pairs.

2. Select the array pairs to check.

3. Check the following items at the protected site:

- Do Device (protected site) and Device (recovery site) match dev_name in the HORCM configuration definition file?
- Does **Status** show **Forward** or **Reverse**?

Performing reprotect and failback

When failure or abnormal termination occurs on the protected site, the recovery plan must be executed to initiate the failover operation.

Failover moves production operations to the recovery site. The following actions are run automatically in an VMware® vCenter SRM™ failover:

1. HBAs are rescanned
2. Datastores are mounted
3. VMs are registered
4. VMs are customized and powered on

After failover or planned migration, protect the recovery site against failure using the reprotect feature, which establishes synchronized replication back to the original protected site.

When reprotect has occurred, perform the failback operation to return the replication environment back to its original state at the protected site. Failback can be managed as a normal server migration process.

VMware® vCenter SRM™ supports reprotect and manual failback in the following scenarios:

- Failure at site A and migration to site B
- Planned host down (ESX/ESXi Server) at site A and migration to site B

To perform reprotect and manual failback

Procedure

1. Execute the reprotect operation on the recovery site.
2. Execute the failover or migration operation on the protected site.
3. Execute the reprotect operation on the protected site.

If these operations fail, proceed as follows:

- Ensure that the remote link and remote array are functional, using the **pairedisplay -g <grp>** command. If necessary, recover the remote link and remote array.
- Re-execute the reprotect operation.

Troubleshooting

This chapter provides information and instructions for troubleshooting configuration problems.

Error messages on VMware® vCenter SRM™ log files

RMXPSRA20 generates error messages in the following order in the VMware® vCenter SRM™ log files:

- **XML errors received from VMware® vCenter SRM™** on page 59
- **Failure to launch scripts** on page 65

You can remove the cause of the error by referring to “[RMSRA20]” and “SRM ERROR messages” in the VMware® vCenter SRM™ log files.

The VMware® vCenter SRM™ log is located in the following directory:

Windows Server 2003: C:\Documents and Settings\All Users\VMware\VMware vCenter Site Recovery Manager\Logs\

Windows Server 2008: C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs\

- By default, logs roll over after reaching 5 MB
- vmware-dr-index contains the most recent Log File number

Docker Container (Configuration 3): /var/log/vmware/srm/

XML errors received from VMware® vCenter SRM™

The following is a list of XML errors received from VMware® vCenter SRM™.

100

- Cause: Required components are not correctly installed or settings of the components are not correct.
- Action: Check if SRM and SRA are correctly installed and settings of SRM and SRA are correct. If you use SSH, you have to also check if plink.exe is correctly installed and settings of plink.exe are correct.

1002

- Cause: The HORCM instance could not start with the specified connection address.
- Action: Check whether the HORCM instance# specified in the connection address is correct, or whether the horcm*.conf file exists.

1003

- Cause: Authentication failed for User/Password for the specified connection address.
- Action: Check whether the User/Password for the connection address is correct.

1400

- Cause: RAID Manager Server's key fingerprint not registered.
- Action: Check that known_host file is set correctly.

1301 [RMSRA20][Time]: [command_main] : XML length over -> [XML parameter strings ...].

- Cause: A parameter in XML was input from VMware® vCenter SRM™ to the SRA, but it exceeds the defined length for the SRA specification.
- Action: Confirm that VMware® vCenter SRM™ received the appropriate parameters in XML from the VMware® vCenter SRM™ log message.

1302, 1303 [RMSRA20][Time]: [command_main] : Parameter in XML was NOT enough.

- Cause: A parameter in XML was input from VMware® vCenter SRM™ to the SRA but it could not be found in any parameters.
- Action: Confirm that VMware® vCenter SRM™ received the appropriate parameters in XML from the VMware® vCenter SRM™ log message.

1304 [RMSRA20][Time]: [command_discoverDevices] : NO ArrayId or No PeerArrayId in XML.

- Cause: A parameter in XML (discoverDevices) was input from VMware® vCenter SRM™ to the SRA but the array ID could not be found.
- Action: Confirm that VMware® vCenter SRM™ received the Array ID parameter in XML from the VMware® vCenter SRM™ log message.

