

# Hitachi Storage Replication Adapter for VMware® vCenter Site Recovery Manager™

02.03.01

---

## Deployment Guide

This document provides deployment and implementation information for VMware® vCenter Site Recovery Manager™ 5.x/ 6.x using Hitachi Storage Replication Adapter 2.x.

© 2009, 2017 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara Corporation (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara Corporation at [https://support.hitachivantara.com/en\\_us/contact-us.html](https://support.hitachivantara.com/en_us/contact-us.html).

**Notice:** Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara Corporation.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals to access relevant data; and
2. Verifying that data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

**Notice on Export Controls.** The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.



# Contents

Preface.....	7
Intended audience.....	8
Product version.....	8
Release notes.....	8
Changes in this release.....	8
Document conventions.....	8
Conventions for storage capacity values.....	9
Accessing product documentation.....	10
Getting help.....	10
Comments.....	11
<b>1 Overview.....</b>	<b>13</b>
About Hitachi Storage Replication Adapter and Site Recovery Manager.....	14
VMware vCenter infrastructure.....	14
Hitachi storage and replication software products.....	14
Command Control Interface (CCI).....	16
How the VMware® vCenter SRM™/SRA solution works.....	17
<b>2 Requirements, planning, and prerequisites.....</b>	<b>19</b>
Requirements.....	20
SRA/VMware® vCenter SRM™/CCI location options.....	22
Test options.....	23
Using the S-VOL for testing.....	23
Required configuration for testing with S-VOL.....	23
Using a copy of the S-VOL for testing.....	24
Required configuration for testing with a copy of S-VOL.....	24
ShadowImage port requirement.....	24
Configurations with protected and recovery VMs on the same site.....	25
Consistency groups and VM failover groups.....	25
Consistency groups and same-time split operations.....	25
About the TrueCopy fence level “Never”.....	26
Prerequisites for global-active device configuration.....	26

AMS 2000 host group options.....	28
<b>3 Deployment.....</b>	<b>31</b>
Deployment workflow.....	32
Installing CCI.....	33
Creating and configuring a command device.....	33
Setting up HORCM configuration definition files.....	36
Editing HORCM.conf files.....	36
Primary HORCM file.....	38
Secondary HORCM file.....	39
In-system test copy HORCM file.....	41
Starting HORCM instances, creating pairs.....	41
Creating a copy for testing on the recovery site.....	42
Setting environment variables.....	43
Defining environment variables using the GUI.....	44
About SSH.....	45
Configuring SRA for testing.....	46
Setting environment variables on the VMware® vCenter SRM™ host.....	46
Setting environment variables on a UNIX Host.....	47
SRA installation.....	47
Installing Hitachi SRA 2.x.....	48
Removing an earlier version of SRA.....	48
Checking the SRA version.....	49
To check the SRA version on a Windows server.....	49
To check the SRA version on a Linux server.....	49
Configuring SRM™ to communicate with RMSRA20 (SRM 5.x or earlier).....	50
Enabling array managers.....	54
Verifying devices.....	54
Configuring SRM to communicate with RMSRA20 (SRM 6.0 or later).....	56
Add array manager.....	56
Command device authentication.....	62
Check devices.....	63
Performing reprotect and failback.....	64
<b>4 Troubleshooting.....</b>	<b>67</b>
Error messages on VMware® vCenter SRM™ log files.....	68
XML errors received from VMware® vCenter SRM™.....	68
CCI command errors in rmsra20.exe.....	70
Configuration and status errors.....	72
Error codes for multiple errors.....	73
Failure to launch scripts.....	75
Correcting UNIX CCI server problems.....	75
Correcting Windows CCI server problems.....	75
Test failover errors.....	76
Collecting information before contacting customer support.....	78
VMware® vCenter SRM™/SRA local configuration.....	78
VMware® vCenter SRM™/SRA remote configuration.....	79
Calling Hitachi Vantara customer support.....	80

5	SRA Change Log.....	81
	Change log for SRA.....	82
A	Configurations with both sites active.....	83
	Protecting both sites.....	84
	HORCM definition file setup.....	85
	Index.....	87





# Preface

This document provides deployment and implementation information for VMware® vCenter Site Recovery Manager™ 5.x/ 6.x using Hitachi Storage Replication Adapter 2.x.

Please read this document carefully to understand the deployment requirements for the VMware vCenter Site Recovery Manager, and maintain a copy for reference.

This preface includes the following information:

- [Intended audience](#)
- [Product version](#)
- [Release notes](#)
- [Changes in this release](#)
- [Document conventions](#)
- [Conventions for storage capacity values](#)
- [Accessing product documentation](#)
- [Getting help](#)
- [Comments](#)

## Intended audience

This document is intended for storage administrators who are involved in the deployment of the VMware vCenter Site Recovery Manager.

Readers of this document should be familiar with the following:

- Hitachi Vantara storage management tools including the Command Control Interface (CCI) software.
- Windows systems, and if a Linux server is intended for use as a CCI server, working knowledge of Linux system administration.
- The VMware vCenter Site Recovery Manager software.

## Product version

This document revision applies to Hitachi Storage Replication Adapter version 2.3, which has a sub-component, RAID Manager Storage Replication Adapter (RMSRA20) versions 02.01.0, 02.01.03, 02.01.04, 02.02.00, 02.03.00 and 02.03.01.

## Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on Hitachi Vantara Support Connect: <https://knowledge.hitachivantara.com/Documents>.

## Changes in this release

- Added information about system requirements and specifications for SRA 02.03.01.

## Document conventions





This document uses the following typographic conventions:

Convention	Description
<b>Bold</b>	<ul style="list-style-type: none"><li>• Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example:</li></ul>



Convention	Description
	Click <b>OK</b> . <ul style="list-style-type: none"> <li>Indicates emphasized words in list items.</li> </ul>
<i>Italic</i>	<ul style="list-style-type: none"> <li>Indicates a document title or emphasized words in text.</li> <li>Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example:               <pre>pairdisplay -g group</pre>               (For exceptions to this convention for variables, see the entry for angle brackets.)             </li> </ul>
Monospace	Indicates text that is displayed on screen or entered by the user. Example: <pre>pairdisplay -g oradb</pre>
< > angle brackets	Indicates variables in the following scenarios: <ul style="list-style-type: none"> <li>Variables are not clearly separated from the surrounding text or from other variables. Example:               <pre>Status-&lt;report-name&gt;&lt;file-version&gt;.csv</pre> </li> <li>Variables in headings.</li> </ul>
[ ] square brackets	Indicates optional values. Example: [ a   b ] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a   b } indicates that you must choose either a or b.
vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [ a   b ] indicates that you can choose a, b, or nothing. { a   b } indicates that you must choose either a or b.

This document uses the following icons to draw attention to information:

Icon	Label	Description
	Note	Calls attention to important or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

## Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10 <sup>3</sup> ) bytes
1 megabyte (MB)	1,000 KB or 1,000 <sup>2</sup> bytes
1 gigabyte (GB)	1,000 MB or 1,000 <sup>3</sup> bytes
1 terabyte (TB)	1,000 GB or 1,000 <sup>4</sup> bytes
1 petabyte (PB)	1,000 TB or 1,000 <sup>5</sup> bytes
1 exabyte (EB)	1,000 PB or 1,000 <sup>6</sup> bytes

Logical capacity values (for example, logical device capacity, cache memory capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: <ul style="list-style-type: none"> <li>• OPEN-V: 960 KB</li> <li>• Others: 720 KB</li> </ul>
1 KB	1,024 (2 <sup>10</sup> ) bytes
1 MB	1,024 KB or 1,024 <sup>2</sup> bytes
1 GB	1,024 MB or 1,024 <sup>3</sup> bytes
1 TB	1,024 GB or 1,024 <sup>4</sup> bytes
1 PB	1,024 TB or 1,024 <sup>5</sup> bytes
1 EB	1,024 PB or 1,024 <sup>6</sup> bytes

## Accessing product documentation

Product user documentation is available on Hitachi Vantara Support Connect: <https://knowledge.hitachivantara.com/Documents>. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

## Getting help

[Hitachi Vantara Support Connect](https://support.hitachivantara.com/en_us/contact-us.html) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: [https://support.hitachivantara.com/en\\_us/contact-us.html](https://support.hitachivantara.com/en_us/contact-us.html).

[Hitachi Vantara Community](#) is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make

connections. **Join the conversation today!** Go to [community.hitachivantara.com](https://community.hitachivantara.com), register, and complete your profile.

## Comments

Please send us your comments on this document to [doc.comments@hitachivantara.com](mailto:doc.comments@hitachivantara.com). Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara Corporation.

**Thank you!**



## Overview

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

The following topics are discussed:

- [About Hitachi Storage Replication Adapter and Site Recovery Manager](#)
- [Command Control Interface \(CCI\)](#)
- [How the VMware® vCenter SRM™/SRA solution works](#)

# About Hitachi Storage Replication Adapter and Site Recovery Manager

VMware® vCenter Site Recovery Manager™ 5.x/6.x (VMware® vCenter SRM™) is a VMware application that automates the disaster recovery process using storage-based replication.

Hitachi Storage Replication Adapter (SRA) is an interface that integrates Hitachi storage systems and replication software with VMware® vCenter SRM™ processes.

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

## VMware vCenter infrastructure

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

- VMware vSphere, the virtualization platform with data center infrastructure. vSphere consists of:
  - 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 on the protected and recovery sites.

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

## Hitachi storage and replication software products

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

- Hitachi Virtual Storage Platform G1x00 (VSP G1x00)
- Hitachi Virtual Storage Platform F1500 (VSP F1500)
- Hitachi Virtual Storage Platform G200, G400, G600, G800 (VSP Gx00 models)
- Hitachi Virtual Storage Platform F400, F600, F800 (VSP Fx00 models)
- Hitachi Virtual Storage Platform (VSP)
- Hitachi Unified Storage (HUS)

- Hitachi Unified Storage VM (HUS VM)
- Hitachi Universal Storage Platform V/VM (USP V/VM)
- Hitachi Adaptable Modular Storage (AMS)



**Note:** A separate Hitachi NAS SRA is available for environments using NFS datastores. View related documentation by clicking: <https://www.hitachivantara.com/en-us/pdf/white-paper/hitachi-storage-replication-adapter-for-hitachi-nas-platform.pdf>.

---

Hitachi 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:

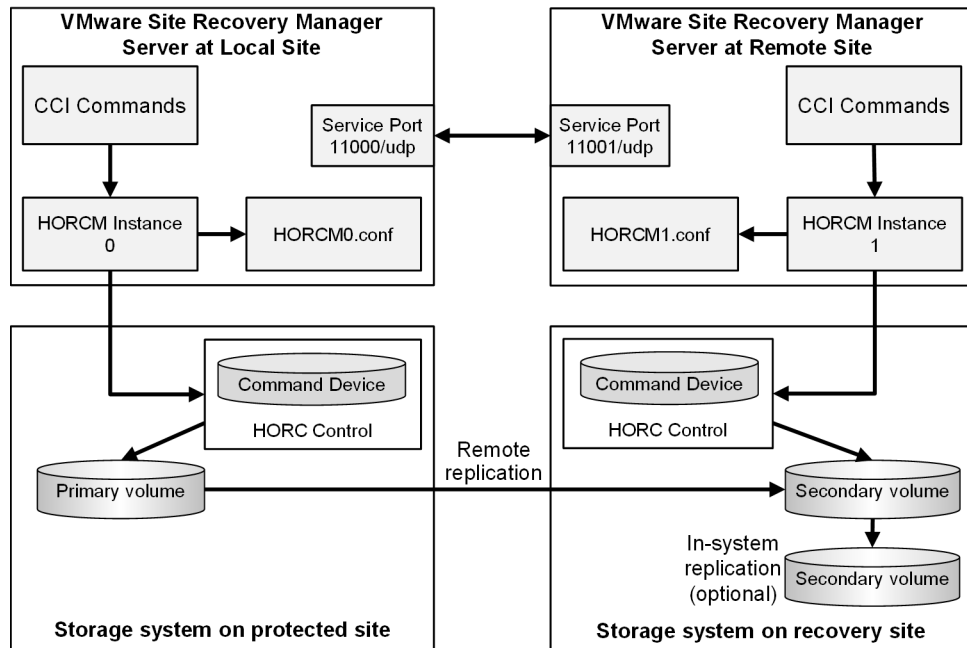
- Hitachi Universal Replicator, which provides long-distance asynchronous replication across any distance without significant impact on host performance.
- Hitachi TrueCopy Remote Replication, which provides synchronous remote replication.
- Global-active device (GAD), which provides synchronous remote replication.
- Hitachi TrueCopy Extended Distance (TCE), which provides asynchronous remote replication. TCE is used with HUS.

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

- Hitachi ShadowImage® (SI), which creates RAID-protected duplicate volumes within the storage system. With ShadowImage, you create a clone of the remote backup volume in the remote storage system.
- Hitachi Thin Image (HTI), which creates a virtual backup of a production volume from a point in time "snapshot".

Hitachi users manage storage and data replication operations using the Command Control Interface (CCI) command line interface (CLI) software product.

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



**Figure 1 VMware® vCenter SRM™ and Hitachi components**

## Command Control Interface (CCI)

Hitachi's remote and in-system replication software require CCI to manage the pairs. The adapter plug-in links CCI with Site Recovery Manager.

There are two CCI components:

- Command devices, which reside on the storage systems. CCI uses the command device as the interface to the storage system from the host. The command device accepts commands from the host and executes them on the storage system. The command device is a dedicated logical volume.
- Hitachi Open Remote Copy Manager (HORCM), which resides on the CCI server. HORCM operates as a daemon process. When activated, HORCM refers to CCI 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, CCI 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 describes the secondary volumes (S-VOLs), which are also referred to as "recovery volumes".



