HITACHI
Inspire the Next

Hitachi Storage Replication Adapter

2.5.0

VMware® vCenter Site Recovery Manager™ Deployment Guide

This document provides deployment and implementation information for using the VMware® vCenter Site Recovery Manager™ software with Hitachi Storage Replication Adapter.

Contents

Contents

Contents

Preface

This document provides deployment and implementation information for VMware® vCenter Site Recovery Manager™ (SRM) 5.*x*, 6.*x*, and 8.*x* using Hitachi Storage Replication Adapter (SRA) 2.*x*.

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

Intended audience

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

Readers of this document should be familiar with the following:

- Hitachi Vantara storage management tools, including the Command Control Interface (CCI) software

- The VMware vCenter Site Recovery Manager software

- Windows® systems

- If a Linux server is intended for use as a CCI server, working knowledge of Linux system administration

Product version

This document revision applies to Hitachi Storage Replication Adapter version 2.5 and RAID Manager Storage Replication Adapter (RMSRA20) versions 02.01.0, 02.01.03, 02.01.04, 02.02.00, 02.03.00, 02.03.01, and 02.05.0*x*.

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 the Hitachi Vantara Support Website: https://knowledge.hitachivantara.com/Documents.

Changes in this release

- Updated information for MU# for UR and GAD (CTG) in the primary HORCM file (Primary HORCM file (on page 31)).

- Added the list of available characters for the username and password when adding an array manager (Add array manager (SRM v8.2 or later) (on page 51)).

- Updated information about the procedure for planned Failover with SRM to Site3 in the GAD+UR+SRM restrictions (on page 79).

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	- Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. - Indicates emphasized words in list items.
Italic	- Indicates a document title or emphasized words in text. - Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: `pairdisplay -g group` (For exceptions to this convention for variables, see the entry for angle brackets.)
Monospace	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`
< > angle brackets	Indicates variables in the following scenarios: - Variables are not clearly separated from the surrounding text or from other variables. Example: `Status-<report-name><file-version>.csv` - Variables in headings.
[ ] 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.

Convention	Description
| 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 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1,000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1,000^3$ bytes
1 terabyte (TB)	1,000 GB or $1,000^4$ bytes
1 petabyte (PB)	1,000 TB or $1,000^5$ bytes
1 exabyte (EB)	1,000 PB or $1,000^6$ 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: ▪ OPEN-V: 960 KB ▪ Others: 720 KB
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1,024^2$ bytes
1 GB	1,024 MB or $1,024^3$ bytes
1 TB	1,024 GB or $1,024^4$ bytes
1 PB	1,024 TB or $1,024^5$ bytes
1 EB	1,024 PB or $1,024^6$ bytes

Accessing product documentation

Product user documentation is available on the Hitachi Vantara Support Website: 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

The Hitachi Vantara Support Website is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website for contact information: 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, register, and complete your profile.

Comments

Please send us your comments on this document to 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 LLC.

Thank you!

Chapter 1: Overview

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

About Hitachi Storage Replication Adapter and Site Recovery Manager

The VMware® vCenter Site Recovery Manager™ 5.x/6.x/8.x (VMware® vCenter SRM™)
software is a VMware application that automates the disaster recovery process using
storage-based replication. Hitachi Storage Replication Adapter (SRA) is the 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
  includes:

  - VMware ESX/ESXi host, which is a virtualization platform that provides a data center
    infrastructure in which many virtual machines share hardware resources from a single
    physical machine. The ESX/ESXi host loads directly on a physical server.

  - vCenter Server, which provides management of one or multiple vSphere environments.

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

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

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 5000 series (VSP 5000 series)

- Hitachi Virtual Storage Platform G1x00 (VSP G1x00) and Hitachi Virtual Storage Platform F1500 (VSP F1500)

- Hitachi Virtual Storage Platform (VSP)

> 📄 **Note:** For the latest information about Hitachi storage systems supported by SRA, see the VMware Compatibility Guide on the VMware website.

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.

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 the basic VMware® vCenter SRM™/SRA components.
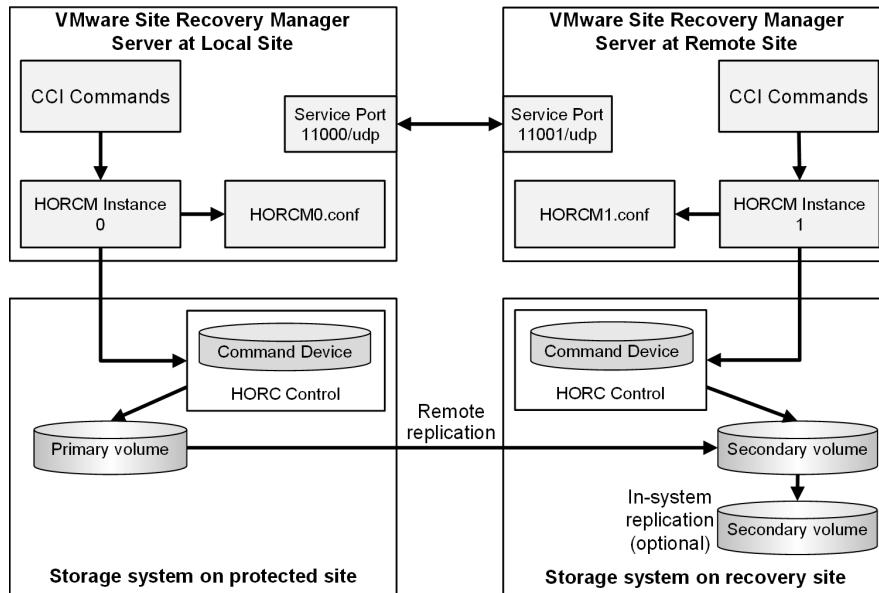
Figure 1 VMware® vCenter SRM™ and Hitachi components

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 (SRM).

There are two CCI components:

- CCI 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 CCI commands from the host and executes them on the storage system. The command device is a dedicated logical volume.

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

- Hitachi Open Remote Copy Manager (HORCM), which resides on the CCI server. HORCM operates as a daemon process. When activated, HORCM refers to the 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 file describes the secondary volumes (S-VOLs), which are also referred to as "recovery volumes".

shows a two-server, two-HORCM-instance setup with optional in-system test copy.

How the VMware® vCenter SRM™/SRA solution works

The VMware® vCenter SRM™ software coordinates processing with 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 that specifies the order in which the virtual machines are to be started up.

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

Finally, VMware® vCenter SRM™-supported failback (VSP 5000 series, VSP G1x00, VSP F1500, VSP G/F350, G/F370, G/F700, G/F900, VSP G200, G/F400, G/F600, G/F800, and VSP) and reprotect operations allow you to restore protection back to the original configuration, with data flow from the protected site to the recovery site.

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

Chapter 2: 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, please review the deployment workflow in .

Requirements

Table 1 Required hardware and software

Item	Description
Hitachi Storage Replication Adapter version	SRA 02.05.0*x*—VMware® vCenter SRM™ 6.1 or later: ▪ Supports CCI version 01-46-03/02 or later. ▪ Supports global-active device (GAD). ▪ Supports iSCSI for VSP 5000 series, VSP G1x00, VSP F1500, VSP G/F350, G/F370, G/F700, G/F900, and VSP G200, G/F400, G/F600, G/F800. ▪ Requires HITACHI_RMHTCSRA_X64-02.05.00.exe or HITACHI_RMHTCSRA_X64-02.05.00.gz or later.
Supported Hitachi storage systems	SRA 02.05.0x—VMware® vCenter SRM™ 6.1 or later: ▪ VSP 5000 series: 90-01-02 or later ▪ VSP G1000: 80-01-01 or later When GAD is used: 80-04-02 or later ▪ VSP G1500, VSP F1500: 80-05-01 or later When GAD is used: 80-05-01 or later ▪ VSP: 70-05-*xx* or later

Item	Description
	📄 **Note:** Refer to the VMware official website for supported storage.
Supported operating systems	▪ Windows Server 2008 and later: SRA 2.2 and later ▪ Linux ▪ Solaris ▪ Solaris/x86 ▪ HP-UX ▪ AIX®
VMware infrastructure	Environments: ▪ SRM (can also be installed on a physical server). ▪ Use SRM 6.5, SRM 8.1, or SRM 8.2. Protected site: ▪ VMware vCenter Server ▪ ESX/ESXi host ▪ Datastore on the ESX/ESXi host Recovery site: ▪ VMware vCenter Server ▪ ESX/ESXi host ▪ Datastores: You do not need to create datastores in the recovery site. However, two volumes with the same capacity as the datastore of the primary ESX/ESXi host are required. The volumes must be mapped to the recovery ESX/ESXi host only when 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.
CCI	CCI must be installed on Windows or UNIX systems at the protected site and recovery site. If Windows is used, CCI and VMware® vCenter SRM™ must be installed on the same server. For more information, see <u>SRA/VMware® vCenter SRM™/CCI location options (on page 17)</u>. Version 01-27-03/04 or later: Supports VSP. Version 01-30-03/03 or later: Adds support for VSP G1000. Version 01-33-03/06 or later: Adds support for VSP G1500 and VSP F1500.