1305 [RMSRA20][Time]: [command_naming] : NO ArrayId or NO DeviceKey and GroupKey in XML.

- Cause: A parameter in XML (naming) was input from VMware® vCenter SRM™ to the SRA, but TargetDevice Key(LDEV# of Cnt Ac-S_S-VOL) or Target Group Key(dev_group in HORCM) could not be found in the parameter.
- Action: Confirm whether VMware® vCenter SRM™ was passed the TargetDevice Key parameter in XML from the VMware® vCenter SRM™ log message.

1XXX : Shows ERROR CODE for "queryErrorDefinitions"

Naming : checkTestFailoverStart/ checkFailover/ testFailoverStart / testFailoverStop/failover/

1305 [RMSRA20][Time]: [command_naming] : NO ArrayId or NO PeerArrayId or NO DeviceKey and GroupKey in XML.

- Cause: A parameter in XML (naming) was input from VMware® vCenter SRM™ to the SRA, but it could not be found in SourceDevice id(LDEV# of Cnt Ac-S_S-VOL) or Consistency Group id(dev_group in HORCM).
- Action: Confirm whether VMware® vCenter SRM™ was passed the SourceDevice id parameter in XML from the VMware® vCenter SRM™ log message.

Naming : syncOnce/ querySyncStatus/ reverseReplication / restoreReplication/

1306 [RMSRA20][Time]: [command_naming] : Unsupported command 'command naming' in XML.

- Cause: A command naming was input from VMware® vCenter SRM™ to the SRA, but it could not be supported.
- Action: Confirm whether VMware® vCenter SRM™ was passed an appropriate command naming in XML from the VMware® vCenter SRM™ log message.

1251 [RMSRA20][Time]: [command_main] : Can't be connected to HORCMINST=X@... with error(0x000000fc).

- Cause: A connection address in XML was input from VMware® vCenter SRM™ to the SRA, but HORCM instance #X could not be found.
- Action: Check whether the HORCM instance#X is running, or whether a connection address (IP Address) specified in Array Manager configuration is appropriate.

RAID Manager command errors in rmsra20.exe

1307 [RMSRA20][Time]: ["XML OUTPUT file name"] : fopen : "system error message"

- Cause: A parameter in XML was input from VMware® vCenter SRM™ to the SRA, but "XML OUTPUT file name" could not be created.
- Action: Confirm that VMware® vCenter SRM™ received the appropriate OutputFile in XML from the VMware® vCenter SRM™ log message, or refer to the system error message.

1270 [RMSRA20][Time]: [system()] : "Command line" : "system error message"

- Cause: An execution of "Command line" failed via system() call.
- Action: Confirm that RAID Manager is installed, that the path of "Command line" is correct, that %HORCMROOT% ENV has been set, or refer to the system error message.

1269 [RMSRA20][Time]: ["Command line"] : popen : "system error message"

- Cause: An execution of "Command line" failed via popen() call.
- Action: Confirm that RAID Manager is installed, that the path of "Command line" is correct, that %HORCMROOT% ENV has been set, or refer to the system error message.

1268[RMSRA20][Time]: [] : malloc : "system error message"

- Cause: Memory was insufficient for executing an RMXPSRA20.
- Action: Increase system capacity of virtual memory, or terminate unnecessary programs or daemon processes that are running simultaneously.

1xxx [RMSRA20][Time]: [] : “Command line” failed with RC=XXX.

- Cause: An execution of “Command line” failed with RC=XXX.
- Action: Check the RAID Manager error code and command error log messages below, then remove the cause of the error.

```
-----  
COMMAND ERROR : EUserId for HORC[24] : root (0) Thu Jul 17 18:38:55  
2008  
CMDLINE : pairedisplay -ICA -d 64015 9 0 -CLI -l -fwe  
18:38:55-41110-14817- ERROR:cm_sndrcv[rc < 0 from HORCM]  
18:38:55-4c5e8-14817- Could not find a group on configuration file for this  
LDEV.(Port# ?,Seq# 64015,LDEV# 9,mun# 0)  
18:38:55-51feb-14817- [pairedisplay][exit(239)]  
[EX_ENOGRP] No such group  
Cause: The group name which was designated or the device name doesn't  
exist in the configuration file, or the network address for remote  
communication doesn't exist.  
Action: Confirm that the group name exists in the configuration file of the  
local and remote host.  
-----
```

Configuration and status errors

1256 : 1258 : 1260 [RMSRA20][Time]: [qrysnc_chk] : “ Command line” ? GRP = , P/S = , Status = , Fence = , PERCT = .