[Figure 1 VMware vCenter SRM and Hitachi components on page 16](#) shows a two-server, two-HORCM instance setup with optional in-system test copy.

## How the VMware® vCenter SRM™/SRA solution works

VMware® vCenter SRM™ coordinates process with Hitachi 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 in which you have specified an order that virtual machines are to be started up.

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

Finally, VMware® vCenter SRM™-supported failback (VSP G1000, VSP G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, VSP, HUS VM, and USP V/VM only) 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™ lets you 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 Hitachi Vantara account team, which will assist you as needed throughout the process. The account team coordinates Hitachi Vantara resources to ensure a successful installation and deployment. Before you begin planning, it might be useful to review the deployment workflow in [Deployment on page 31](#).

This chapter provides requirements and planning information in the following topics:

- [Requirements](#)
- [SRA/VMware® vCenter SRM™/CCI location options](#)
- [Test options](#)
- [Configurations with protected and recovery VMs on the same site](#)
- [Consistency groups and VM failover groups](#)
- [Consistency groups and same-time split operations](#)
- [About the TrueCopy fence level “Never”](#)
- [Prerequisites for global-active device configuration](#)
- [AMS 2000 host group options](#)

# Requirements

This section lists hardware and software requirements.

**Table 1 Required hardware and software**

Item	Description
Hitachi Storage Replication Adapter version	<ul style="list-style-type: none"> <li>• SRA 02.01.04—VMware® vCenter SRM™ 5.x/6.0/6.1.               <ul style="list-style-type: none"> <li>○ Supports SSH connections</li> <li>○ Supports VMware® vCenter SRM™ on one array in loopback mode, for testing only in non-production environments</li> <li>○ Requires HITACHI_RMHTCSRA_X64-02.01.4.exe</li> </ul> </li> <li>• SRA 02.02.00—VMware® vCenter SRM™ 6.1 or later.               <ul style="list-style-type: none"> <li>○ Supports CCI version 01-36-03/03 or later</li> <li>○ Supports global-active device (GAD).</li> <li>○ Requires HITACHI_RMHTCSRA_X64-02.02.00.exe</li> </ul> </li> <li>• SRA 02.03.00—VMware® vCenter SRM™ 6.5 or later.               <ul style="list-style-type: none"> <li>○ Supports CCI version 01-36-03/03 or later</li> <li>○ Supports iSCSI for VSP G1000, VSP G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, and HUS.</li> <li>○ Requires HITACHI_RMHTCSRA_X64-02.03.00.exe</li> </ul> </li> <li>• SRA 02.03.01—VMware® vCenter SRM™ 6.1 or later.               <ul style="list-style-type: none"> <li>○ Supports CCI version 01-36-03/03 or later.</li> <li>○ Supports global-active device (GAD).</li> <li>○ Supports iSCSI for VSP G1000, VSP G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, and HUS.</li> <li>○ Requires HITACHI_RMHTCSRA_X64-02.03.01.exe</li> </ul> </li> </ul>
Supported Hitachi storage systems and microcode levels	<ul style="list-style-type: none"> <li>• SRA 02.01.04—VMware® vCenter SRM™ 5.x/6.0/6.1.               <ul style="list-style-type: none"> <li>○ VSP Gx00 models firmware 83-00-xx or later</li> <li>○ VSP Fx00 models firmware 83-02-xx or later</li> <li>○ HUS VM microcode 73-01-01 or later</li> <li>○ VSP G1000 microcode 80-01-01 or later</li> <li>○ VSP microcode 70-05-xx or later</li> <li>○ USP V/VM microcode 60-07-xx or later</li> <li>○ TagmaStore USP: 50-09-xx or later TagmaStore NSC: 50-09-xx or later</li> <li>○ HUS firmware 0930/A-H or later</li> <li>○ AMS firmware 08C3/E or later</li> </ul> </li> <li>• SRA 02.02.00—VMware® vCenter SRM™ 6.1 or later.               <ul style="list-style-type: none"> <li>○ VSP Gx00 models firmware 83-01-01 or later When GAD is used: 83-04-01 or later</li> <li>○ VSP Fx00 models firmware 83-02-xx or later When GAD is used: 83-04-01 or later</li> <li>○ HUS VM microcode 73-01-01 or later</li> <li>○ VSP G1000 microcode 80-01-01 or later When GAD is used: 80-04-02 or later</li> <li>○ VSP G1500, VSP F1500 microcode 80-05-01 or later When GAD is used: 80-05-01 or later</li> <li>○ VSP microcode 70-05-xx or later</li> <li>○ USP V/VM microcode 60-07-xx or later</li> </ul> </li> </ul>

Item	Description
	<ul style="list-style-type: none"> <li>• SRA 02.03.00—VMware® vCenter SRM™ 6.5 or later. <ul style="list-style-type: none"> <li>○ VSP Gx00 models firmware 83-01-01 or later</li> <li>○ VSP Fx00 models firmware 83-02-xx or later</li> <li>○ HUS VM microcode 73-01-01 or later</li> <li>○ VSP G1000 microcode 80-01-01 or later</li> <li>○ VSP G1500, VSP F1500 microcode 80-05-01 or later</li> <li>○ VSP microcode 70-05-xx or later</li> <li>○ USP V/VM microcode 60-07-xx or later</li> <li>○ HUS firmware 0930/A-H or later</li> </ul> </li> <li>• SRA 02.03.01—VMware® vCenter SRM™ 6.1 or later. <ul style="list-style-type: none"> <li>○ VSP Gx00 models firmware 83-01-01 or later. When GAD is used: 83-04-01 or later.</li> <li>○ VSP Fx00 models firmware 83-02-xx or later When GAD is used: 83-04-01 or later</li> <li>○ HUS VM microcode 73-01-01 or later</li> <li>○ VSP G1000 microcode 80-01-01 or later When GAD is used: 80-04-02 or later</li> <li>○ VSP G1500, VSP F1500 microcode 80-05-01 or later When GAD is used: 80-05-01 or later</li> <li>○ VSP microcode 70-05-xx or later</li> <li>○ USP V/VM microcode 60-07-xx or later</li> <li>○ HUS firmware 0930/A-H or later</li> </ul> </li> </ul>
Supported operating systems	<ul style="list-style-type: none"> <li>• SRA 2.1 or earlier: Windows Server 2003 or later</li> <li>• SRA 2.2, 2.3: Windows Server 2008 or later</li> <li>• Linux</li> <li>• Solaris</li> <li>• Solaris/x86</li> <li>• HP-UX</li> <li>• AIX®</li> </ul>
VMware infrastructure	<p>Environments:</p> <ul style="list-style-type: none"> <li>• Site Recovery Manager (SRM) (can also be installed on a physical server)</li> <li>• Use SRM 5.x, SRM 6.0, SRM 6.1, and SRM 6.5</li> </ul> <p>Protected site:</p> <ul style="list-style-type: none"> <li>• VMware vCenter Server</li> <li>• ESX/ESXi host</li> <li>• Datastore on the ESX/ESXi host</li> </ul> <p>Recovery site:</p> <ul style="list-style-type: none"> <li>• VMware vCenter Server</li> <li>• ESX/ESXi host</li> <li>• 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 TC or UR is used. Do not install datastores on these volumes. In the case of GAD, secondary volumes of GAD pairs are recognized as datastores in the recovery site.</li> </ul>
CCI	<ul style="list-style-type: none"> <li>• Version 01-27-03/04 or later: Supported for VSP, HUS VM, USP V/VM, TagmaStore USP/TagmaStore NSC.</li> <li>• Version 01-30-03/03 or later: Supported for VSP G1000, VSP, HUS VM, USP V/VM, TagmaStore USP/TagmaStore NSC.</li> </ul>

Item	Description
	<ul style="list-style-type: none"> <li>Version 01-33-03/06 or later: Supported for the Hitachi storage systems listed in "Supported Hitachi storage systems and microcode levels".</li> <li>CCI must be installed on protected and recovery sites on Windows or UNIX systems. If Windows is used, CCI and VMware® vCenter SRM™ must be installed on the same server. For more information, see <a href="#">SRA/VMware® vCenter SRM™/CCI location options on page 22</a>.</li> </ul>
Remote replication	<ul style="list-style-type: none"> <li>When using VSP G1x00, VSP F1500, VSP, VSP Gx00 models, VSP Fx00 models, HUS VM, and USP V/VM, use one of the following: <ul style="list-style-type: none"> <li>TrueCopy Remote Replication</li> <li>Universal Replicator</li> <li>Global-active device (VSP G1x00, VSP F1500, VSP Gx00 models, VSP Fx00 models)</li> </ul> </li> <li>When using HUS, use one of the following: <ul style="list-style-type: none"> <li>TrueCopy Remote Replication</li> <li>TrueCopy Extended Distance</li> </ul> </li> <li>When using AMS 2000 Family, use TrueCopy Remote Replication.</li> </ul>
In-system replication license key	<p>ShadowImage, Thin Image, or Copy-on-Write Snapshot. Used for testing.</p> <ul style="list-style-type: none"> <li>Optional for VSP G1x00, VSP F1500, VSP Gx00 models, VSP Fx00 models, VSP, USP V/VM, and HUS testing</li> <li>Required for AMS testing</li> </ul>

## SRA/VMware® vCenter SRM™/CCI location options

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

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

\* SRA 2.3 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 VSP G1000, VSP G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, VSP, USP V/VM, and HUS, testing is done using either a copy of the S-VOL (recommended) or the remote S-VOL.

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

- For AMS, testing can only be done using a copy of the S-VOL.

## Using the S-VOL for testing

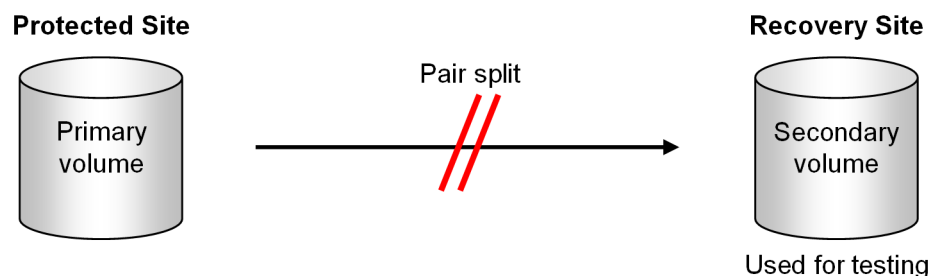
If your storage system is a VSP G1000, VSP G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, VSP, USP V/VM, or HUS, VMware® vCenter SRM™ can use the S-VOL on the remote site for test failover.

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 TrueCopy or Universal Replicator 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 46](#).

## 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.

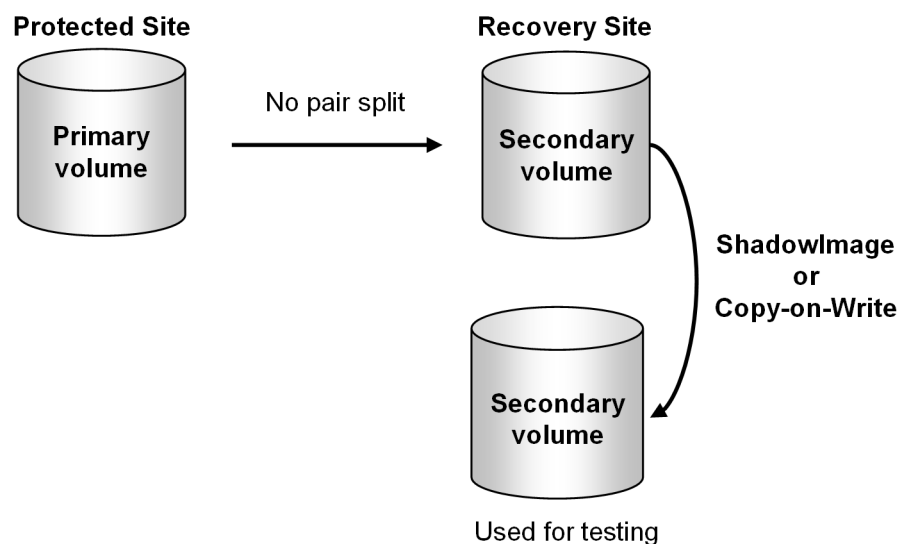
ShadowImage, Thin Image, and Copy-on-Write Snapshot are Hitachi in-system replication products available for creating copies of the S-VOL on the remote site. These products are supported for the SRA/VMware® vCenter SRM™ solution on the VSP G1000, VSP G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, VSP, USP V/VM, HUS, and AMS 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 46](#).

The following figure shows an example of test failover using a ShadowImage copy.



### ShadowImage port requirement

The ShadowImage S-VOL must be presented on the same Fibre Channel or iSCSI port as the ShadowImage 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 83](#).

## Consistency groups and VM failover groups

CCI 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

P-VOLs in the same CCI consistency group are split at the same time. In addition, you can specify a time that a split operation is to be performed on the consistency group.

This CCI 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 CCI consistency group.

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

See the TrueCopy, Universal Replicator, or global-active device user guide for your storage system for information about using consistency groups and the At-Time Split operation.

## About the TrueCopy fence level “Never”

Using “Never” for the fence level for TrueCopy 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 VM’s. This makes the fence level “Never” acceptable despite the horctakeover return of EX\_VOLCUR.