Chapter 2: Requirements, planning, and prerequisites

Item	Description
	Version 01-46-03/02 or later: Adds support for VSP G/F350, G/F370, G/F700, G/F900. 01-51-03/02 or later: Adds support for VSP 5000 series.
Remote replication	For VSP 5000 series, VSP G1x00, VSP F1500, VSP, VSP G/F350, G/F370, G/F700, G/F900, VSP G200, G/F400, G/F600, G/F800, use one of the following: For VSP 5000 series, VSP F1500, and VSP, use one of the following: ▪ TrueCopy Remote Replication ▪ Universal Replicator ▪ Global-active device
In-system replication	ShadowImage, Thin Image, or Copy-on-Write Snapshot. Used for testing: ▪ Optional for VSP 5000 series, VSP G1x00, VSP F1500, VSP, VSP G/F350, G/F370, G/F700, G/F900, and VSP G200, G/F400, G/F600, G/F800

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 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.

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 5000 series, VSP G1x00, VSP F1500, VSP, VSP G/F350, G/F370, G/F700, G/F900, and VSP G200, G/F400, G/F600, G/F800, testing is done using either a copy of the S-VOL (recommended) or the remote S-VOL.

Chapter 2: Requirements, planning, and prerequisites

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

Using the S-VOL for testing

For VSP 5000 series, VSP G1x00, VSP F1500, VSP G/F350, G/F370, G/F700, G/F900, VSP G200, G/F400, G/F600, G/F800, and VSP, 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.

Protected Site   **Recovery Site**

Primary volume — Pair split → Secondary volume
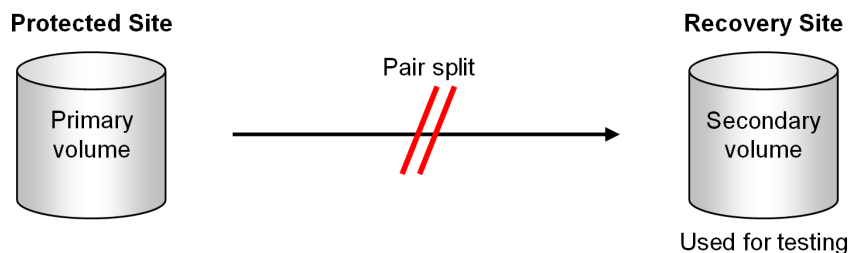
Used for testing

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 .

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 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 5000 series, VSP G1x00, VSP F1500, VSP G/F350, G/F370, G/F700, G/F900, VSP G200, G/F400, G/F600, G/F800, and VSP 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 44).

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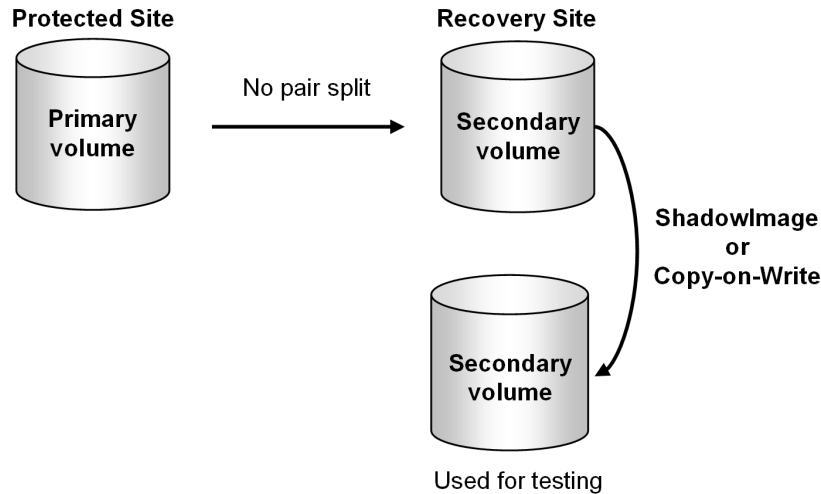
ShadowImage port requirement

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 70).

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

All P-VOLs in the same CCI consistency group can be split at the same time. In addition, you can specify the time the split operation is to be performed on the consistency group. This 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 VMs. This makes the fence level "Never" acceptable despite the horctakeover return of EX_VOLCUR.

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

Prerequisites for 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 2 Connections when using GAD
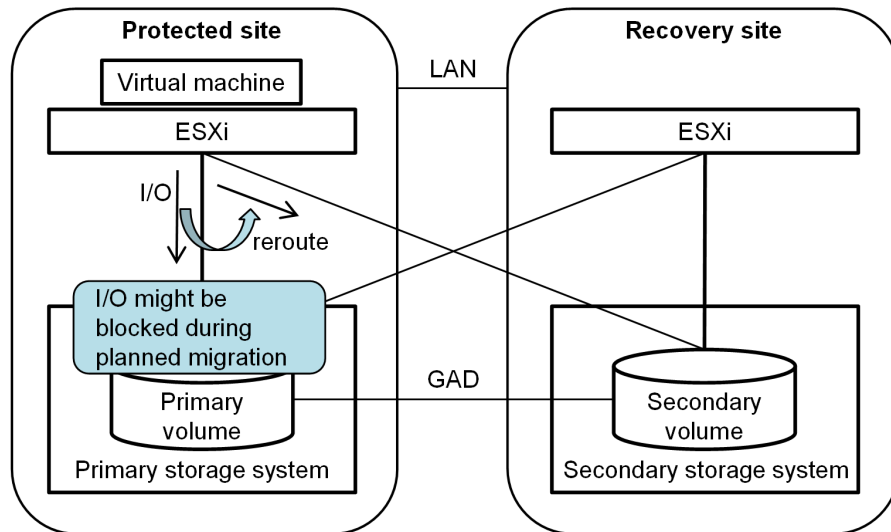
Figure 3 I/O rerouting by multipath software

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 21) 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.
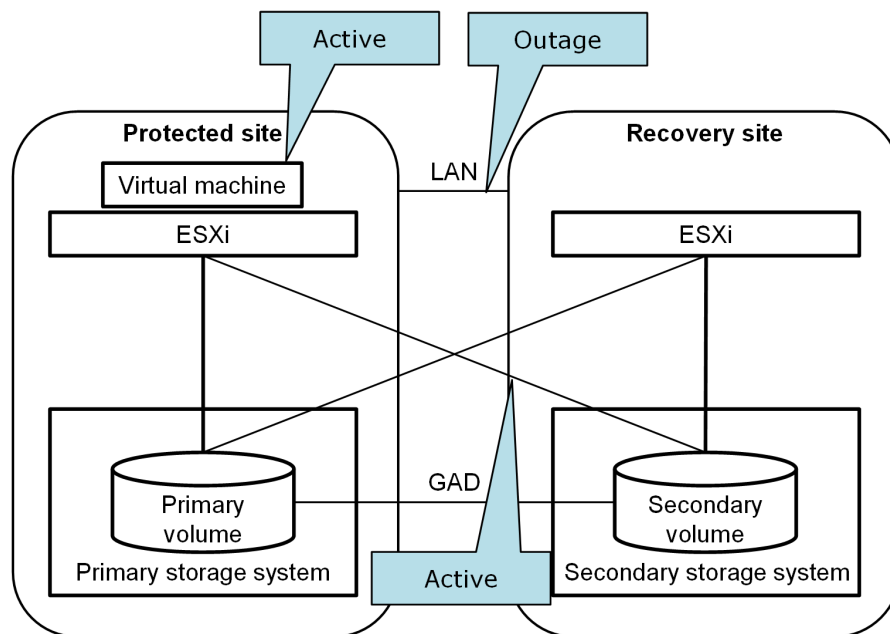
Chapter 3: Deployment

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

Supported SRM/SRA configurations

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

The following table lists the supported SRM/SRA versions.

SRM Version	SRA Version	Supported configurations
SRM 8.1 and earlier	SRA 2.3.1 and earlier	Configurations 1 and 2
SRM 8.2	SRA 2.5	Configurations 1, 2, and 3*
SRM 8.3 and later	SRA 2.5	Configuration 3*
For SRM 8.2 and later, Configuration 3 is the configuration used by SRM appliances.		