- Cause: The pair status of a source volume specified with syncOnce/ querySyncStatus is incorrect (its pair status is SMPL or PSUS, or the volume is S-VOL).
- Action: Confirm that the volume status is correct (the volume is P-VOL and its pair status is PAIR or COPY) using the pairedisplay command.

1266 : [RMSRA20][Time]: [qrysnc_chk] : The output of “Command line” is missing.

- Cause: The correct format could not be found in the output of the “Command line” command via syncOnce/querySyncStatus.
- Action: Confirm that the RAID Manager version is correct and supports RMXPSRA20.

1256 : 1257 : 1260 [RMSRA20][Time]: [failover_chk] : “Command line” ? GRP = , P/S = , Status = , Fence =

- Cause: The pair status of a target volume specified with failover is inappropriate (its pair status is SMPL or COPY, or the volume is P-VOL).
- Action: Confirm that volume status is correct (the volume is S-VOL and its pair status is PAIR) using the pairedisplay command.

1266 : [RMSRA20][Time]: [failover_chk] : The output of “Command line” is missing.

- Cause: The correct format could not be found in the output of the “Command line” command via failover.
- Action: Confirm that the RAID Manager version is correct and supports RMXPSRA20.

1256 : 1257 : 1260 [RMSRA20][Time]: [testFailover_chk] : “ Command line” ? GRP = , L/R = , P/S = , Status = , CTG = .

- Cause: The pair status of a target volume specified with testFailover is incorrect (its pair status is SMPL or NOT PAIR, or the volume is P-VOL).
- Action: Confirm that the volume status is correct (the volume is S-VOL of BC or FS and its pair status is PAIR) using the pairedisplay command.

1266 : [RMSRA20][Time]: [testfailover_chk] : The output of “Command line” is missing.

- Cause: The correct format could not be found in the output of the “Command line” command via testFailover.
- Action: Confirm that the RAID Manager version is correct and supports RMXPSRA20.

1272 : [RMSRA20][Time]: [fov_group_exe] : invalid arrayId (...).

- Cause: A parameter in XML (naming) was input from VMware® vCenter SRM™ to the SRA, but the correct array ID could not be found.
- Action: Confirm whether VMware® vCenter SRM™ was passed an array ID parameter in XML (failover) from the VMware® vCenter SRM™ log message.

Naming : checkTestFailoverStart/ checkFailover/ testFailoverStart / testFailoverStop/failover/

: syncOnce/ querySyncStatus/ reverseReplication / restoreReplication/

1265 : [RMSRA20][Time]: [failover_chk] : Unknown LWWN.

- Cause: The LUN WWN could not be found in the output of the pairedisplay –fwe command with checkfailover/failover.
- Action: Confirm that the RAID Manager version is correct and supports RMXPSRA20.

1265 : [RMSRA20][Time]: [testfailover_chk] : Unknown LWWN.

- Cause: The LUN WWN could not be found in the output of the pairedisplay –fwe command with checktestfailover/testfailover.
- Action: Confirm that the RAID Manager is the correct version supported by RMXPSRA20.

Error codes for multiple errors

RMXPSRA20 defines an error code by an “OR” flag of 32 bits so you can identify multiple errors for a transaction from the XML data strings. For example:

```
[RMSRA20][Sun Aug 3 16:25:56 2008]: [command_main] :  
'testFailover_start' failed with error(0x00002000) on  
arrayId(64015) .
```

The following table describes these error codes.