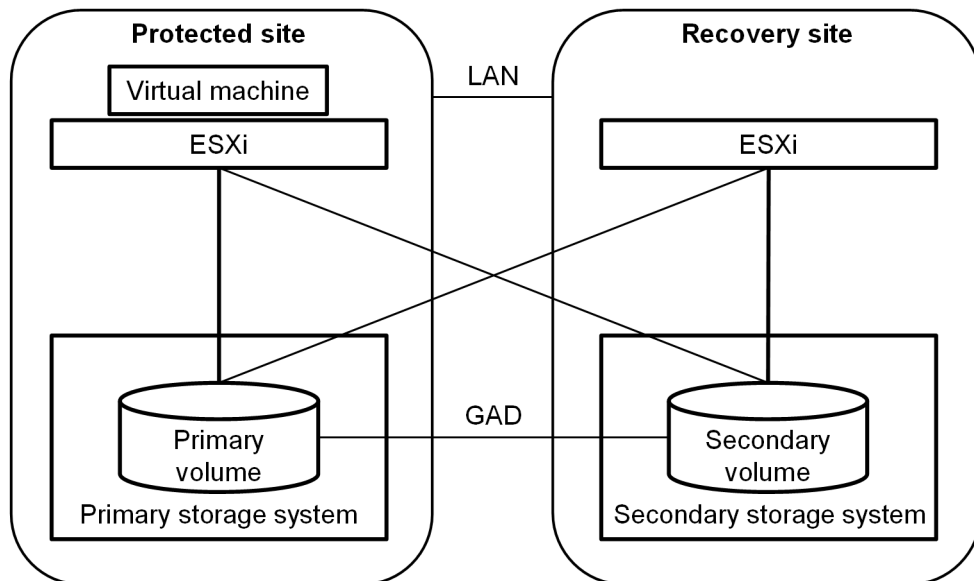
If you use “Never”, remember that the recovery will be on APP (SQL/ Exchange/Oracle/..).

## Prerequisites for global-active device configuration

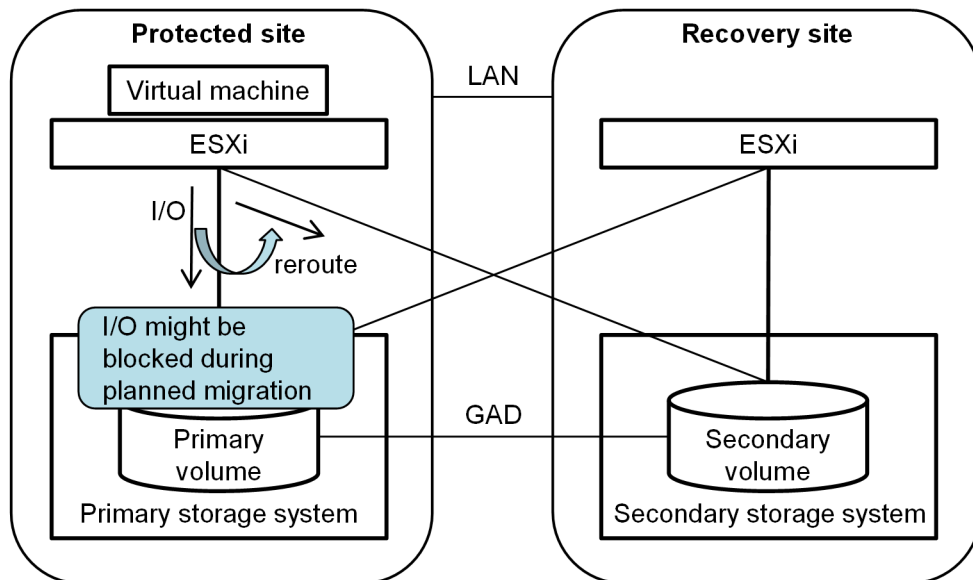
When you use global-active device (GAD) for remote replication, each ESXi host must be connected to both primary and secondary volumes as shown in the figure.

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 27](#).



**Figure 2 Connections when using GAD**



**Figure 3 I/O rerouting by multipath software**

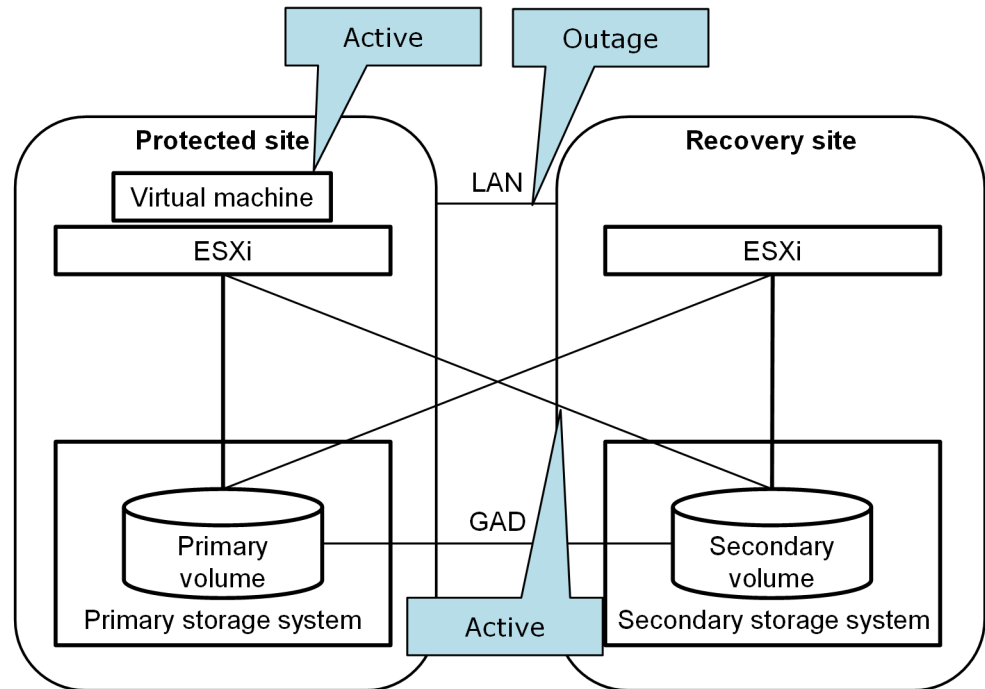
Note the following when using GAD:

- Rerouting caused by I/O blockade on primary volumes shown in [Figure 3 I/O rerouting by multipath software on page 27](#) 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.

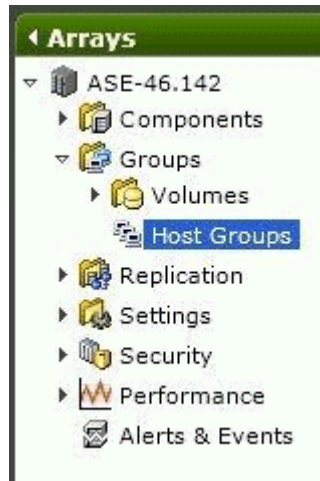


## AMS 2000 host group options

When using an AMS 2000 Family storage system, the host group options listed in the following procedure must be enabled in Storage Navigator2.

### Procedure

1. Navigate to **Arrays > Groups > Host Groups > Options** tab.



2. Ensure that the following are specified or not specified as listed:
  - Platform: VMware
  - Middleware: Not specified
  - Common Setting: Standard Mode

- Additional Setting: Enable only Unique Extended COPY Mode and Unique Write Same Mode.

Summary			
<b>Name</b>	000:G000	<b>Platform</b>	VMware
<b>Port</b>	0B	<b>Middleware</b>	not specified
<div style="display: flex; justify-content: space-between; border-bottom: 1px solid black;"> <span>WWNs</span> <span>Volumes</span> <span style="background-color: #4F81BD; color: white; padding: 2px 5px;">Options</span> </div>			
<b>Common Setting</b>		Standard Mode	
Additional Setting			
Mode Name			Mode Enable
HP-UX Mode			No
PSUE Read Reject Mode			No
Mode Parameters Changed Notification Mode			No
NACA Mode			No
Task Management Isolation Mode			No
Unique Reserve Mode 1			No
Port-ID Conversion Mode			No
Tru Cluster Mode			No
Product Serial Response Mode			No
Same Node Name Mode			No
CCHS Mode			No
NOP-In Suppress Mode			No
S-VOL Disable Advanced Mode			No
Discovery CHAP Mode			No
Unique Extended COPY Mode			Yes
Unique Write Same Mode			Yes
Unique Compare Write Mode			No
DP Depletion Detail Reply Mode			Yes
Unit Attention Change Mode			No

## Deployment

This chapter provides instructions for deploying Hitachi Storage Replication Adapter 2.0. The following topics are discussed:

- [Deployment workflow](#)
- [Installing CCI](#)
- [Creating and configuring a command device](#)
- [Setting up HORCM configuration definition files](#)
- [Starting HORCM instances, creating pairs](#)
- [Setting environment variables](#)
- [Configuring SRA for testing](#)
- [SRA installation](#)
- [Configuring SRM™ to communicate with RMSRA20 \(SRM 5.x or earlier\)](#)
- [Configuring SRM to communicate with RMSRA20 \(SRM 6.0 or later\)](#)
- [Performing reprotect and failback](#)

## Deployment workflow

The following workflow shows a 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 <a href="#">Requirements on page 20</a> .
2. Configure the storage area network	See the Hitachi whitepaper, <i>Deploying VMware Site Recovery Manager 5.0 with VMware vSphere 5.0 on Hitachi Virtual Storage Platform, Implementation Guide (3/2012)</i> .
3. Configure Hitachi remote replication using Storage Navigator. Includes storage, pair volume, port, logical path, and data path setup.	See the appropriate TrueCopy, Universal Replicator, or global-active device user guide for instructions.
4. (Optional). Configure in-system replication for testing SRA/VMware® vCenter SRM™.	See the appropriate ShadowImage or Thin Image user guide for information.
5. Install Command Control Interface (CCI) to manage storage replication.	See <a href="#">Installing CCI on page 33</a> .
6. Create and map a command device.	See <a href="#">Creating and configuring a command device on page 33</a> .
7. Set up CCI HORCM files with pair and path information.	See <a href="#">Setting up HORCM configuration definition files on page 36</a> .
8. Create pairs.	See <a href="#">Starting HORCM instances, creating pairs on page 41</a> .
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 <a href="#">SRA installation on page 47</a> .
11. Connect protected and recovery sites.	See VMware vCenter Site Recovery Manager documentation.
12. Configure SRA in Site Recovery Manager.	See <a href="#">Configuring SRM™ to communicate with RMSRA20 (SRM 5.x or earlier) on page 50</a> or <a href="#">Configuring SRM to communicate with RMSRA20 (SRM 6.0 or later) on page 56</a> .
13. Set up inventory mappings, protection group, recovery plan, perform test recovery.	See VMware vCenter Site Recovery Manager documentation.  Note: In a GAD configuration, the protection groups are created with Storage Policy base.



## Installing CCI

Command Control Interface (CCI) is a collection of executable files that you use to manage replication and data protection operations.

You run CCI 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 CCI version 01-24-03/13 or later.
- SRA 2.2 and SRA 2.3 require CCI version 01-36-03/03 or later.

For installation and upgrade instructions, see the *Hitachi Command Control Interface Installation and Configuration Guide*.

If CCI is installed on the VMware® vCenter SRM™ host, Hitachi Vantara recommends that you run HORCM as a service. (HORCM is described in [Setting up HORCM configuration definition files on page 36.](#))

## Creating and configuring a command device

A command device (CMD) is a dedicated logical device on the storage system used by CCI for communications between the host and the storage system.

The CMD allows the CCI software to send commands using in-band protocol to the storage system. One CMD is required by CCI per storage system.

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

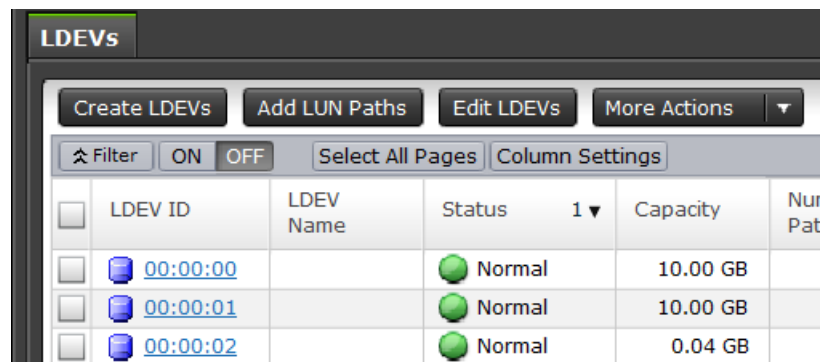
In the following procedure, you will create an LDEV, assign it as a CMD in the storage system, map it to a physical server or Windows virtual machine on the ESXi host—where VMware® vCenter SRM™ and CCI are installed, and configure it.

### Procedure

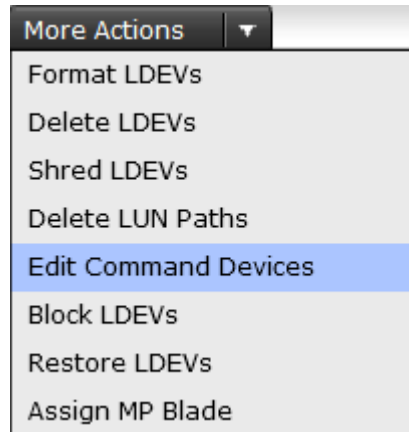
1. In the Storage Navigator **Explorer** pane, click **Storage Systems**, expand the target storage system, and then click **Logical Devices**.