The following images show the deployment example for each configuration.
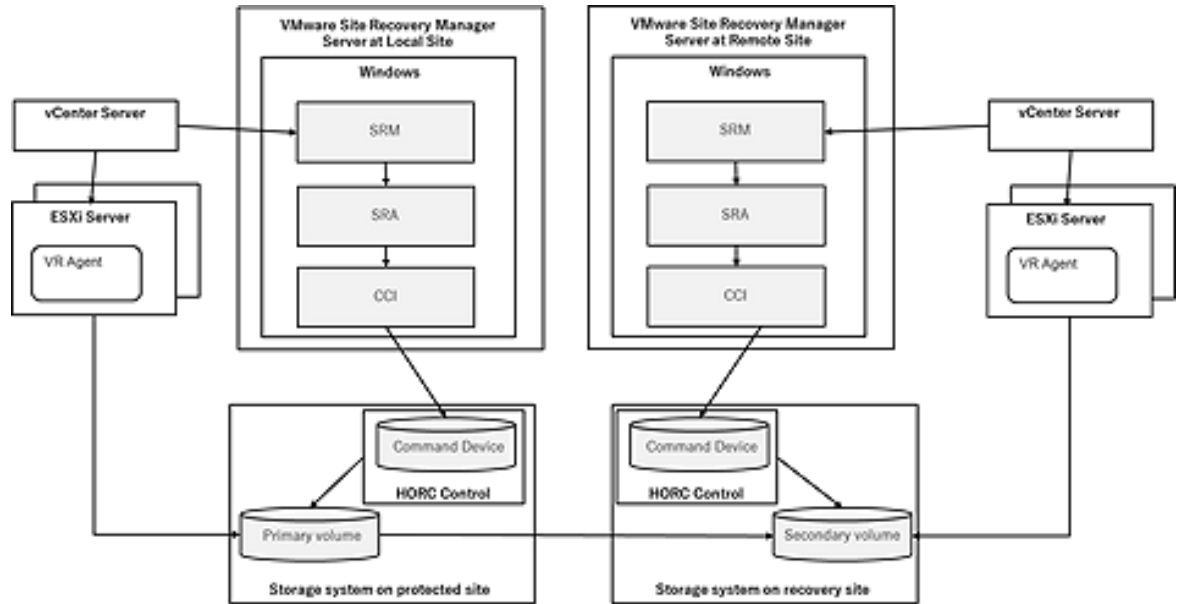
Figure 4 Configuration 1
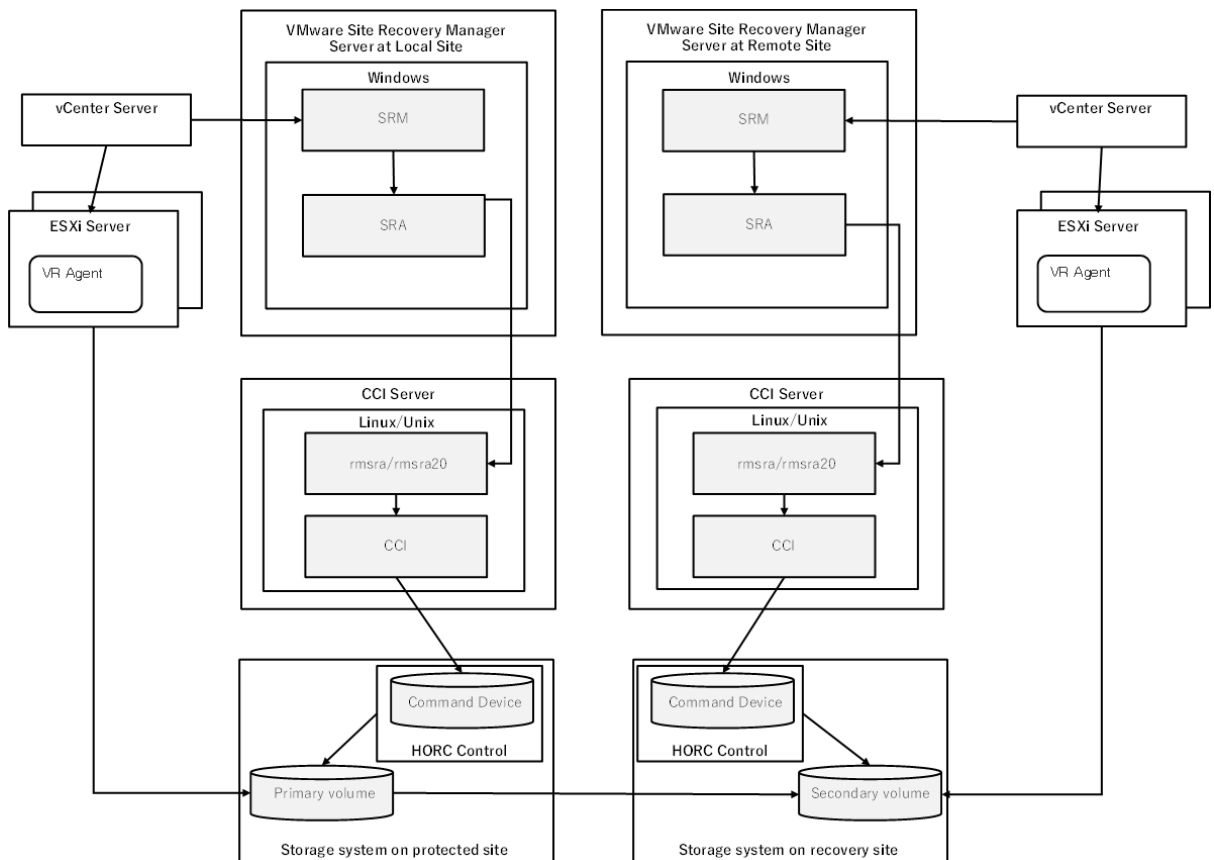
Figure 5 Configuration 2
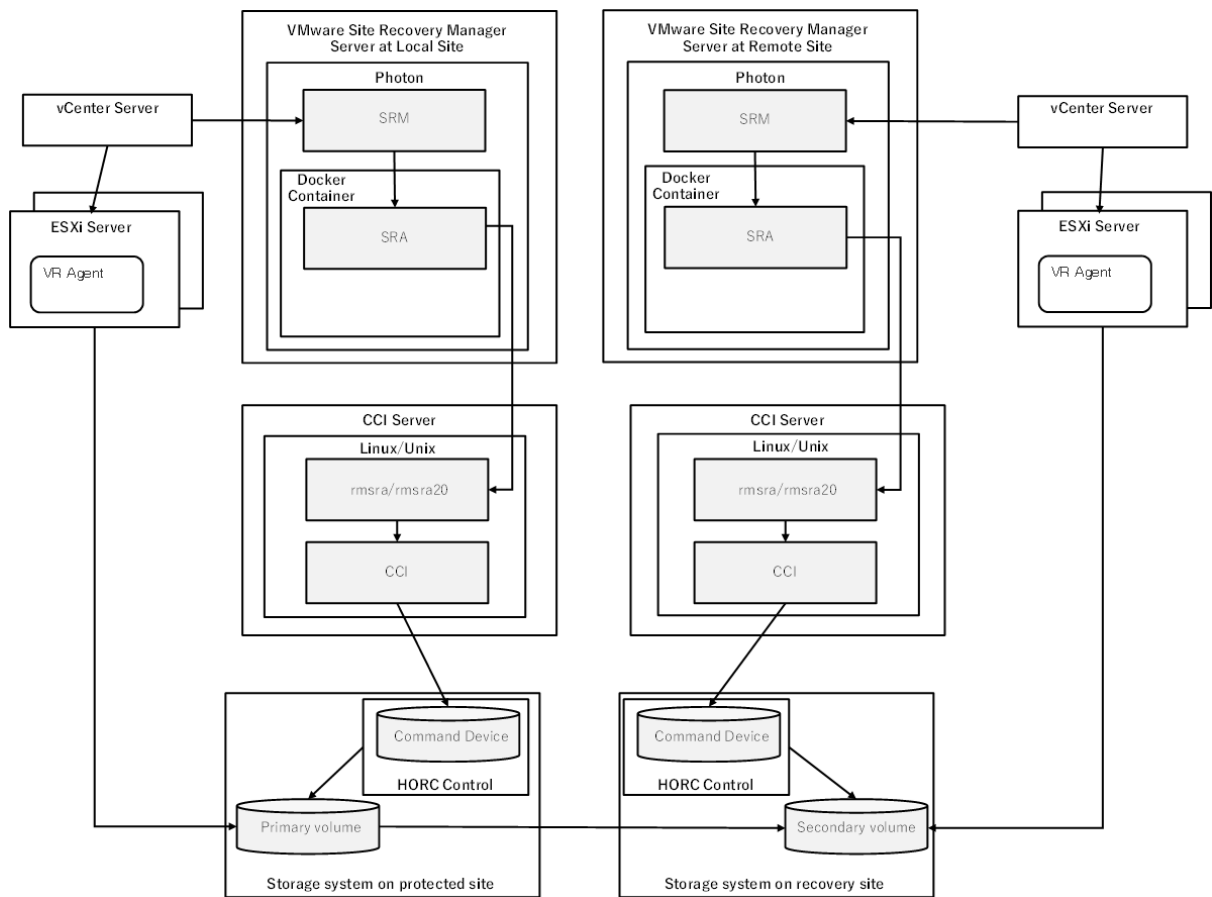
Figure 6 Configuration 3

Deployment workflow

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

Table 2 Workflow for deploying

Task	How to
1. Review requirements and planning considerations.	See Requirements (on page 15).
2. Configure the storage area network.	See the Hitachi whitepaper, *Deploying VMware Site Recovery Manager 5.0 with VMware vSphere 5.0 on Hitachi Virtual Storage Platform, Implementation Guide* (3/2012).