Table 4: Error codes

Error Codes	Error Bits	Description
1200-1255	0x000000XX	XX : exit code returned from RAID Manager command. Refer to the RAID Manager command error code.
1256	0x00000100	The volume is in SMPL status
1257	0x00000200	The volume is inappropriate property as "P-VOL"
1258	0x00000400	The volume is inappropriate property as "S-VOL"
1259	0x00000800	undefined
1260	0x00001000	The volume pair status is not the correct status to run the operation
1261	0x00002000	The volume has no Consistency Group setting
1262	0x00004000	undefined
1263	0x00008000	undefined
1264	0x00010000	The pairedisplay command has no PWWN in the output
1265	0x00020000	The pairedisplay command has no LUN WWN in the output
1266	0x00040000	The pairedisplay command does not support SRA
1267	0x00080000	undefined
1268	0x00100000	Memory allocation error
1269	0x00200000	Popen() function of the system was returned with ERROR
1270	0x00400000	System() function of the system was returned with ERROR
1271	0x00800000	undefined
1272	0x01000000	Error in XML from VMware® vCenter SRM™
1273	0x02000000	undefined
1274	0x04000000	undefined
1275	0x08000000	undefined

Table Continued

Error Codes	Error Bits	Description
1276	0x10000000	undefined
1277	0x20000000	undefined
1278	0x40000000	undefined
1279	0x80000000	undefined
1300	-	Memory allocation error for XML input
1301	-	Length error in XML parameter strings
1302	-	There is no parameter for a command in XML
1303	-	There is no connection parameter for a command in XML
1304	-	There is no arrayID parameter for a command in XML
1305	-	There is no arrayID or Device Key parameter for a command in XML
1306	-	There is not a supported command name in XML
1307	-	Open error for the specified file in XML
1308	-	Unexpected RAID Manager command error
1400	-	RAID Manager Server's key fingerprint not registered

Failure to launch scripts

If VMware vCenter Site Recovery Manager array manager configuration fails to launch the SRA 2.0, an error message appears as shown in **Figure 7: Error message** on page 65.

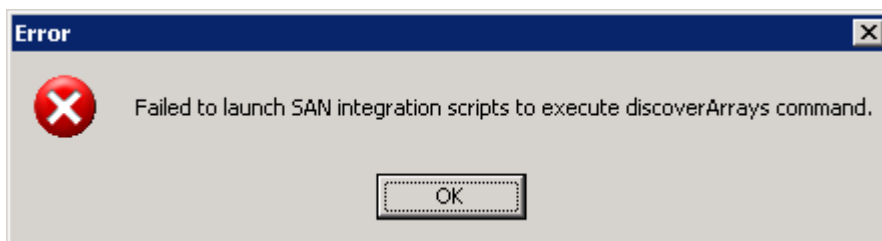


Figure 7: Error message

Correcting UNIX RAID Manager server problems

Procedure

1. Log in to UNIX as **root**.
2. Check that the HORCM instance is running using the command **ps -ef | grep horcm**.
3. Check that the correct version of RMXPSRA20 is installed using the following command:
/HORCM/usr/bin/rmsra20 -h

Ver&Rev: 02.01.01

4. Check that the Alias is entered correctly. For example: HORCMINST=X@<RAID Manager server IP>.

Correcting Windows RAID Manager server problems

If RAID Manager is running on a Windows server, it must be installed together with VMware vCenter Site Recovery Manager on the same server. No remote communication is allowed on the Windows SRA.

Procedure

1. Check that the HORCM instance is running using the command **horcmstart <instance number>**.
2. Check the version of rmsra in the HORCM installation.

C:\HORCM\etc>rmsra20 -h

Ver&Rev: 02.01.01

Collecting information before contacting customer support

Please collect the following information before contacting customer support.

VMware® vCenter SRM™/SRA local configuration

On Windows where VMware® vCenter SRM™ is running, perform the following procedures.

Procedure

1. Collect the VMware® vCenter SRM™ log file on Windows on both protected and recovery sites. Collect the following VMware® vCenter SRM™ log file including the error messages of “[RMSRA]” and “VMware® vCenter SRM™ ERROR messages” and the RAID Manager command error log.