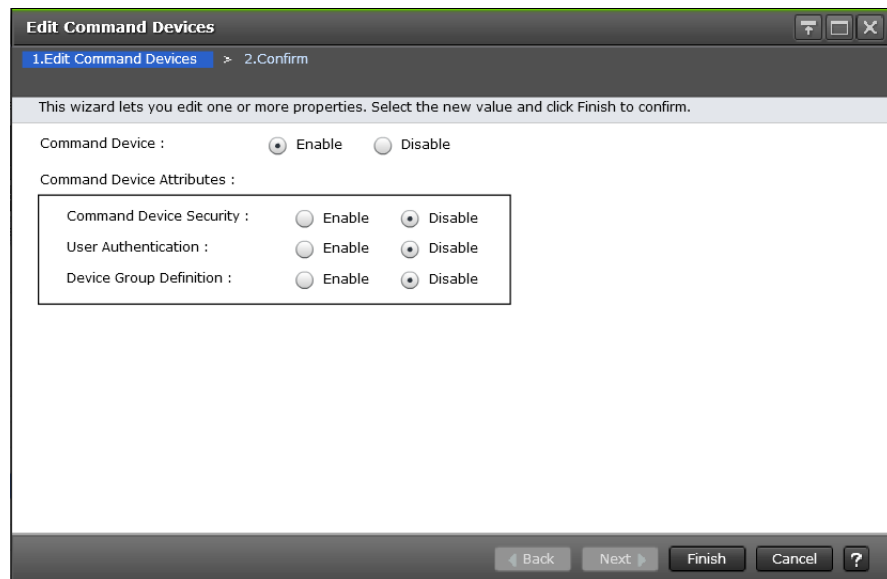
2. On the **LDEVs** tab-lower right, click **Create LDEVs** to create a new volume to be used as a command device.



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



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



6. Click **Finish**.
7. Now map the CMD volume to the CCI server (virtual or physical). If the CCI 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:
  1. In Microsoft Windows 2008, from the Server Manager menu, point to Storage and click **Disk Management**.
  2. Right-click the RDM disk and click **Online**.
  3. Right-click the RDM disk and click **Initialize Disk**.
  4. 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), the other file describes the secondary volumes (S-VOLs).

A third HORCM configuration definition file is required if you use a ShadowImage, Thin Image, or Copy-on-Write Snapshot copy of the remote site S-VOL for testing.

[Figure 1 VMware vCenter SRM and Hitachi components on page 16](#) 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 CCI command.

You can copy and modify the HORCM files included with the remote replication bundle. You will identify your pair volumes and data paths in these files.

Note the following when editing HORCM.conf files:

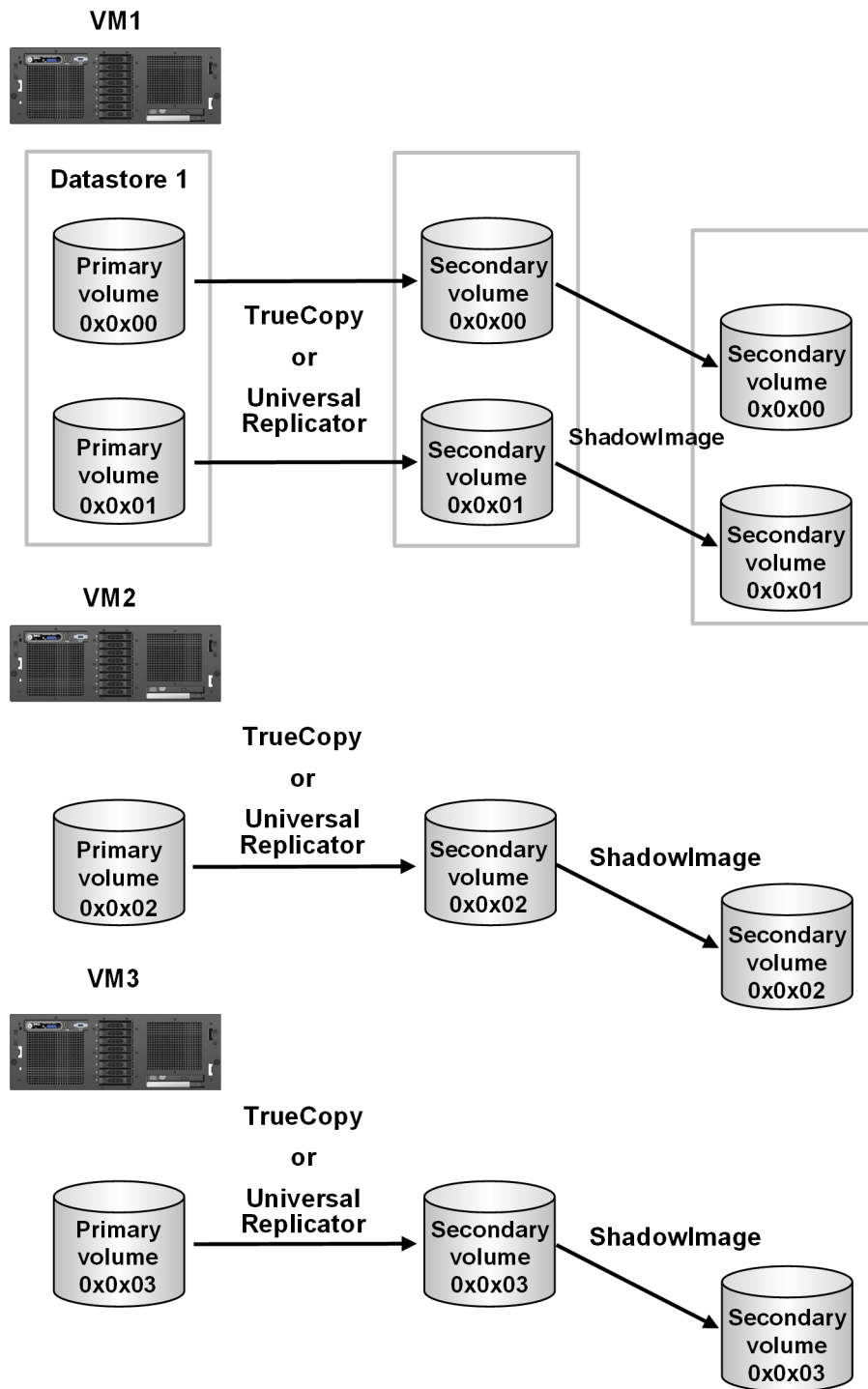
- Use a text editor to edit HORCM files. Default HORCM.conf files are located in:
  - Hitachi TrueCopy Remote Replication bundle files
  - Hitachi Universal Replicator files
  - (Optional) Hitachi ShadowImage Heterogeneous Replication files
- Save a copy of the HORCM.conf files on the local and remote CCI servers in the C:\Windows folder.
- 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 ShadowImage, Thin Image, or Copy-on-Write 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 Hitachi SRA 2.1.4 and later is supported. The HORCM\_LDEVG parameter defines the device group information that the CCI 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 *Command Control Interface User and Reference Guide* (MK-90RD7010).



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 39](#) 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#
TC_UR_SRM1     01A_01B      64015        00:1A

HORCM_INST
#dev_group      ip_address    service
TC_UR_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 ShadowImage, Thin Image, and Copy-on-Write Snapshot. You do not need to specify MU# for TC, UR, and GAD. If you want to specify MU# for TC, UR, and GAD, use MU#h0 for TC and MU#h0-h3 for UR and GAD.
- **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 40](#) 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#
TC_UR_SRM1     01A_01B      64016        00:1B
SI_SRM1        01B_01C      64016        00:1B           0

HORCM_INST
#dev_group      ip_address    service
TC_UR_SRM1     172.17.46.38 horcm0
SI_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 ShadowImage pair used for testing. The remote pair's S-VOL is the in-system pair's P-VOL. When using ShadowImage 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 TC or UR group must be defined before the SI group.
- The MU# (h0-h3) for UR and GAD devices must be specified.
- The MU# for ShadowImage 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 46](#) for instructions.



## In-system test copy HORCM file

[Example HORCM2.conf for secondary site in-system test pair on page 41](#) 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 24.](#))

### 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#
SI_SRM1         01B_01C      64016        00:1C

HORCM_INST
#dev_group      ip_address    service
SI_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.

For additional information on CCI commands and expected output, see the Command Control Interface manuals.

### 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> -IH<HORCM instance #> -fcx
```

3. On the primary server, create the TrueCopy (TC), Universal Replicator (UR), or GAD pair using the paircreate command:
  - For TC, use: **paircreate.exe -g <grp> -vl -fg <fence> <CTGID> -IH<HORCM instance #>**
  - For UR, use: **paircreate.exe -g <grp> -vl -f async -jp <journal id> -js <journal id> -IH<HORCM instance #>**
  - For GAD, use: **paircreate.exe -g <grp> -vl -fg never -jq <quorum id> -IH<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.
  - On the primary server, run **horcmshutdown.exe 0**.
  - On the recovery server, run **horcmshutdown.exe 1**.

## 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.

### Before you begin

- For ShadowImage, assign the pair to a consistency group using the **-m grp** option.

- Split mode must be set to **quick** using the command option **-fq quick**.
- ShadowImage 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 using the `pairdisplay` command.

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

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

3. Create the pair 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 ShadowImage quick split.
- For Thin Image or Copy-on-Write 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**.

## Setting environment variables

RMSRA20 requires that the following system environment variables be defined in order to make certain parameters available.

Command line examples are included. To define the variables using the GUI, see [Defining environment variables using the GUI on page 44](#).

**Table 3 Environment variables**

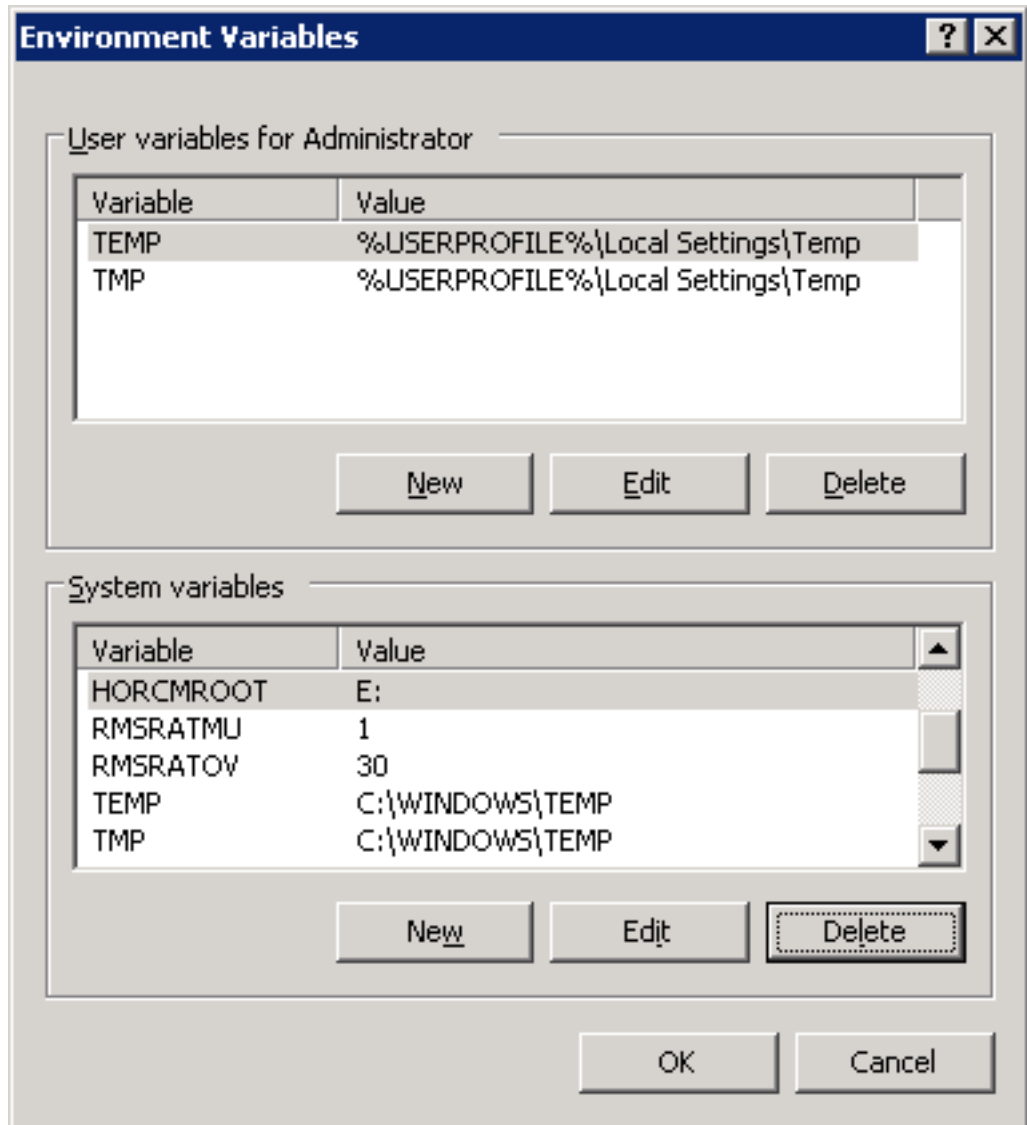
Variable	Description	Command line example
<b>HORCMROOT</b>	Used to specify the installed HORCM directory if CCI is on Windows. If CCI is not used on either the local or remote system, the C: drive is used.  If CCI is used on UNIX, HORCMROOT is not required.	To set the directory to the E: drive  C:\>setx HORCMROOT E: /m
<b>RMSRATOV</b>	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.	To the set timeout value to 30 seconds  C:\>setx RMSRATOV 30 /m
<b>RMSRATMU</b>	Used to specify 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.	To specify MU#1  C:\>setx RMSRATMU 1 /m
<b>RMSRA_MULT_CAP</b>	Used to report support for SRM "Multiple Array".	C:\>setx RMSRA_MULT_CAP 1 /m
<b>RMSRA_USE_SSH</b>	Used to specify an SSH connection instead of Telnet. For more information, see <a href="#">About SSH on page 45</a> .	C:\>setx RMSRA_USE_SSH 1 /m

## 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.

## About SSH

If SSH is available in your environment, use SSH instead of Telnet.

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 instead of Telnet. 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

## Configuring SRA for testing

Testing requires an S-VOL on which to perform testFailover. The S-VOL used for testing is set up as follows.

ShadowImage (SI), Hitachi Thin Image (HTI), and Copy-on-Write Snapshot (COW) are supported on the respective Hitachi Vantara Storage platform for this use case.

- SRA automatically searches MU#0 to test with. If you have created the SI, HTI, or COW 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 TC/UR S-VOL)  
**Note:** SplitReplication=true is not supported for GAD pairs.
  - **RMSRATMU=MUX**, where x is an unused MU number other than 0.

With these variables set, SRA would search for the SI, HTI, or COW S-VOL at MU#0, fail, and then continue the operation using the TC or UR S-VOL.

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

- If CCI is installed on the VMware® vCenter SRM™ host, then you set the environment variables on the VMware® vCenter SRM™ host.
- If CCI 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 CCI is installed on another drive (e.g. E:), then use the HORCMROOTD variable:
6. Optional: The default timeout value for failover using UR/Async is 60sec. This can be changed using RMSRATOV variable:

```
setx HORCMROOTD E: /m
```

```
setx RMSRATOV 120 /m
```

## Setting environment variables on a UNIX Host

VMware® vCenter SRM™ will telnet as root to the UNIX host to execute RMSRA20 (Hitachi SRA) commands.

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 TrueCopy pairs are suspended and utilized for testing. When testFailover is done on virtual machine 2, the ShadowImage pairs at MU#1 are suspended and used for testing.

## SRA installation

You can perform a new installation of Hitachi SRA 2.x or upgrade an existing version.

This section discusses both options.

- If you are installing a new version of SRA 2.x, continue to [Installing Hitachi SRA 2.x on page 48](#).
- If you are upgrading an existing version of SRA 2.x, you must remove it before continuing. See [Removing an earlier version of SRA on page 48](#) for instructions.

- To check your SRA version, see [Checking the SRA version on page 49](#).

## Installing Hitachi 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:
  - If using VMware® vCenter SRM™ 5.x/6.0, download HITACHI\_RMHTCSRA\_X64-02.01.4.exe.
  - If using VMware® vCenter SRM™ 6.1 or 6.5, download HITACHI\_RMHTCSRA\_X64-02.03.01.exe
- If a previous version of SRA is installed, it must be removed before installing SRA 2.x. See [Removing an earlier version of SRA on page 48](#) for instructions.
- Install SRA on the VMware® vCenter SRM™ servers on the protected and recovery sites.
- Make sure the RMSRA20 executable in the CCI installation is the latest version.

### 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 SRA installation, restart the VMware® vCenter SRM™ service.
  1. Right click **My Computer** and select **Manage**.
  2. Click **Services and Application**, then select **Services**.
  3. Locate **VMware Site Recover Manager**, then click **Restart**.

## 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.

If you are not sure, you can check the installed version; see [Checking the SRA version on page 49](#).



## Procedure

1. Open Windows **Control Panel**.
2. Click **Add or Remove Programs**.
3. Select **Hitachi 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\RMHTC
7. Right-click the Hitachi Storage Replication Adapter folder and click **Delete**. SRA is removed.

## Checking the SRA version

You can check your existing version of the Hitachi SRA on the following operating system servers:

- Windows server
- Linux server

### To check the SRA version on a Windows server

#### Procedure

1. On the Windows server that is running VMware® vCenter SRM™ and CCI, 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\RMHTC.
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 RMSRA20 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 CCI 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 CCI.
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 RMSRA20 installed with the SRA:

```
./rmsra20 -h
```

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

```
Ver&Rev: 02.01.03
```

## Configuring SRM™ to communicate with RMSRA20 (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.

Please note that the screen shots in the procedures may differ depending on your environment.

### Before you begin

- CCI 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.
- Hitachi SRA must be installed on both servers.
- The local and remote sites must be paired in VMware® vCenter SRM™.

## Procedure

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 an SRA is still not listed, then no SRA has been installed on the VMware® vCenter SRM™ host. See the procedure in [Installing Hitachi SRA 2.x on page 48](#) for information.

The screenshot shows the 'Site Recovery for Protected' interface. The 'SRAs' tab is selected and circled in red. A 'Reload SRAs' button is also circled in red. Below the tabs, there is a link 'How do I download an approved SRA?'. The main content area is titled 'RAID Manager Storage Replication Adapter' and contains the following information:

SRA:	RAID Manager Storage Replication Adapter
Status:	OK
Version:	02.00.08
Vendor:	Hitachi Disk Array
Install location:	C:/Program Files (x86)/VMware/VMware vCenter Site Recovery Manager/storage/sra/RMHTC

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

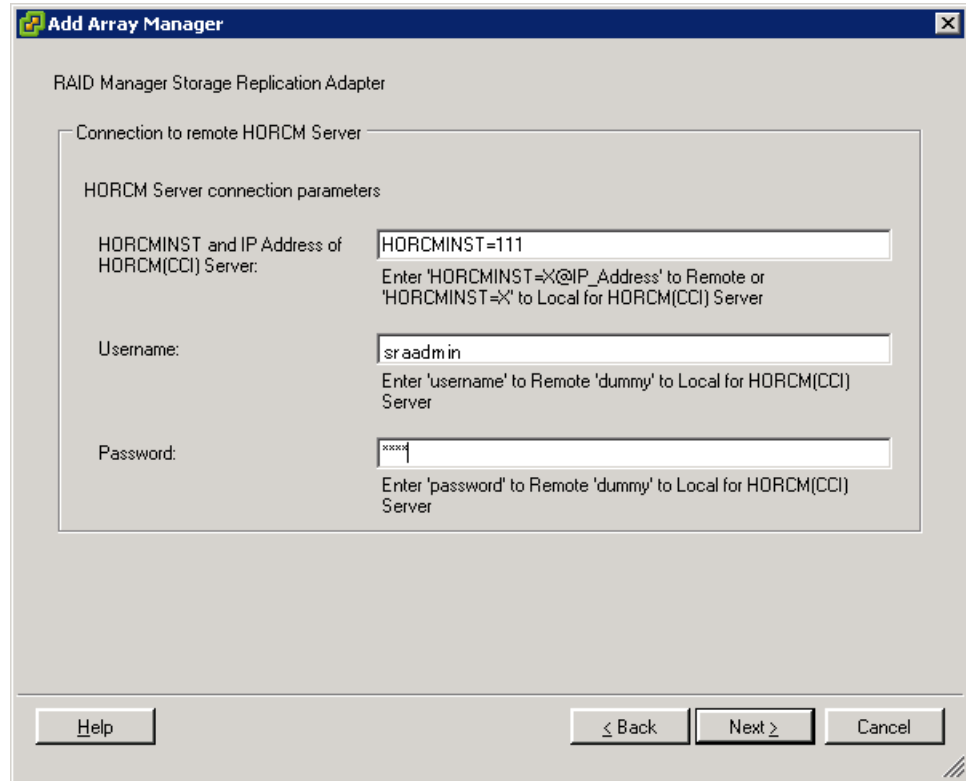
The screenshot shows the 'Add Array Manager' dialog box. The 'Array Manager Information' section is active, with the following fields:

- Display Name: Recovery
- SRA Type: RAID Manager Storage Replication Adapter

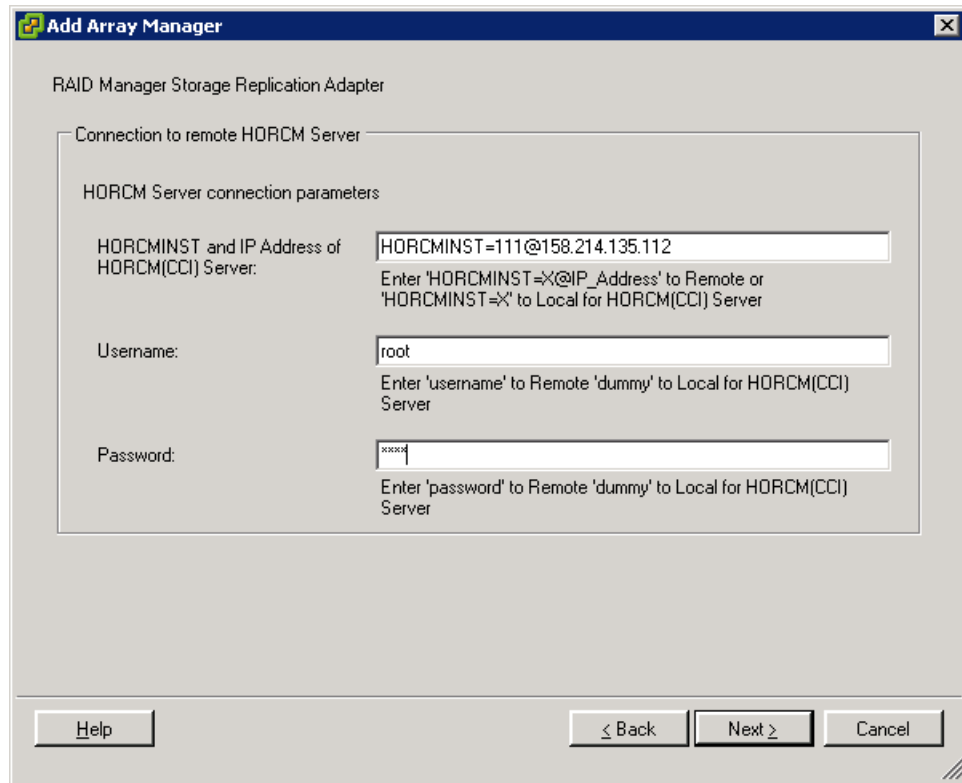
Additional information about available SRA types and versions is available on the SRAs tab of the array manager folder for each site.

Buttons at the bottom: Help, < Back, Next >, Cancel.

6. For **SRA Type**, select **RAID Manager 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(CCI) Server**, enter one of the following:
  - If CCI 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.



- If CCI 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.

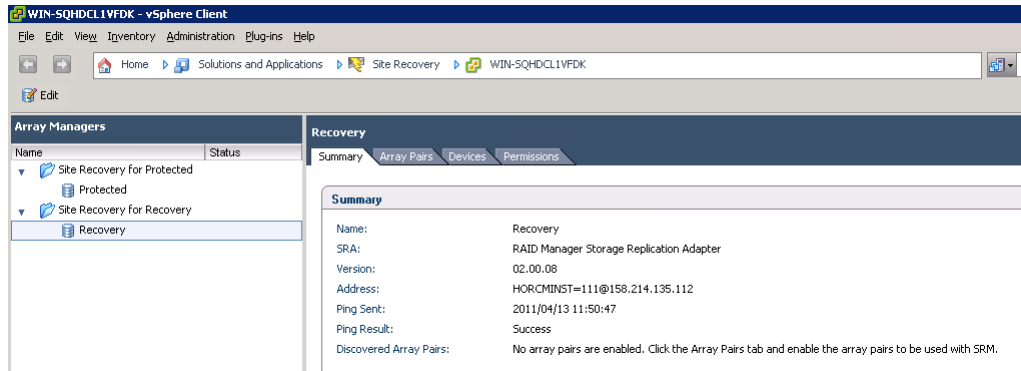


**9.** Enter a **Username** and **Password** as follows:

- If CCI 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 CCI and the command device are located on a remote UNIX server and no root user is needed for telnet use, then you must have permission for using CCI commands. See the section on changing the CCI user in *Command Control Interface User and Reference 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 RAID Manager Storage Replication Adapter.



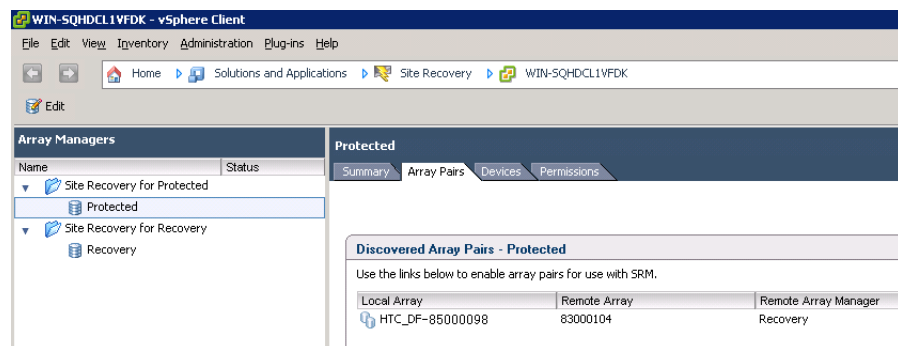
12. Repeat this procedure to configure an array adapter for the recovery site.

## 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.



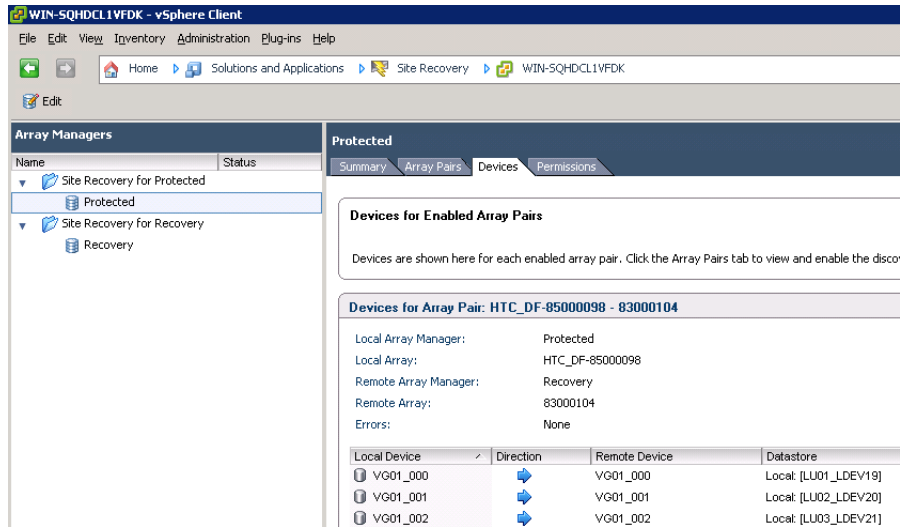
2. Verify that the **Local Array** ID and **Remote Array** ID are discovered on the array manager.
3. Click **Enable**.
4. Repeat this procedure for the recovery site array manager.

## Verifying devices

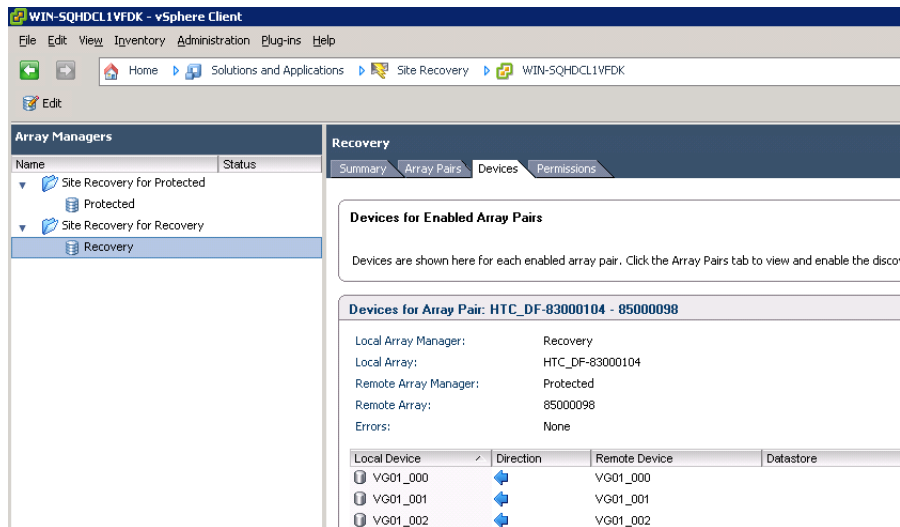
After enabling array managers, you must verify that the local and remote devices are discovered on VMware® vCenter SRM™.

### 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 RMSRA20 (SRM 6.0 or later)

To configure SRM 6.0 or later to communicate with RMSRA20, complete the following tasks:

- [Add array manager on page 56](#)
- [Check devices on page 63](#)

### 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.

Please note that the screen shots in the procedure may differ depending on your environment.

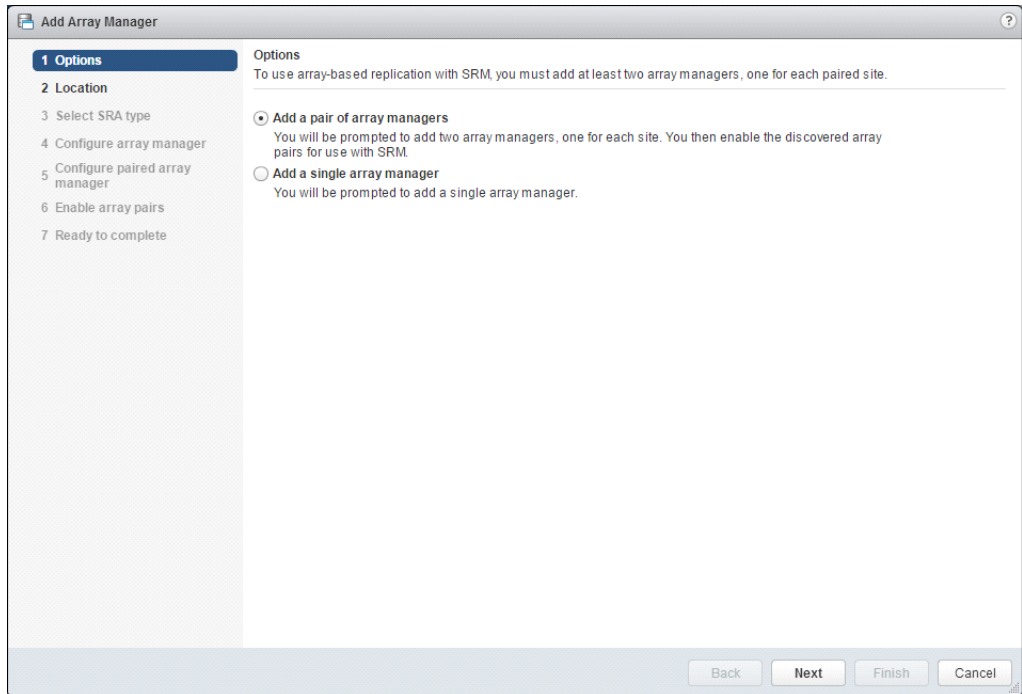
#### Before you begin

- SRM is installed at the protected site and the recovery site.
- RMSRA20 is installed in the same server as SRM at both sites.
- The protected site and the recovery site must be paired in SRM.
- CCI is installed in a correct configuration.
- All HORCM configuration definition files are defined, and HORCM instances are started.
- Remote replication has been configured.

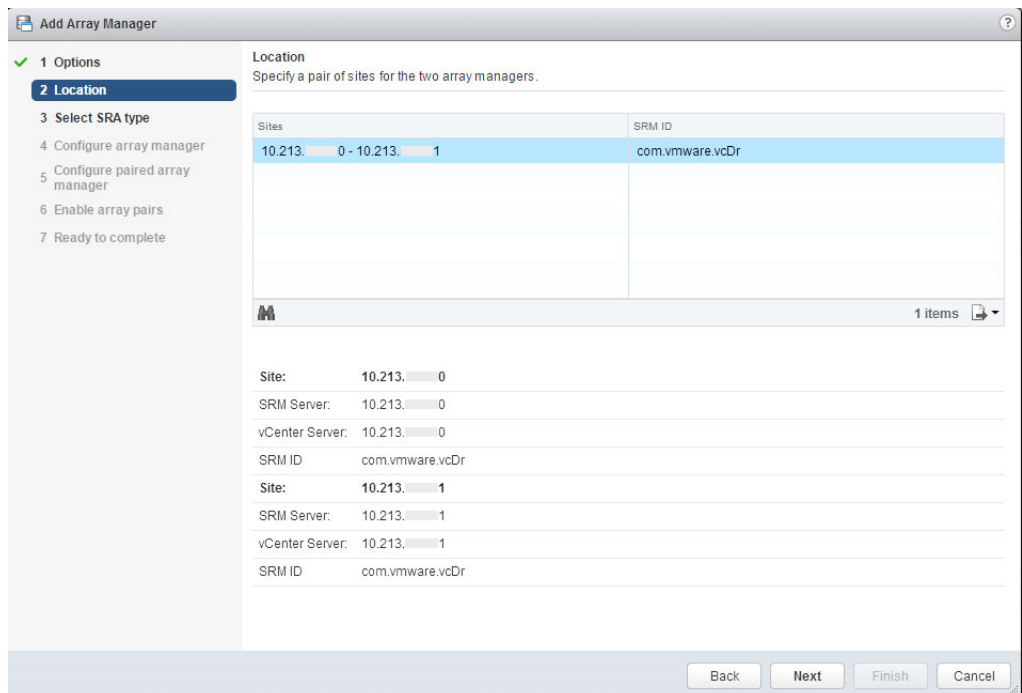
#### Procedure

1. Connect to the vCenter server at the protected site 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**.

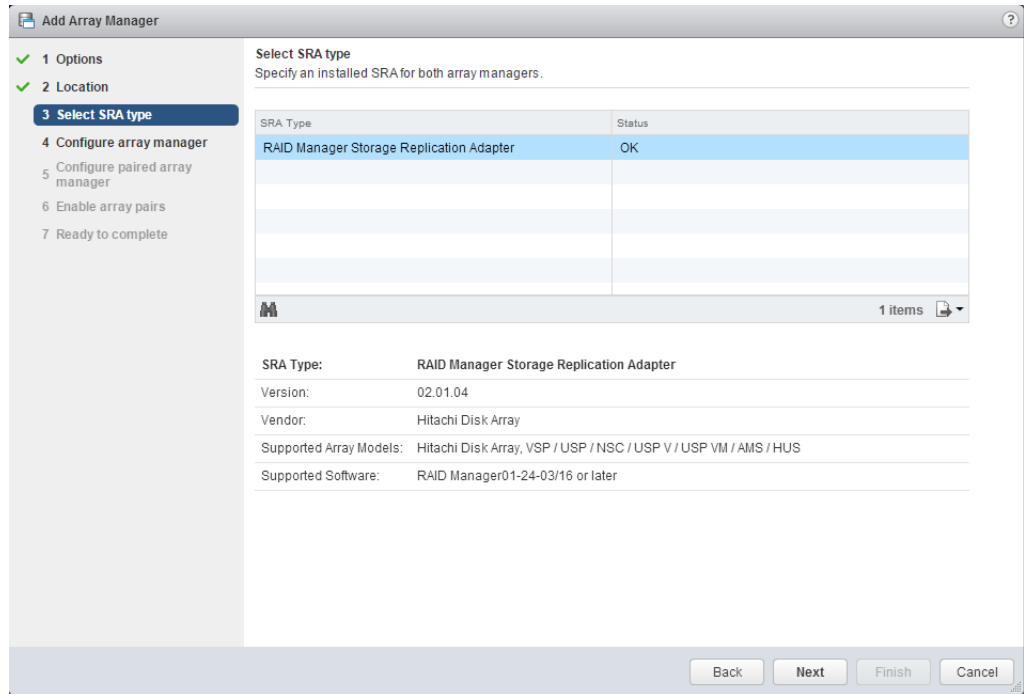




5. In **Location**, select a pair of sites and click **Next**.



6. In **Select SRA type**, select SRA type from the menu. To use a Hitachi storage system, select **RAID Manager Storage Replication Adapter**. After selecting it, click **Next**.



If RAID Manager Storage Replication Adapter is not displayed, check if RMSRA20 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(CCI) Server:** The value that should be entered depends on the configuration. Enter it as follows.
  - When Windows version of CCI is used (CCI 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 CCI is used (CCI 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 CCI server at the recovery site for X. Enter the host name or the IP address of the CCI 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 CCI 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 CCI 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 RMSRA20. 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 CCI is used:

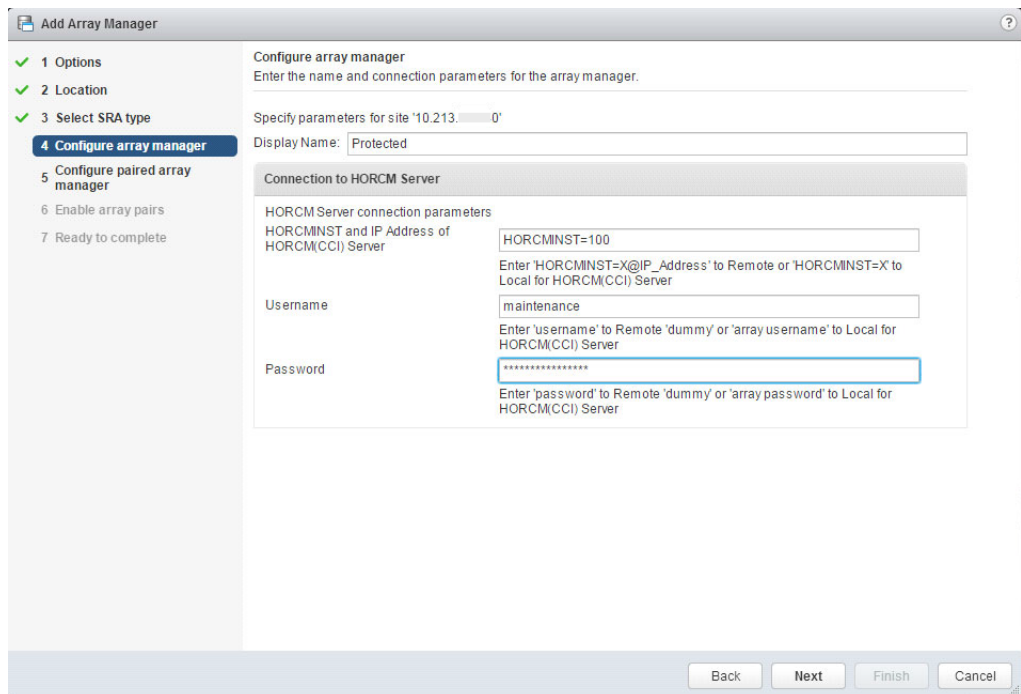
Enter the login information of the CCI server.

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

To use command device authentication, command device authentication needs to succeed in the CCI server in advance. For more information, see [Command device authentication on page 62](#).

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

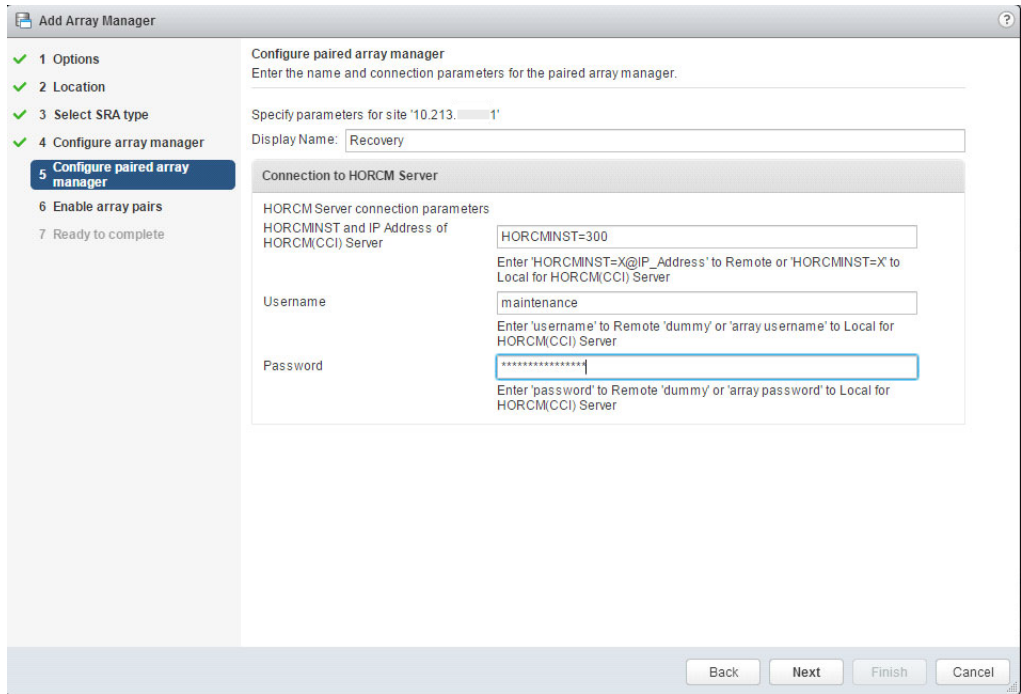
```
> setx RMSRA_TEL_WAITS "/terminal type\? /i" /m
> setx RMSRA_TEL_RESPS vt100 /m
```



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.

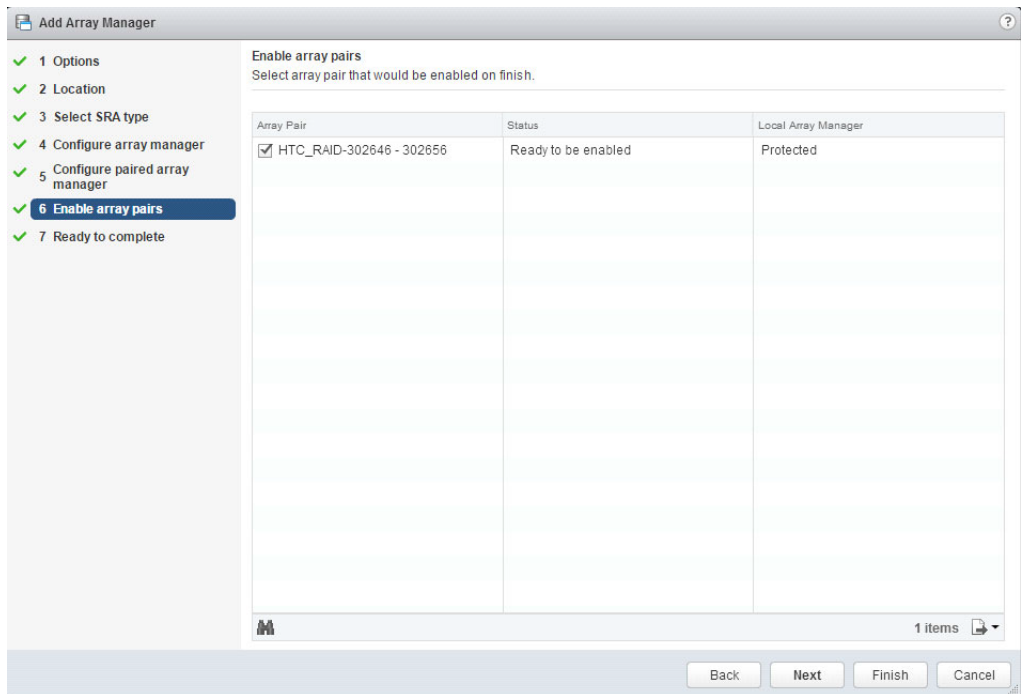
- **Display Name:** Enter (name) the array name. For example, enter "Recovery".
- **HORCMINST and IP Address of HORCM(CCI) Server:** The value that should be entered depends on the configuration. Enter it as follows.
  - When Windows version of CCI is used (CCI is installed in the SRM server): Enter "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 CCI is used (CCI 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 CCI server at the recovery site for X. Enter the host name or the IP address of the CCI 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 CCI 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 CCI 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 RMSRA20. 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 CCI is used:  
 Enter the login information of the CCI server.  
 To set information of a user who does not have the root permission, you need to give the permission to perform CCI.  
 To use command device authentication, command device authentication needs to succeed in the CCI server in advance. For more information, see [Command device authentication on page 62](#).  
 When the CCI 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
```