Task	How to
3. Configure Hitachi remote replication using Storage Navigator. Includes storage, pair volume, port, logical path, and data path setup.	See the 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 ShadowImage or Thin Image user guide for information.
5. Install Command Control Interface (CCI) to manage storage replication.	See Installing CCI (on page 26).
6. Create and map a command device.	See Creating and configuring a CCI command device (on page 27).
7. Set up CCI HORCM files with pair and path information.	See Setting up HORCM configuration definition files (on page 29).
8. Create pairs.	See Starting HORCM instances, creating pairs (Windows) (on page 35).
9. Ensure the VMware® vCenter SRM™ 2013 and VMware® vCenter SRM™ databases are installed.	See the VMware vCenter Site Recovery Manager documentation.
10. Install SRA 2.*x*.	See SRA installation (on page 46).
11. Connect protected and recovery sites.	See the VMware vCenter Site Recovery Manager documentation.
12. Configure SRA in Site Recovery Manager.	See Configuring SRM to communicate with RMSRA20 (SRM v8.2 or later) (on page 51).
13. Set up inventory mappings, protection group, recovery plan, perform test recovery.	See the VMware vCenter Site Recovery Manager documentation. **Note:** In GAD configurations, 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.

CCI version requirements:

- SRA 2.2 and 2.3: 01-36-03/03 or later

- SRA 2.5: 01-46-03/02 or later

For Configuration 1, CCI is installed in Windows on the SRM servers. For Configurations 2 and 3, CCI is installed on the CCI servers.

When CCI is installed on the VMware vCenter SRM™ host, you should run HORCM as a service. (HORCM is described in .)

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

Creating and configuring a CCI command device

A CCI 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 enables the CCI software to send commands using in-band protocol to the storage system. One CMD per storage system is required.

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

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

> 📄 **Note:** It is recommended to use In-Band command devices described in the procedure below. If you use Out-of-Band command devices (virtual command devices), the following must be taken into account. Refer to the Command Control Interface User and Reference Guide for details about Out-of-Band.
>
> If Out-of-Band is used for a large configuration that has a large number of replication pairs, a timeout error of SRM could occur because the communication speed of Out-of-Band is slower than that of In-Band. Use Out-of-band only for small configurations.
>
> Out-of-Band is unavailable during microcode exchange, SVP/GUM reboot, and/or MP failure. Use Out-of-band only for environments where temporary service outage is acceptable.

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.
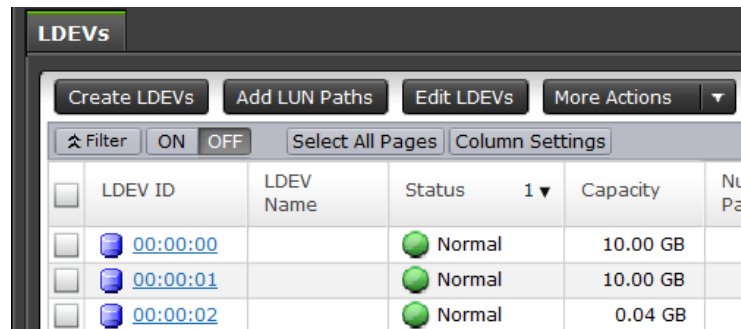
3. Proceed through the **Create LDEVs** wizard, keeping the following in mind:

   ▪ 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**.

Chapter 3: Deployment
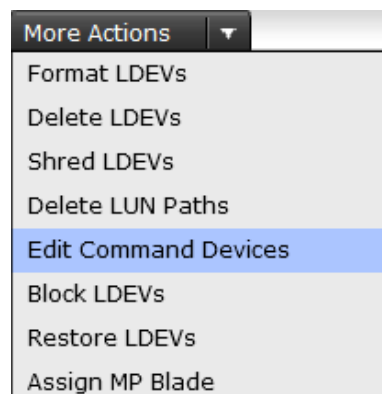
5. In the **Edit Command Devices** wizard, select **Enable** for **Command Device**. Leave the Command Device Attributes disabled.
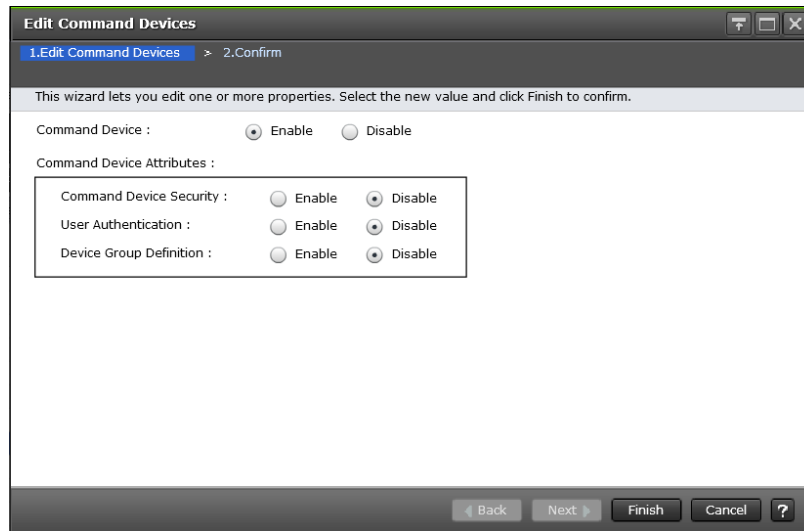
6. Click **Finish**.

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:

   a. In Microsoft Windows 2008, from the Server Manager menu, point to Storage and click **Disk Management**.

   b. Right-click the RDM disk and click **Online**.

   c. Right-click the RDM disk and click **Initialize Disk**.

   d. Click **MBR** (Master Boot Record) as the partition style.

10. Present a CMD volume from the primary storage system to the primary ESX/ESXi server, and another CMD volume from the secondary storage system to the recovery ESX/ESXi server.

Setting up HORCM configuration definition files

You will need two HORCM configuration definition files to define the pair relationship: one file describes the primary volumes (P-VOLs), and the other file describes the secondary volumes (S-VOLs). A third HORCM configuration definition file is required if you use a 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 13) 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 or /etc folder, according to the CCI server's OS.

- HORCM files must be named **horcm#.conf**, where "#" represents the HORCM instance.

  - The instance on the primary site is usually **0**. In this case, the HORCM file on the primary site would be named, **horcm0.conf**.

  - The # of the secondary instance must be the primary instance number plus 1. Thus, if the primary instance is 0, the HORCM file on the secondary site would be named, **horcm1.conf**.

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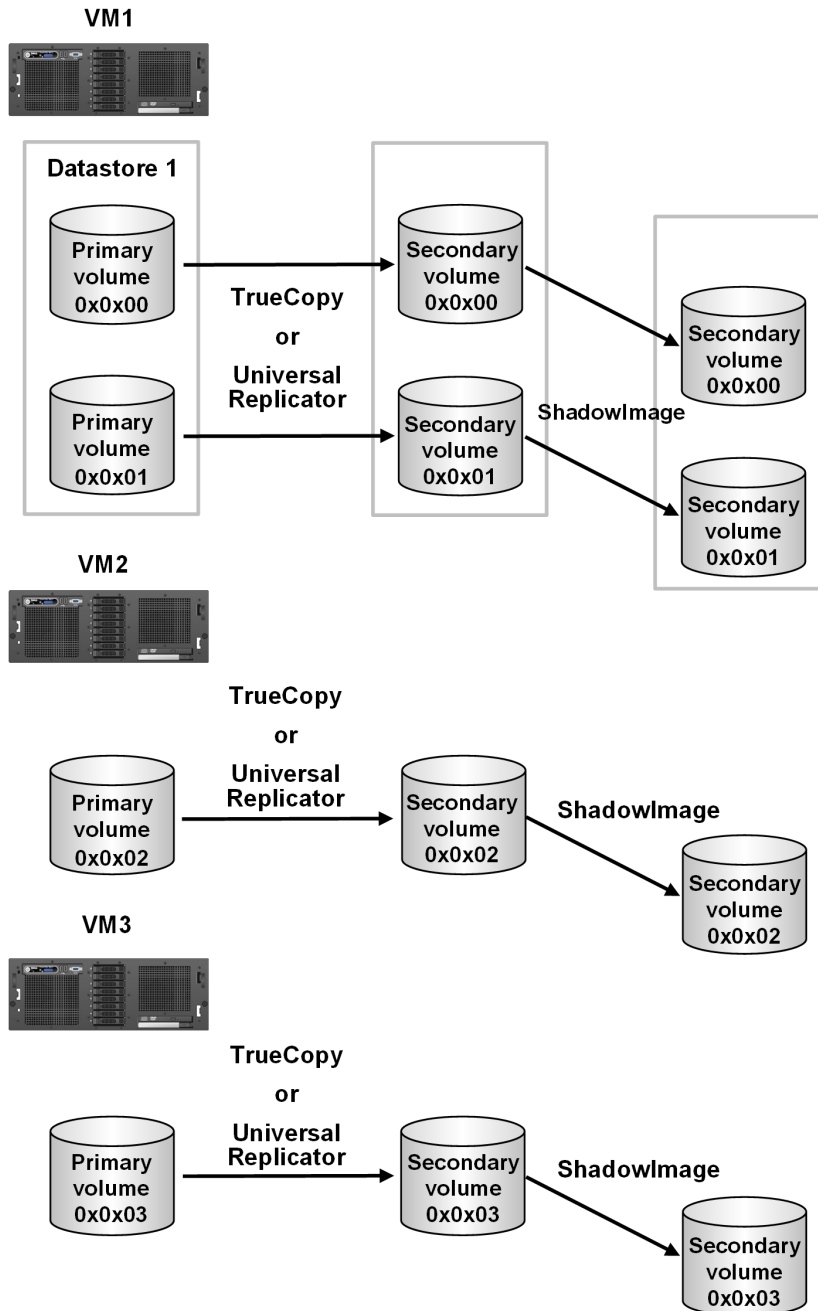
HORCM examples are provided in the following sections for the primary site, secondary site, and an optional secondary-site test pair.