%ALLUSERSPROFILE%\ Application Data\VMware\VMware Site
Recovery Manager\Logs\vmware*.log

2. Collect the outputs of the following command on HORCMINST=XX (where # is the instance number for SRA):

- **set**
- **%HORCMROOT%\HORCM\etc\raidqry -l -l#**

- %HORCMROOT%\HORCM\etc\raidqry -g -l#
- %HORCMROOT%\HORCM\etc\pairedisplay -ICA# -g ??? -CLI -l -fwe (where ??? is a group name shown by `raidqry -g`)
- %HORCMROOT%\HORCM\etc\raidscan -ICA# -p port(e.g. cl1-a-0) - CLI (port connected to ESX/ESXi server)

If Business Copy is installed:

%HORCMROOT%\HORCM\etc\pairedisplay -g ??? -CLI -l -few -m cas -l# (where ??? is a group name shown by `raidqry -g`)

VMware® vCenter SRM™/SRA remote configuration

On Windows where VMware® vCenter SRM™ is running, and on UNIX where RAID Manager is running, perform the following procedures.

Procedure

1. Collect the VMware® vCenter SRM™ log file on Windows on both protected and recovery site.
2. Collect the following VMware® vCenter SRM™ log file including the error messages of “[RMSRA]” and “SRM ERROR messages” and the RAID Manager command error log.
 %ALLUSERSPROFILE%\ Application Data\VMware\VMware Site Recovery Manager\Logs\vmware*.log
3. Collect the outputs of the following command on HORCMINST=XX on remote UNIX, where # is the SRA instance number.
 - env
 - raidqry -l -l#
 - raidqry -g -l#
 - pairedisplay -ICA# -g ??? -CLI -l -fwe (where ??? is the group name shown by `raidqry -g`)
 - raidscan -ICA# -p port (e.g. cl1-a-0) -CLI (port connected to ESX/ESXi sever)
4. If Business Copy is installed, collect the following:
 pairedisplay -g ??? -CLI -l -few -m cas -l# (where ??? is the group name shown by `raidqry -g`)

VMware® vCenter SRM™/SRA Photon™ OS configuration

For Photon™ OS on which VMware® vCenter SRM™ is running, and on UNIX where RAID Manager is running, perform the following procedure.

Procedure

1. Collect the VMware® vCenter SRM™ log file on Photon™ OS from both the protected and recovery site:
 /opt/vmware/support/logs/srm/vmware*.log
2. Collect the outputs of the following command on HORCMINST=XX on UNIX where RAID Manager is running (where # is the instance number for SRA):

- `raidqry -l -l#`
 - `raidqry -g -l#`
 - `pairdisplay -lH# -g ??? -CLI -l -fwe` (where ??? is the group name shown by `raidqry -g`)
 - `raidscan -lH# -p port` (e.g., `cl1-a-0`) -CLI (port connected to the ESX/ESXi server)
3. If Business Copy is installed, collect the following:
`pairdisplay -g ??? -CLI -l -few -m cas -l#` (where ??? is the group name shown by `raidqry -g`)

SRA Change Log

This chapter provides the change log for HPE Storage Replication Adapter (SRA).

Change log for SRA

The following table provides the change log for SRA.

SRA version	Command.pl revision*	Command_dc.pl revision*	Description of change
2.1.4	2.7	Not Installed.	Initial release of SRA 2.1.4
2.1.4	2.8	Not Installed.	Fixed the following problem: Test failover with local replication pairs fails, if the local replication pairs use an MU# other than 0 and SSH remote connection is used between SRA and RAID Manager.
2.2	2.9	Not Installed.	<ul style="list-style-type: none">• Added support for High Availability (HA).• Discontinued support for XP12000 Disk Array, XP10000 Disk Array.