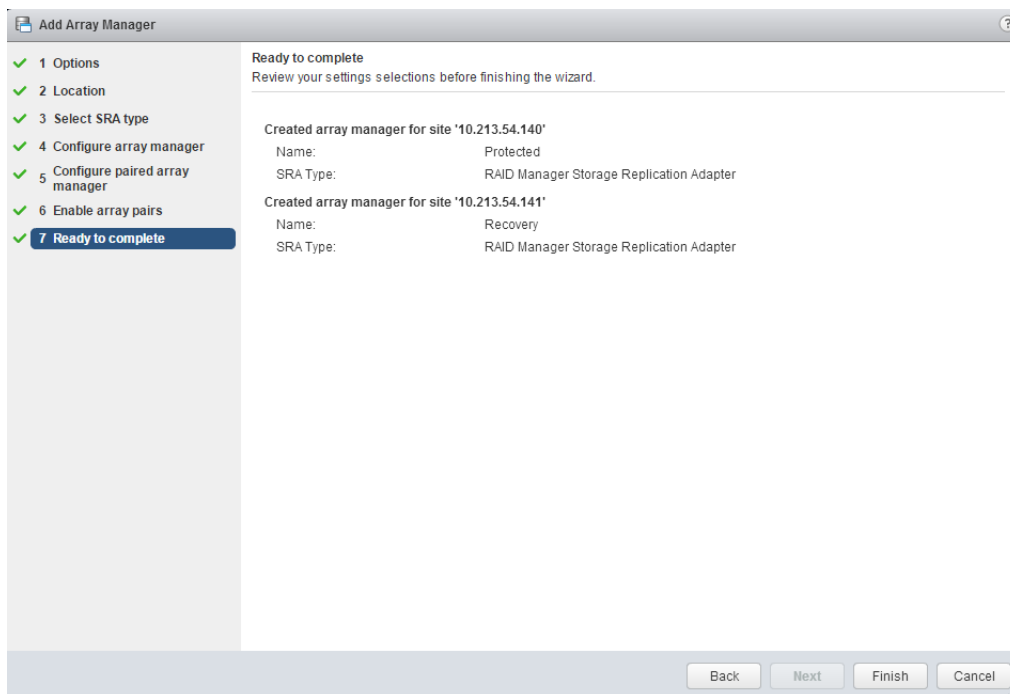


**10.** Click **Next**. In the event of an error, check the configuration and the entered values.

**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 CCI 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 properly by SRM. You can check it by using 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?

## 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 **pairdisplay -g <grp>** command. If necessary, recover the remote link and remote array.



**Note:** With AMS arrays, you must delete the remote replication and then recreate it in the reverse direction. Issue a **pairsplit -g <grp> -S** to delete the pairs, then issue the paircreate command.

---

- Re-execute the reprotect operation.



# 4

## Troubleshooting

This chapter provides information and instructions for troubleshooting configuration problems. The following topics are discussed:

- [Error messages on VMware® vCenter SRM™ log files](#)
- [Collecting information before contacting customer support](#)
- [Calling Hitachi Vantara customer support](#)

## Error messages on VMware® vCenter SRM™ log files

RMSRA20 generates error messages in the following order in the VMware® vCenter SRM™ log files:

- [XML errors received from VMware® vCenter SRM™ on page 68](#)
- [Failure to launch scripts on page 75](#)
- [Test failover errors on page 76](#)

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\

- Logs rollover after reaching 5 MB by default
- vmware-dr-index contains the most recent Log File number

## XML errors received from VMware® vCenter SRM™

The following is a list of XML errors.

### 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.

**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 TC\_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 TC\_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.

## **CCI 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 CCI 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 CCI 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 RMSRA20.
- 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 CCI 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 : pairdisplay -IH -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- [pairdisplay][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]: [qrysync\_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 pairdisplay command.

**1266 : [RMSRA20][Time]: [qrysync\_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 CCI version is correct and supports RMSRA20.

**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 pairdisplay 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 CCI version is correct and supports RMSRA20.

**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 SI or HTI and its pair status is PAIR) using the pairdisplay 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 CCI version is correct and supports RMSRA20.

**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 pairdisplay – fwe command with checkfailover/failover.
- Action: Confirm that the CCI version is correct and supports RMSRA20.

**1265 : [RMSRA20][Time]: [testfailover\_chk] : Unknown LWWN.**

- Cause: The LUN WWN could not be found in the output of the pairdisplay – fwe command with checktestfailover/testfailover.
- Action: Confirm that the CCI is the correct version supported by RMSRA20.

## Error codes for multiple errors

RMSRA20 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.

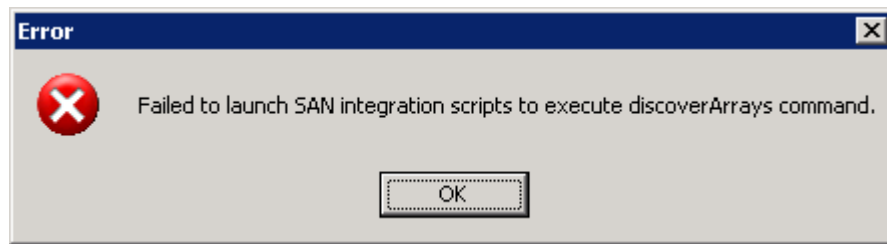
**Table 4 Error codes**

Error Codes	Error Bits	Description
1200-1255	0x000000XX	XX : exit code returned from CCI command. Refer to the CCI command error code.
1256	0x00000100	The volume is in SMPL status.
1257	0x00000200	The volume is inappropriate property as “P-VOL”

Error Codes	Error Bits	Description
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 pairdisplay command has no PWWN in the output.
1265	0x00020000	The pairdisplay command has no LUN WWN in the output.
1266	0x00040000	The pairdisplay 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
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 CCI command error

## 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 4 Error message on page 75](#).



**Figure 4 Error message**

## Correcting UNIX CCI server problems

### Procedure

1. Check that the HORCM instance is running using the command **ps -ef | grep horcm**.
2. If using telnet, check that telnet as root is allowed. From the VMware® vCenter SRM™ server, telnet to the CCI server as root.
3. Check that the correct version of RMSRA20 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@<CCI server IP>.

## Correcting Windows CCI server problems

If CCI 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**

## Test failover errors

If test failover produces errors in Prepare Storage as shown in the history screen below, perform the steps in the following procedure.

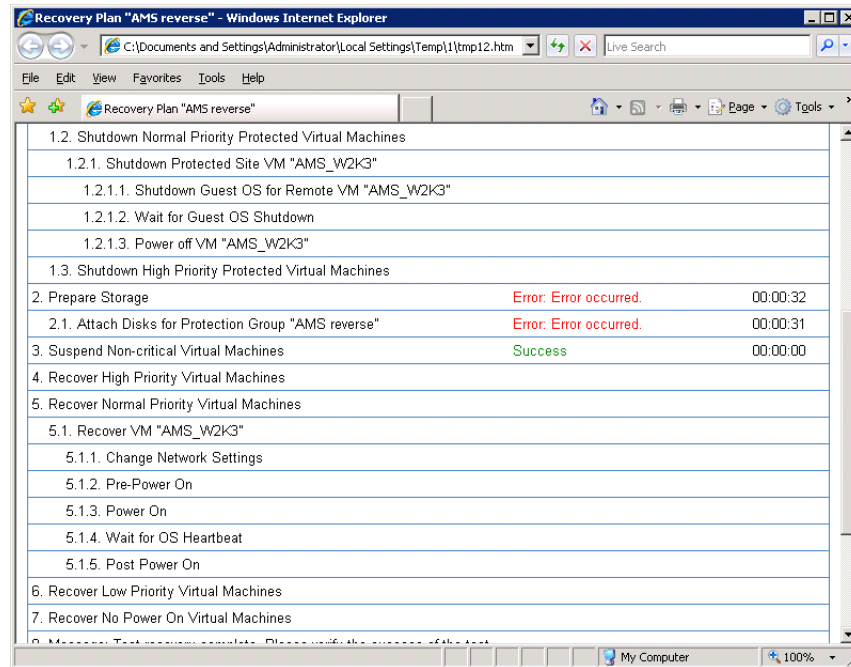


Figure 5 History screen

### Procedure

1. Check the VMware® vCenter SRM™ log on the recovery site (see the following example). Search for the XML code produced by the SRA.

#### Example: VMware® vCenter SRM™ log

```
----->
[RMSRA20] [Sun Aug 14 02:26:48 2011]: [TF_split] : true -->
[RMSRA20] [Sun Aug 14 02:26:48 2011]: [RMSRASPLIT] : true -->
[RMSRA20] [Sun Aug 14 02:26:48 2011]: [RMSRAVER] : 02.01.00 --
>
[RMSRA20] [Sun Aug 14 02:26:48 2011]: [XML_name] : failover --
>
[RMSRA20] [Sun Aug 14 02:26:48 2011]: [XML_con_id] :
HORCM_REMOTE_LOCAL
-->
[RMSRA20] [Sun Aug 14 02:26:48 2011]: [XML_con_addr] :
HORCMINST=0@172.17.26.90 -->
[RMSRA20] [Sun Aug 14 02:26:48 2011]: [XML_outfile] :
C:\Windows\TEMP\vmware-SYSTEM\sra-output-928-0 -->
[RMSRA20] [Sun Aug 14 02:26:48 2011]: [XML_statfile] :
C:\Windows\TEMP\vmware-SYSTEM\sra-status-929-0 -->
[RMSRA20] [Sun Aug 14 02:26:48 2011]: [XML_logdir] :
C:\ProgramData\VMware\VMware vCenter Site Recovery
Manager\Logs\SRAs\RMHTC -->
[RMSRA20] [Sun Aug 14 02:26:48 2011]: [XML_loglvl] : verbose
```

```

-->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_arrayId] : 53011 --
>
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_peerId] : -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [RMSRATOV] : 60 sec -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [RMSRATMU] : 0 -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [TF_split] : -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_Con_ID] :
HORCM_REMOTE_LOCAL
-->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_Con_ADR] :
HORCMINST=0@172.17.26.90 -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_DeviceKey] : 238 --
>
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_RecvPID] : -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_DeviceKey] : 242 --
>
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_RecvPID] : -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_DeviceKey] : 243 --
>
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_RecvPID] : -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_DeviceKey] : 246 --
>
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_RecvPID] : -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [horcmconn_exe] :
'/usr/bin/raidqry
-IH -l 2>/dev/null 1>/dev/null' returned with RC=0 on
HORCMINST=0.
-----

```



**Note:** In this case there is no ShadowImage or Copy-on-Write Snapshot for test failover, therefore the SplitReplication parameter must be set to true. [RMSRASPLIT]:true is logged on both the VMware® vCenter SRM™ and UNIX servers (if UNIX is used for CCI in the UNIX server root profile, see [Correcting UNIX CCI server problems on page 75](#) for more information).