Primary HORCM file

Example HORCM0.conf for primary site remote replication pair (on page 32) 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 GAD (non-CTG), and MU#h0-h2 for UR and GAD (CTG).

- **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

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 <u>Configuring SRA for testing (on page 44)</u> for instructions.

In-system test copy HORCM file

<u>Example HORCM2.conf for secondary site in-system test pair (on page 34)</u> 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 <u>Using a copy of the S-VOL for testing (on page 18)</u>.)

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.

Chapter 3: Deployment

Starting HORCM instances, creating pairs

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

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

For additional information about CCI commands and expected output, see the *Command Control Interface Command Reference*.

> 📄 **Note:** If the Windows version of CCI is used, CCI is installed on the SRM server. If the UNIX version of CCI is used, CCI is installed on a location other than the SRM server.

Starting HORCM instances, creating pairs (Windows)

Procedure

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

   cd c:\HORCM\etc

   horcmstart.exe *

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

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

   pairdisplay.exe -g <grp> -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. For example:

   ▪ On the primary server, run **horcmshutdown.exe 0**.

   ▪ On the recovery server, run **horcmshutdown.exe 1**.

Starting HORCM instances, creating pairs (UNIX)

Procedure

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

   cd /HORCM/usr/bin

   horcmstart.sh *

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

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

   pairdisplay -g <grp> -IH<HORCM instance #> -fcx

3. On the primary UNIX host, create the TrueCopy(TC), Universal Replicator(UR), or GAD pair using the paircreate command:

   ▪ For TC, use: **paircreate -g <grp> -vl -fg <fence> <CTGID> -IH<HORCM instance#>**

   ▪ For UR, use: **paircreate -g <grp> -vl -f async -jp <journal id> -js <journal id> -IH<HORCM instance #>**

   ▪ For GAD, use: **paircreate -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).

   📄 **Note:** The HORCM instances of CCI are installed on the primary and secondary UNIX hosts must be running.

Creating a copy for testing on the recovery site

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

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

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

Chapter 3: Deployment

Before you begin

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

- For Split mode, you must set to **quick** by using the command option **-fq quick**.

- For 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 by using the pairdisplay command.

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

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

3. Create the pair by using the following:

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

   - **-m grp** creates a consistency group for all LUNs in the pair group.

   - **-fq quick** allows for 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**.

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

Before you begin

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

- For Split mode, you must set to **quick** by using the command option **-fq quick**.

- For 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 /HORCM/usr/bin

    horcmstart.sh *

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

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

    pairdisplay -g <grp> -IM<HORCM instance #> -fcx

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

3. Create the pair by using the following:

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

    - **-m grp** creates a consistency group for all LUNs in the pair group.

    - **-fq quick** allows for 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.

    > **Note:** The HORCM instances of CCI are installed on the primary and secondary UNIX hosts must be running.

Setting environment variables

RMSRA20 requires that the following system environment variables be defined in order to make certain parameters available. The following table lists the environment variables that are required for each configuration. Command line examples are included.

> **Note:** In configurations 2 and 3, SRA on the SRM server connects to the CCI server with the non-interaction SSH shell. When you set environmental variables for SRA on the CCI server, make sure that the non-interaction shell can read the environmental variable set on the CCI server. For example, the environmental variable must be set on `~/.bashrc` when you use Linux.

Table 3 Environment Variables

Variable	Description	Command line example	Configuration
HORCMROOT	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	1 **Configuration 1**: Set the variable on the Windows SRM server. **Configuration 2**: Setting the variable is not required. **Configuration 3**: Setting the variable is not required.
RMSRATOV	Used to specify the timeout value for failover using Universal Replicator. If not specified on either the local or remote system, 60 seconds is the default.	**Configuration 1 and 2**: To the set timeout value to 30 seconds: C:\>setx RMSRATOV 30 /m **Configuration 3**: See Defining environment variables using the environmental setting file (on page 42).	1, 2, and 3 **Configuration 1**: Set the variable on the Windows SRM server. **Configuration 2**: Set the variable on the Windows SRM server. **Configuration 3**: Set the variable *env.conf* on the Docker SRM server.
RMSRATMU	Used to specify the MU# of the in-system replication volume for testFailover. If not specified, then MU#0 is the default and this variable is not specified on the remote.	**Configuration 1 and 2**: To specify MU#1 C:\>setx RMSRATMU 1 /m **Configuration 3**: See Defining environment variables using the environmental setting file (on page 42).	1, 2, and 3 **Configuration 1**: Set the variable on the Windows SRM server. **Configuration 2**: Set the variable on the Windows SRM server. **Configuration 3**: Set the variable *env.conf*on the Docker SRM server.

Variable	Description	Command line example	Configuration
RMSRA_MULT_CAP	Used to report support for SRM "Multiple Array".	C:\>setx RMSRA_MULT_CAP 1 /m Note: This is set on a CCI Server not on Windows OS or Photon™ OS.	1, 2, and 3 **Configuration 1**: Set the variable on the Windows SRM server. **Configuration 2**: Set the variable on the CCI server. **Configuration 3**: Set the variable on the CCI server.
RMSRA_USE_SSH	Used to specify an SSH connection instead of Telnet.	C:\>setx RMSRA_USE_SSH 1 / m	2 **Configuration 1**: Setting the variable is not required. **Configuration 2**: Set the variable on the Windows SRM server. **Configuration 3**: Setting the variable is not required.
RMSRAFNGPTCHK	Used to specify whither to check the FingerPrint of CCI servers or not. "yes" is the default that means to check the FingerPrint. "no" means not to check the FingerPrint. If not specified, then set to check the FingerPrint of CCI servers.	Cannot set the RMSRAFNGPTCHK by command line. See Defining environment variables using the environmental setting file (on page 42).	3 **Configuration 1**: Setting the variable is not required. **Configuration 2**: Setting the variable is not required. **Configuration 3**: Set the variable *env.conf* on the Docker SRM server.
SplitReplication	Used when you need to execute `testfailover`	C:\>setx SplitReplication true /m	1, 2, and 3

Variable	Description	Command line example	Configuration
	without ShadowImage or Thin Image.		**Configuration 1**: Set the variable on the Windows SRM server. **Configuration 2**: Set the variable on the CCI server. **Configuration 3**: Set the variable on the CCI server.

Defining environment variables using the GUI

Define the variables using the GUI as follows.