Table Continued

SRA version	Command.pl revision*	Command_dc.pl revision*	Description of change
2.3.1	2.9	Not Installed.	<ul style="list-style-type: none"> Fixed the following problem that occurred: When "Planned Migration" is performed in the HA configuration, the error message of "Unexpected element 'Identity' found" appears, and "Prepare storage for migration at protected site" process ends abnormally. Additionally, this problem might occur when all the following conditions apply: <ul style="list-style-type: none"> "Planned Migration" is performed. "Disaster Recovery" was performed after a failure had occurred on the protected site. The protected site recovered from the failure after "Planned Migration" is performed.
2.5.x	2.9	1.1	Added Command_dc.pl for SRA running on Docker Container.
<p>*The revision is described in the header of the <code>command.pl</code> or <code>command_dc.pl</code> file. These files are located in <code><SRM install directory>\storage\sra\RMHTC</code> or <code>/srm/sra</code>.</p>			

Configurations with both sites active

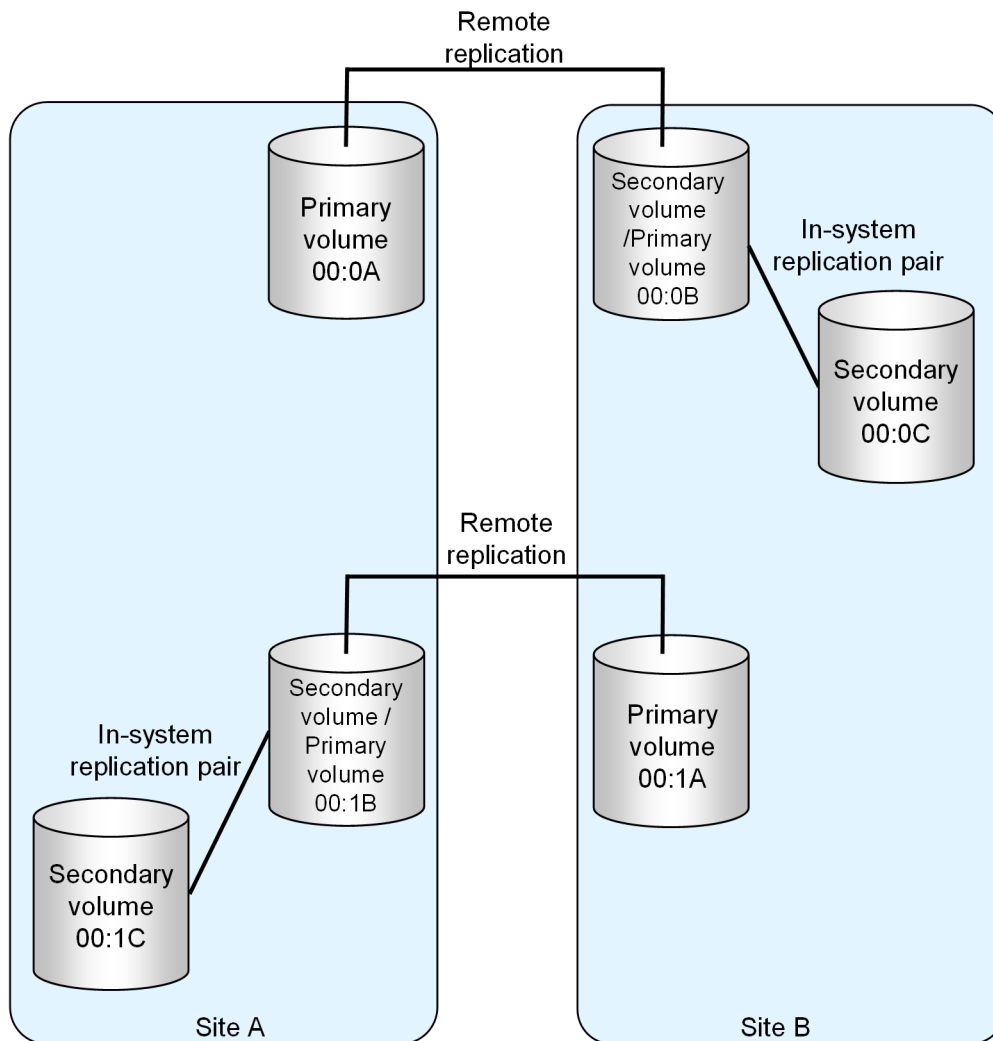
This chapter describes configurations in which both protected and recovery VMs are present on the local and remote sites.