2. **[RMSRASPLIT] : false** must be set. However, this must be changed to true both on the VMware® vCenter SRM™ server and the UNIX servers (if UNIX is used for CCI in the UNIX servers root profile, see [Correcting UNIX CCI server problems on page 75](#) for more information).

After corrections are made, the test is complete. XML should be similar to the following example.

**Example: VMware® vCenter SRM™ log after corrections**

```

----->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [RMSRAVER] : 02.01.00 --
>
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_name] : failover --
>
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_con_id] :
HORCM_REMOTE_LOCAL
-->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_con_addr] :

```

```

HORCMINST=0@172.17.26.90 -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_outfile] :
C:\Windows\TEMP\vmware-SYSTEM\sra-output-928-0 -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_statfile] :
C:\Windows\TEMP\vmware-SYSTEM\sra-status-929-0 -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_logdir] :
C:\ProgramData\VMware\VMware vCenter Site Recovery
Manager\Logs\SRAs\RMHTC -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_loglvl] : verbose
-->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_arrayId] : 53011 --
>
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_peerId] : -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [RMSRATOV] : 60 sec -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [RMSRATMU] : 0 -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [TF_split] : -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_Con_ID] :
HORCM_REMOTE_LOCAL
-->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_Con_ADR] :
HORCMINST=0@172.17.26.90 -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_DeviceKey] : 238 --
>
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_RecvPID] : -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_DeviceKey] : 242 --
>
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_RecvPID] : -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_DeviceKey] : 243 --
>
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_RecvPID] : -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_DeviceKey] : 246 --
>
[RMSRA20][Sun Aug 14 02:26:48 2011]: [XML_RecvPID] : -->
[RMSRA20][Sun Aug 14 02:26:48 2011]: [horcmconn_exe] :
'/usr/bin/raidqry
-IH -l 2>/dev/null 1>/dev/null' returned with RC=0 on
HORCMINST=0.
-----

```

## 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 CCI 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 (instance# for SRA):
  - set
  - %HORCMROOT%\HORCM\etc\raidqry -l
  - %HORCMROOT%\HORCM\etc\raidqry -g
  - %HORCMROOT%\HORCM\etc\pairedisplay -IH -g ??? -CLI -l -fwe (where ??? is a group name shown by **raidqry -g**)
  - %HORCMROOT%\HORCM\etc\raidscan -IH -p port(i.e. cl1-a-0) - CLI (port where connecting to ESX/ESXi server)

If ShadowImage is installed:

- %HORCMROOT%\HORCM\etc\pairedisplay -g ??? -CLI -l -few -m cas (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 CCI 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 CCI 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(instance# for SRA) on remote UNIX.
  - env
  - raidqry -l
  - raidqry -g
  - pairedisplay -IH -g ??? -CLI -l -fwe (where ??? is a group name shown by **raidqry -g**)
  - raidscan -IH -p port(i.e. cl1-a-0) -CLI (port where connecting to ESX/ESXi sever)

If ShadowImage is installed, collect the following:

- pairdisplay -g ??? -CLI -l -few -m cas (where ??? is a group name shown by raidqry -g)

## Calling Hitachi Vantara customer support

If you need to call Hitachi Vantara customer support, make sure to provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure.
- The exact content of any messages displayed on the host or Storage Navigator.
- Service information messages (SIMs), including reference codes and severity levels, displayed by Storage Navigator.
- The information collected in [Collecting information before contacting customer support on page 78](#).

The Hitachi Vantara customer support staff is available 24 hours a day, seven days a week. If you need technical support, log on to Hitachi Vantara Support Connect for contact information: [https://support.hds.com/en\\_us/contact-us.html](https://support.hds.com/en_us/contact-us.html).



## SRA Change Log

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

- [Change log for SRA](#)

## Change log for SRA

The following table provides the change log for SRA.

SRA version	command.pl revision*	Description of change
2.1.4	2.7	Initial release of SRA 2.1.4
2.1.4	2.8	Fixed the following problem: [Problem] Test failover with local replication pairs fails, if the local replication pairs use MU# other than 0 and SSH remote connection is used between SRA and CCI.
2.2	2.9	<ul style="list-style-type: none"> <li>Added support for global-active device (GAD) and VSP Fx00 models.</li> <li>Discontinued support for TagmaStore USP, TagmaStore NSC, and Adaptable Modular Storage.</li> <li>Deprecated the iSCSI protocol supporting HUS.</li> </ul>
2.3	2.9	<ul style="list-style-type: none"> <li>Added iSCSI support as the protocol for the connection between the storage system (VSP G1000, VSP G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, and HUS) and VMware ESXi.</li> <li>Discontinued support for the telnet protocol for UNIX version of CCI.</li> </ul>
2.3.1	2.9	<ul style="list-style-type: none"> <li>Added support for the GAD configuration in VMware Site Recovery Manager 6.5 environment.</li> <li>Fixed the following problem:               <ul style="list-style-type: none"> <li>[Problem] When "Planned Migration" is performed in the GAD configuration, the error message of "Unexpected element 'Identity' found" appears, and "Prepare storage for migration at protected site" process ends abnormally.</li> <li>This problem might occur when all the following conditions 1) and 2) are met, and "Planned Migration" is performed.                   <ol style="list-style-type: none"> <li>"Disaster Recovery" was performed after a failure had occurred on the protected site.</li> <li>The protected site recovered from the failure after condition 1.</li> </ol> </li> </ul> </li> </ul>
<p>*Note: The revision is described in the header of the <code>command.pl</code> file. The <code>command.pl</code> file is located in <code>&lt;SRM install directory&gt;\storage\sra\RMHTC</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. The following topics are discussed:

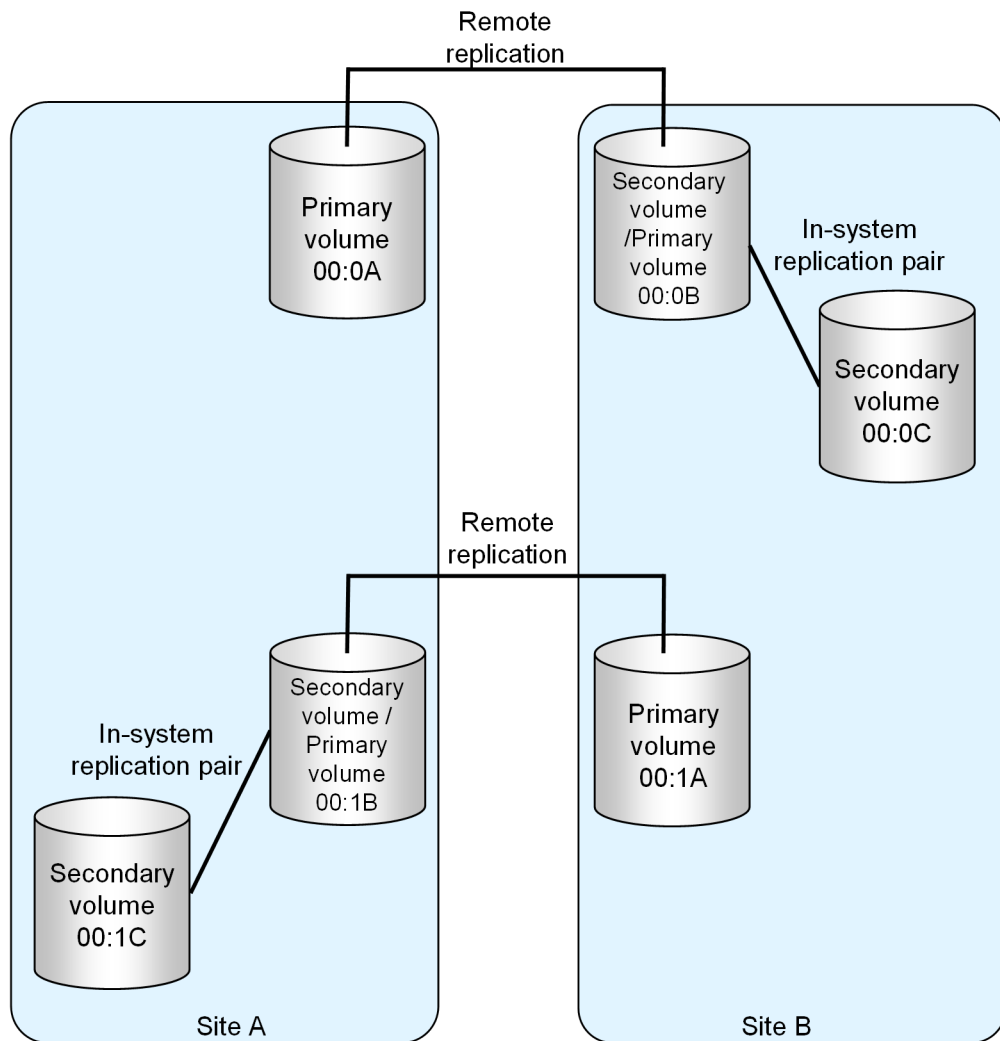
- [Protecting both sites](#)
- [HORCM definition file setup](#)

## 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
TC_UR_SRM1      01A_01B      64015        00:0A
#Replication Site B to Site B
TC_UR_SRM2      01B_01A      64015        00:1B
#CoW or SI copy for testfailover
SI_SRM2         SI_01B_01C   64015        00:1B          0

HORCM_INST
#dev_group      ip_address    service
TC_UR_SRM1      172.17.46.39 horcm1
TC_UR_SRM2      172.17.46.39 horcm1
SI_SRM2         172.17.46.38 horcm3
```

### Site A SI/COW 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#
SI_SRM2         SI_01B_01C   64015        00:1C

HORCM_INST
#dev_group      ip_address    service
SI_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
TC_UR_SRM1      01A_01B      64016      00:0B
#Replication Site B to Site A
TC_UR_SRM2      01B_01A      64016      00:1A
#CoW or SI copy for testfailover
SI_SRM1      SI_01B_01C      64016      00:0B      0

HORCM_INST
#dev_group      ip_address      service
TC_UR_SRM1      172.17.46.39      horcm0
TC_UR_SRM2      172.17.46.39      horcm0
SI_SRM1      172.17.46.39      horcm2

```

### Site B SI/COW 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#
SI_SRM1      SI_01B_01C      64016      00:0C

HORCM_INST
#dev_group      ip_address      service
SI_SRM1      172.17.46.39      horcm1

```

# Index

- A**
  - AMS
    - host group requirement 28
  - array managers
    - configuring 50
    - enabling 54
  - At-Time Split operation
    - planning 23
  
- C**
  - Command Control Interface (CCI) 16
    - consistency groups 25
    - installing 33
    - location options 22
    - overview 13
    - splitting pairs 25
  - command device
    - configuring 33
    - creating 33
  - command device authentication 62
  
- D**
  - deployment workflow 32
  
- E**
  - environment variables settings 43
  
- G**
  - global-active device
    - configuration prerequisites 26
  
- H**
  - HORCM
    - creating pairs 41
    - creating test copy 42
    - editing HORCM.conf files 36
    - setting up HORCM configuration definition files 36
  
- I**
  - starting an instance 41
  - in-system replication 23
  
- R**
  - Recovery
    - failback 64
    - failover operation 64
    - reprotect 64
  - Requirements
    - operating systems 20
    - server locations for SRA/SRM/CCI 20
    - supported micro code levels 20
    - supported replication software 20
    - Unix host 20
  
- S**
  - ShadowImage
    - port requirement 24
    - splitting pairs 25
  - SRA
    - checking version 49
    - configuring 46
    - installing 47
    - overview 14
    - removing SRA version 48
    - replication support 14
    - storage support 14
    - storage, replication software products 14
    - version 20
  - SRA/SRM
    - location options 22
    - setup workflow 32
  - SRM
    - XML errors 68
  - SRM host
    - setting variables 46
  - SRM/SRA
    - how it works 17

**T**

- testing
  - creating copy 42
  - setting environment variables 43
- troubleshooting 67
- TrueCopy
  - fence level 26

**U**

- Unix host
  - setting variables 47
  - upgrading CCI 33
- UNIX systems 62

**V**

- verifying devices 54
- VMware environment 20

**X**

- XML errors 68





## Hitachi Vantara



Corporate Headquarters  
2845 Lafayette Street  
Santa Clara, CA 95050-2639 USA  
[www.HitachiVantara.com](http://www.HitachiVantara.com)  
[community.HitachiVantara.com](http://community.HitachiVantara.com)

Regional Contact Information  
Americas: +1 866 374 5822 or [info@hitachivantara.com](mailto:info@hitachivantara.com)  
Europe, Middle East and Africa: +44 (0) 1753 618000 or [info.emea@hitachivantara.com](mailto:info.emea@hitachivantara.com)  
Asia Pacific: +852 3189 7900 or [info.marketing.apac@hitachivantara.com](mailto:info.marketing.apac@hitachivantara.com)