Procedure

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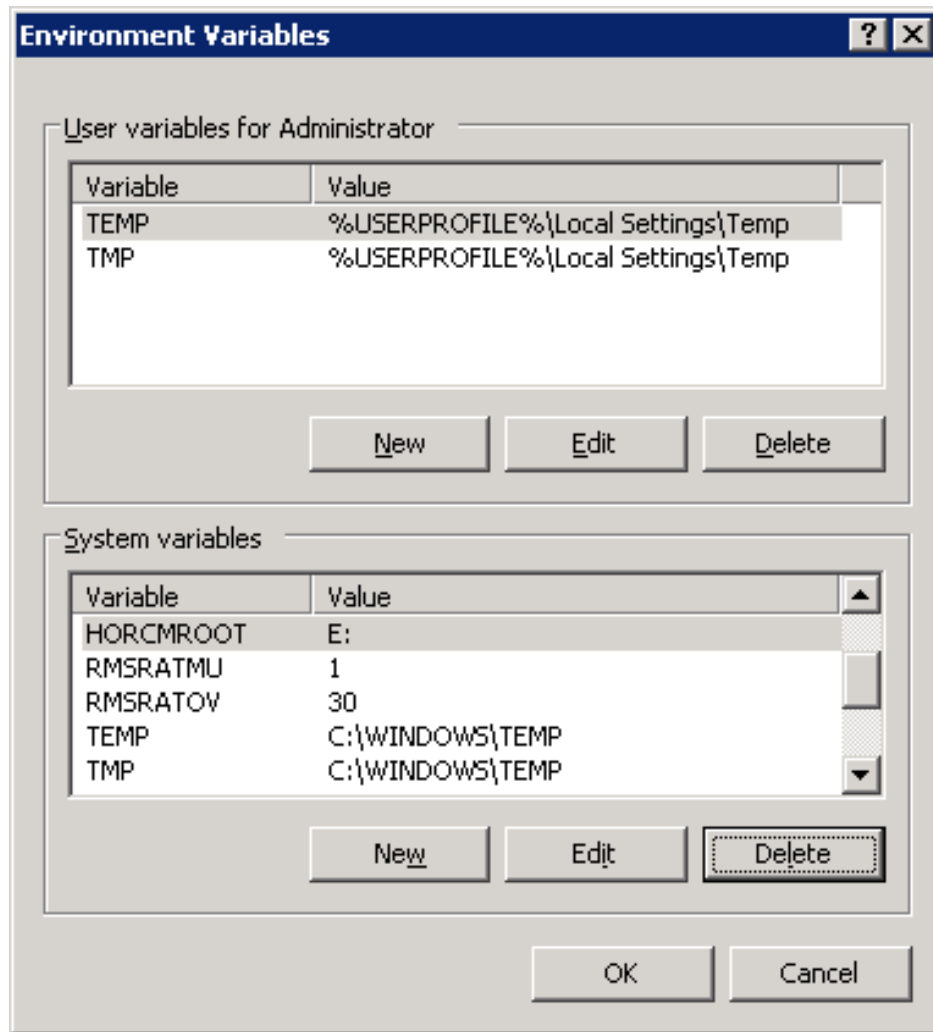
4. Reboot Windows.

Defining environment variables using the environmental setting file

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

Procedure

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

    User: admin (Initial admin user)

    Password: (Initial admin user password)

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

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

    Password: Initial root user password

3. Deploy "env.conf":

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

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

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

4. Save the env.conf file.

5. Change the env.conf file:

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

About SSH

SRM/SRA Configuration 1 and 2

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

SRM/SRA Configuration 3

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

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

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

Chapter 3: Deployment

SRA version	Docker Image ID
02.05.00	c2ac27ec747a5919f4d4c146025b3b74be9a0c2a1ffb3acccdedb7508bd4eefe

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

Example deployment of known_hosts:

1. Use SSH to log in to SRM (Photon™ OS).
2. Move to root user.
3. Run the Docker container:

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

4. Log in to the Docker container:

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

5. Get information from **known_hosts**:

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

6. Copy the contents of known_hosts_file into the local tmp file of your PC.
7. Press Ctrl+D to log out of the Docker Container.
8. Delete the Docker container:

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

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

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

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

10. Deploy **known_hosts**:

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

    root@photon [ ]$vi known_hosts
    ```

11. Copy the content of **known_hosts_file** into **known_hosts**, then save the file.
12. Change the mode of **known_hosts**:

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

Configuring SRA for testing

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:

   setx HORCMROOT E: /m

6. Optional: The default timeout value for failover using UR/Async is 60sec. This can be changed using RMSRATOV variable:

   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/.bashrc** 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 <u>Installing Hitachi SRA 2.x (on page 46)</u>.

- If you are upgrading an existing version of SRA 2.x, you must remove it before continuing. See <u>To remove an earlier version of SRA (Configuration 1, 2) (on page 48)</u> for instructions.

- To check your SRA version, see <u>Checking the SRA version (on page 48)</u>.

Installing Hitachi SRA 2.x

Read the following conditions before performing the installation.

- Site Recovery Manager (SRM™) must be installed on both the protected and recovery sites.

- Download the required version of SRA from the VMware® website:

  - For SRM™ 6.1, 6.5, or 8.1, download HITACHI_RMHTCSRA_X64-02.03.01.exe.

  - For SRM™ 8.2 or 8.3, download HITACHI_RMHTCSRA_X64-02.05.00.exe or HITACHI_RMHTCSRA_X64-02.05.00.gz or later.

- If a previous version of SRA is installed, remove it before installing SRA 2.x. See <u>To remove an earlier version of SRA (Configuration 1, 2) (on page 48)</u> for instructions.

- Install SRA on the SRM™ servers on the protected and recovery sites.

- Make sure the RMSRA20 executable in the CCI installation is the latest version. If your site has implemented Configuration 3, you can obtain the latest RMSRA20 version from the SRM (Photon™ OS) directory.

Installation for Configuration 1 or 2

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

Procedure

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

    a. Right click **My Computer** and select **Manage**.

    b. Click **Services and Application**, then select **Services**.

    c. Locate **VMware Site Recover Manager**, then click **Restart**.

Installation for Configuration 3

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

📄 **Note:** Before you begin, verify that the CONFIGURE APPLIANCE setting has been configured.

Procedure

1. Log in to **SRM Appliance Management**.
2. Click **Storage Replication** >**New Adapter**.
3. Click **UPLOAD**, and then select HITACHI_RMHTCSRA_X64-02.xx.xx.gz.
4. Confirm the SRA version.

Removing an earlier version of SRA

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

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

If needed, you can check the installed version. For information, see .

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

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

Procedure

1. Open Windows **Control Panel**.
2. Click **Add or Remove Programs**.
3. Select **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.

To remove an earlier version of SRA (Configuration 3)