Protecting both sites

This section describes the typical SRM configuration with one protected site (A) and one recovery site (B). You create HORCM definition files explicitly defining protected and recovery volumes.

You can also set up a configuration in which both sites are active, thus providing protection for each site. In this scenario, some VMs on site A are protected with recovery on site B; and some VMs on site B are protected, with recovery on site A.

The following illustration shows a configuration with the protected and recovery sites active.



HORCM definition file setup

HORCM files must reflect your configuration. The following four figures show examples of the local and remote site HORCM configuration files (HORCM.conf) for the configuration shown in the preceding figure.

Site A horcm0

```
HORCM_MON
#ip_address      service      poll(10ms)      timeout(10ms)
172.17.46.38     horcm0          1000            3000

HORCM_CMD
#dev_name
\\.\CMD-64015

HORCM_LDEV
#dev_group      dev_name      Serial#      CU:LDEV(LDEV#)      MU#
#Replication Site A to Site B
CA_CAJ_SRM1      01A_01B      64015        00:0A
#Replication Site B to Site A
CA_CAJ_SRM2      01B_01A      64015        00:1B
#Snapshot or BC copy for testfailover
BC_SRM2          BC_01B_01C    64015        00:1B                0

HORCM_INST
#dev_group      ip_address      service
CA_CAJ_SRM1      172.17.46.39   horcm1
CA_CAJ_SRM2      172.17.46.39   horcm1
BC_SRM2          172.17.46.38   horcm3
```

Site A BC/Snapshot horcm3

```
HORCM_MON
#ip_address      service      poll(10ms)      timeout(10ms)
172.17.46.38     horcm3        1000            3000

HORCM_CMD
#dev_name
\\.\CMD-64015

HORCM_LDEV
#dev_group      dev_name      Serial#      CU:LDEV(LDEV#)      MU#
BC_SRM2          BC_01B_01C    64015        00:1C

HORCM_INST
#dev_group      ip_address      service
BC_SRM2          172.17.46.38   horcm0
```

Site B horcm1

```
HORCM_MON
#ip_address      service      poll(10ms)      timeout(10ms)
172.17.46.39     horcm1        1000            3000

HORCM_CMD
#dev_name
\\.\CMD-64016

HORCM_LDEV
#dev_group      dev_name      Serial#      CU:LDEV(LDEV#)      MU#
#Replication Site A to Site B
CA_CAJ_SRM1      01A_01B      64016        00:0B
#Replication Site B to Site A
```


CA_CAJ_SRM2	01B_01A	64016	00:1A	
#SnapShot or BC copy for testfailover				
BC_SRM1	BC_01B_01C	64016	00:0B	0

HORCM_INST		
#dev_group	ip_address	service
CA_CAJ_SRM1	172.17.46.38	horcm0
CA_CAJ_SRM2	172.17.46.38	horcm0
BC_SRM1	172.17.46.39	horcm2

Site B BC/Snapshot horcm2

HORCM_MON			
#ip_address	service	poll(10ms)	timeout(10ms)
172.17.46.39	horcm2	1000	3000

HORCM_CMD	
#dev_name	
\\.\CMD-64016	

HORCM_LDEV				
#dev_group	dev_name	Serial#	CU:LDEV(LDEV#)	MU#
BC_SRM1	BC_01B_01C	64016	00:0C	

HORCM_INST		
#dev_group	ip_address	service
BC_SRM1	172.17.46.39	horcm1

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](#) on page 75.

XP websites

XP7 documentation (Storage Information Library)

www.hpe.com/info/xp7-docs

XP7 documentation (HPESC)

www.hpe.com/info/XP7manuals

XP7 Command View Advanced Edition documentation (Storage Information Library)

www.hpe.com/info/cvae-docs

XP7 Command View Advanced Edition documentation (HPESC)

www.hpe.com/support/CVAE7/manuals

Support and other resources

Accessing Hewlett Packard Enterprise Support

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

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 information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-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

HPE 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.