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

Procedure

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

Checking the SRA version

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

- Windows server
- Linux server
- Docker container on Photon

To check the SRA version on a Windows server

Procedure

1. On the Windows server that is running VMware® vCenter SRM™ and 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: 02.05.0x or later
```

To check the SRA version on a Docker Container on Photon

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

Procedure

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

Obtaining the latest rmsra20

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

Procedure

1. Use SSH to log in to SRM (Photon OS).
2. Move to root user.
3. Locate rmrsa20:

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

   Refer to the table for the SRA Docker Image ID.
4. Obtain rmsra20 using the scp command, for example:

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

Deploying rmsra20

After obtaining rmsra20 (see), you can deploy the latest rmsra20 to the CCI Server.

Procedure

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

   ```
   scp rmsra20.linux64 "[CCI Server's username]"@"[CCI Server's IP
   Adress]":/HORCM/usr/bin
   ```

2. Replace the original rmsra20 with the latest rmsra20.

   ```
   cp /HORCM/usr/bin/rmsra20 /HORCM/usr/bin/rmsra20_bak
   cp /HORCM/usr/bin/rmsra20.linux64 /HORCM/usr/bin/rmsra20
   ```

Configuring SRM to communicate with RMSRA20 (SRM v8.2 or later)

To configure SRM v8.2 or later* to communicate with RMSRA20, complete the following tasks:

- [Add array manager (SRM v8.2 or later) (on page 51)](#)
- [Check devices (SRM v8.2 or later) (on page 53)](#)

* For details about configuring SRM v8.1 or earlier, please refer to the previous revision (15) of this document.

Add array manager (SRM v8.2 or later)

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.

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 are 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 using vSphere Web Client.
2. Click **Site Recovery** then click **VIEW DETAILS**.
3. Click **Configure** > **Array Based Replication** > **Storage Replication Adapters**.
4. Make sure that the version of SRA is the one that you installed:
    - If not on display, Click RESCAN ADAPTERS on both the protected site and the recovery site.
    - If the version on display differs from the one that you installed, re-install SRA. See [Installing Hitachi SRA 2.x (on page 46)](#).
5. Click **Configure** > **Array Based Replication** > **Array Pairs** then click **+ADD**.
6. In Storage replication adapter, confirm whether **Status** is **OK**. If it is, click **NEXT**.
7. In **Local array manager**, enter appropriate values and verify information:
    Enter a name for the array manager. In the following example, X is the HORCM instance number on the CCI Server: HORCMINST=X@Host-name
    Enter a Username and Password for the CCI Server.

Available characters for Username and password are as follows:

- 0-9, a-zA-Z (alphanumeric characters)

- - (hyphen)

- , (comma)

- . (period)

- : (colon)

- @ (at sign)

- _ (under score)

- / (slash)

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

Confirm that remote replication has been configured.

8. Click **NEXT**.

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

9. In **Remote array manager**, enter appropriate values and verify information:

    Enter a name for the array manager. In the following example, X is the HORCM instance number on the CCI Server: HORCMINST=X@Host-name

    Enter a Username and Password for the CCI Server.

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

    Confirm that remote replication has been configured.

10. Click **NEXT**.

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

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

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

    In the event of an error, check the configuration.

> 📄 **Note:** For information about command device authentication on UNIX systems of the CCI Server, see .

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 (SRM v8.2 or later)

Check if the protected volumes are recognized by SRM (v8.2 or later) by completing the following procedure. In the event of an unintended result or an error, check the configuration.

Procedure

1. Click **Configure** > **Array Based Replication** > **Array Pairs**.
2. Select the array pairs to check.
3. Check the following items at the protected site:

    - Do Device (protected site) and Device (recovery site) match dev_name in the HORCM configuration definition file?

    - Does **Status** show **Forward** or **Reverse**?

Performing reprotect and failback

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

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

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

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

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

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

- Failure at site A and migration to site B

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

To perform reprotect and manual failback

Procedure

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

   If these operations fail, proceed as follows:

   - Ensure that the remote link and remote array are functional, using the **pairdisplay -g <grp>** command. If necessary, recover the remote link and remote array.

   - Re-execute the reprotect operation.

Chapter 4: Troubleshooting

This chapter provides information and instructions for troubleshooting configuration problems.

Error messages on VMware® vCenter SRM™ log files

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

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 2008 or later:** C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs\

  - By default, logs roll over after reaching 5 MB.

  - vmware-dr-index contains the most recent Log File number.

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

If you need to contact customer support, see .

XML errors received from VMware® vCenter SRM™

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

100

- Cause: Required components are not correctly installed or settings of the components are not correct.

- Action: Check if SRM and SRA are correctly installed and settings of SRM and SRA are correct. If you use SSH, you have to also check if plink.exe is correctly installed and settings of plink.exe are correct.

1002

- Cause: The HORCM instance could not start with the specified connection address.

- Action: Check whether the HORCM instance# specified in the connection address is correct, or whether the horcm*.conf file exists.

1003

- Cause: Authentication failed for User/Password for the specified connection address.

- Action: Check whether the User/Password for the connection address is correct.

1400

- Cause: CCI Server's key fingerprint not registered.

- Action: Check that known_host file is set correctly.

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

- Cause: A parameter in XML was input from VMware® vCenter SRM™ to the SRA, but it exceeds the defined length for the SRA specification.

- Action: Confirm that VMware® vCenter SRM™ received the appropriate parameters in XML from the VMware® vCenter SRM™ log message.

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

- Cause: A parameter in XML was input from VMware® vCenter SRM™ to the SRA but it could not be found in any parameters.

- Action: Confirm that VMware® vCenter SRM™ received the appropriate parameters in XML from the VMware® vCenter SRM™ log message.

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

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

- Action: Confirm that VMware® vCenter SRM™ received the Array ID parameter in XML from the VMware® vCenter SRM™ log message.

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

- Cause: A parameter in XML (naming) was input from VMware® vCenter SRM™ to the SRA, but TargetDevice Key(LDEV# of 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"
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

Error Codes	Error Bits	Description
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

Chapter 4: Troubleshooting

Error Codes	Error Bits	Description
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
1400	-	CCI Server's key fingerprint not registered

Failure to launch scripts

If VMware vCenter Site Recovery Manager array manager configuration fails to launch the SRA 2.0, an error message appears as shown in Figure 7 Error message (on page 62).
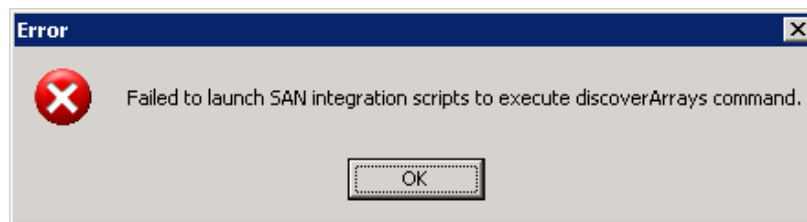
Figure 7 Error message

Correcting UNIX CCI server problems

Procedure

1. Log in to UNIX as **root**.

2. Check that the HORCM instance is running using the command **ps -ef | grep horcm**.

3. If using telnet, check that telnet as root is allowed. From the VMware® vCenter SRM™ server, telnet to the CCI server as root.

4. Check that the correct version of RMSRA20 is installed using the following command:

   /HORCM/usr/bin/rmsra20 -h

   Ver&Rev: 02.01.01

5. 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.
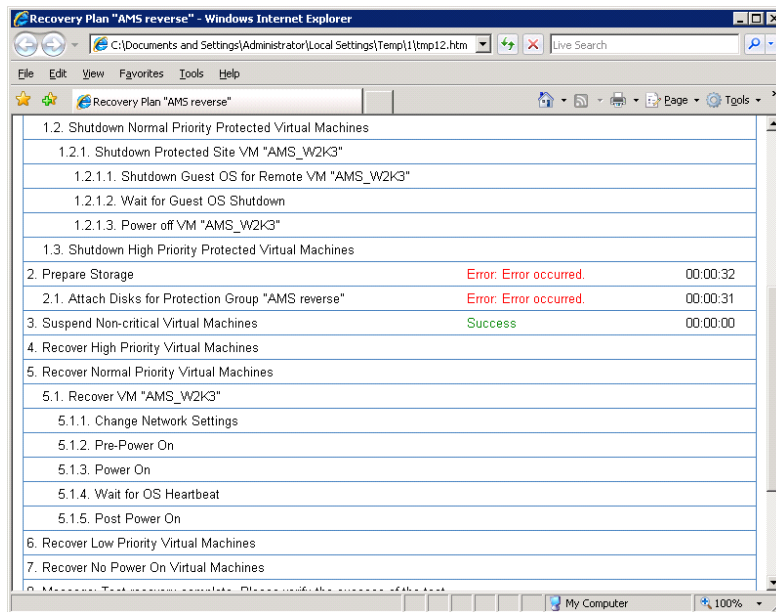
Figure 8 History screen

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 -->
   ```

Chapter 4: Troubleshooting

```
[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 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 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 -->
```

Chapter 4: Troubleshooting

```
[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 (where # is the instance number for SRA):

   - set

   - %HORCMROOT%\HORCM\etc\raidqry -l -I#

   - %HORCMROOT%\HORCM\etc\raidqry -g -I#

   - %HORCMROOT%\HORCM\etc\pairdisplay -IH# -g ??? -CLI -l -fwe (where ??? is a group name shown by **raidqry -g**)

   - %HORCMROOT%\HORCM\etc\raidscan -IH# -p port(e.g. cl1-a-0) - CLI (port connected to ESX/ESXi server)

   If ShadowImage is installed:

   - %HORCMROOT%\HORCM\etc\pairdisplay -g ??? -CLI -l -few -m cas -I# (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 on remote UNIX, where # is the SRA instance number.

   - env

   - raidqry -l -I#

   - raidqry -g -I#

   - pairdisplay -IH# -g ??? -CLI -l -fwe (where ??? is the group name shown by raidqry -g)

   - raidscan -IH# -p port (e.g. cl1-a-0) -CLI (port connected to ESX/ESXi sever)

4. If ShadowImage is installed, collect the following:

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

VMware® vCenter SRM™/SRA Photon™ OS configuration

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

Procedure

1. Collect the VMware® vCenter SRM™ log file on Photon™ OS from both the protected and recovery site:

   `/opt/vmware/support/logs/srm/vmware*.log`

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

   - raidqry -l -I#

   - raidqry -g -I#

   - pairdisplay -IH# -g ??? -CLI -l -fwe (where ??? is the group name shown by raidqry -g)

   - raidscan -IH# -p port (e.g., cl1-a-0) -CLI (port connected to the ESX/ESXi server)

3. If ShadowImage is installed, collect the following:

   pairdisplay -g ??? -CLI -l -few -m cas -I# (where ??? is the 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 <u>Collecting information before contacting customer support (on page 65)</u>.

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: <u>https://support.hds.com/en_us/contact-us.html</u>.

Chapter 5: SRA Change Log

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

Change log for SRA

The following table provides the change log for SRA.

SRA version	Command.pl revision*	Command_dc.pl revision*	Description of change
2.1.4	2.7	Not Installed.	Initial release of SRA 2.1.4
2.1.4	2.8	Not Installed.	Fixed the following problem: Test failover with local replication pairs fails, if the local replication pairs use an MU# other than 0 and SSH remote connection is used between SRA and CCI.
2.2	2.9	Not Installed.	- Added support for global-active device (GAD) and VSP F400, F600, F800. - Discontinued support for TagmaStore USP, TagmaStore NSC, and Adaptable Modular Storage. - Deprecated the iSCSI protocol supporting HUS.
2.3	2.9	Not Installed.	- Added iSCSI support as the protocol for the connection between the storage system and VMware ESXi. - Discontinued support for the telnet protocol for UNIX version of CCI.

SRA version	Command.pl revision*	Command_dc.pl revision*	Description of change
2.3.1	2.9	Not Installed.	▪ Added support for the GAD configuration in VMware Site Recovery Manager 6.5 environment. ▪ Fixed the following problem that occurred: 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. Additionally, this problem might occur when all the following conditions apply: • "Planned Migration" is performed. • "Disaster Recovery" was performed after a failure had occurred on the protected site. • The protected site recovered from the failure after "Planned Migration" is performed.
2.5.x	2.9	1.1	Added Command_dc.pl for SRA running on Docker Container.
*The revision is described in the header of the `command.pl` or `command_dc.pl` file. These files are located in `<SRM install directory>\storage\sra\RMHTC` or `/srm/sra`.			

Appendix A: Configurations with both sites active

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

Protecting both sites

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

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

The following illustration shows a configuration with the protected and recovery sites active.
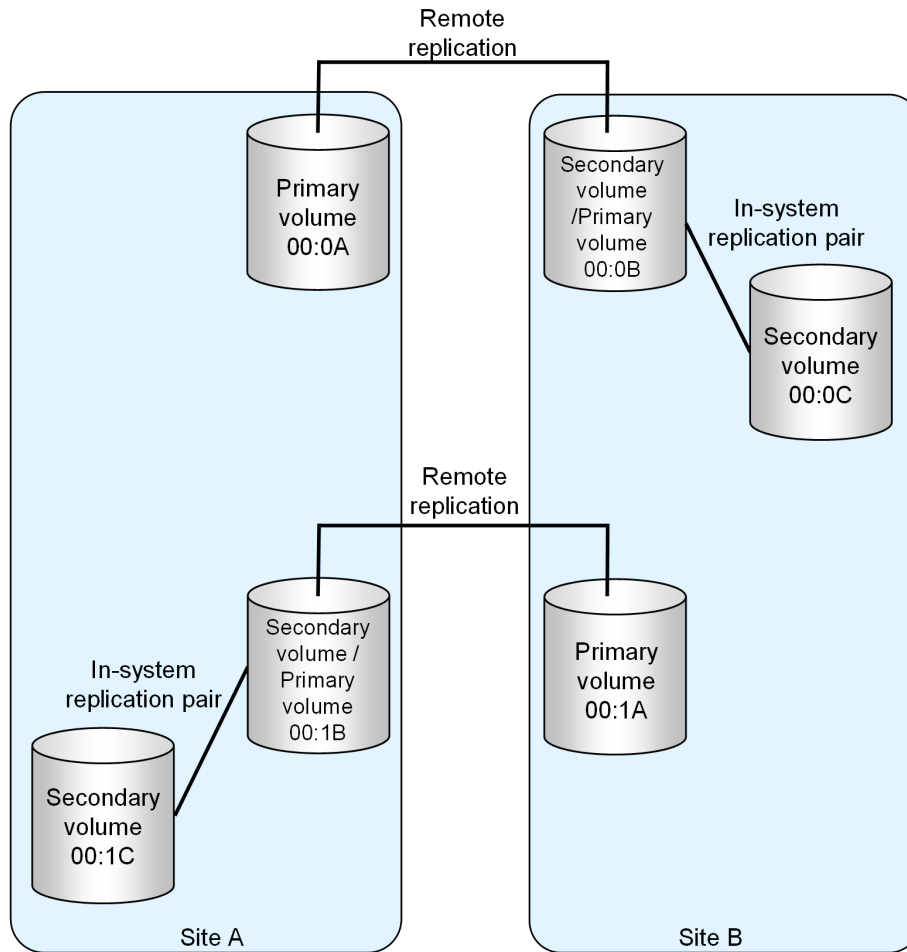
HORCM definition file setup

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

Site A horcm0

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


HORCM_CMD
#dev_name
\\.\CMD-64015


HORCM_LDEV
#dev_group          dev_name        Serial#    CU:LDEV(LDEV#)    MU#
#Replication Site A to Site B
TC_UR_SRM1          01A_01B         64015      00:0A
```

Appendix A: Configurations with both sites active

```
#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
```

Appendix A: Configurations with both sites active

```
TC_UR_SRM1          172.17.46.38    horcm0
TC_UR_SRM2          172.17.46.38    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
```

Appendix A: Configurations with both sites active

Appendix B: Configuration with GAD, UR, and SRM

The configuration with GAD, UR, and SRM (GAD+UR+SRM) provides robust disaster recovery and high availability functions for your data.

About GAD+UR+SRM

The GAD+UR+SRM configuration enables quick system recovery in the event of a failure or disaster and improves system availability by using three storage systems and a virtual environment.

GAD+UR+SRM achieves the following goals:

1. Not only protects data in the event of a failure, but also simplifies the system recovery procedure and reduce the system recovery time by integrated management of storage systems and virtual machines (VM).

2. In the event of a failure at the primary site (Site 1), recovers the system quickly by using the secondary site (Site 2).

3. When both the primary site and the secondary site are affected by a large-scale disaster, recovers the system by using the remote site (Site 3).

Components and configuration for GAD+UR+SRM

The GAD+UR+SRM configuration involves three sites: two protected sites and one recovery site.

Overview of the GAD+UR+SRM configuration

The following figure shows the overview of the GAD+UR+SRM configuration. In the figure, vCenter1 and SRM1 manage Protected site, and vCenter2 and SRM2 manage Recovery site.
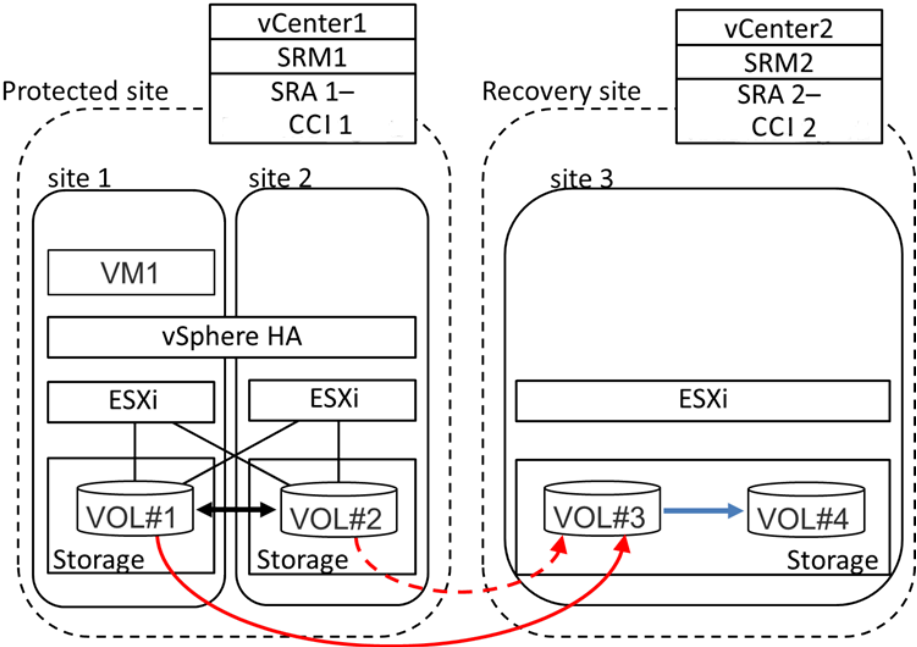
GAD+UR+SRM components

ESXi

ESXi is a virtual platform. A virtual machine is created and runs on ESXi.

vCenter

vCenter Server is a service that provides integrated management of ESXi hosts connected in the network.

In the preceding overview of configuration, vCenter1 and SRM1 manage Site1 and Site 2, and vCenter2 and SRM2 manage Site 3. At Site 1 and Site 2, when a failure occurs at either of the sites, VM is restarted at the other site to continue the system.

vSphere HA (High Availability)

vSphere HA provides high availability to a virtual machine by pooling the virtual machine and the host where the machine is installed to a cluster.

SRM (Site Recovery Manager)

SRM is disaster recovery software.

With GAD+UR+SRM, SRM is used for starting VM at Recovery site when Protected site becomes unavailable due to a large-scale disaster, and so on.

SRA (Storage Replication Adapter)

SRA is a program that is provided by an array vendor. It enables SRM to run simultaneously with a specific type of array. With GAD+UR+SRM, when SRA for VSP G1000 is used, VSP G1000 can be managed from SRM.

The above components are the products of VMware Inc. For details of ESXi, vCenter, and vShpere HA, refer to "VMware vSphere Documentation Center". For details of SRM and SRA, refer to "VMware Site Recovery Manager Documentation Center".

SI/HTI PAIR

SI/HTI PAIR is a pair of the source volume and the target volume that is created by SI (ShadowImage) or HTI (Thin Image). For details, see Hitachi ShadowImage® User Guide or Hitachi Thin Image User Guide. For other components, see Global-Active Device User Guide and Hitachi Universal Replicator User Guide.

Flow of failover by using GAD+UR+SRM

With GAD+UR+SRM, when Protected site (both Site 1 and Site 2) becomes unavailable, the system can continue at Recovery site (Site 3) by performing failover.

The following shows the flow of failover from Site 1 to Site 3 of GAD+UR+SRM.
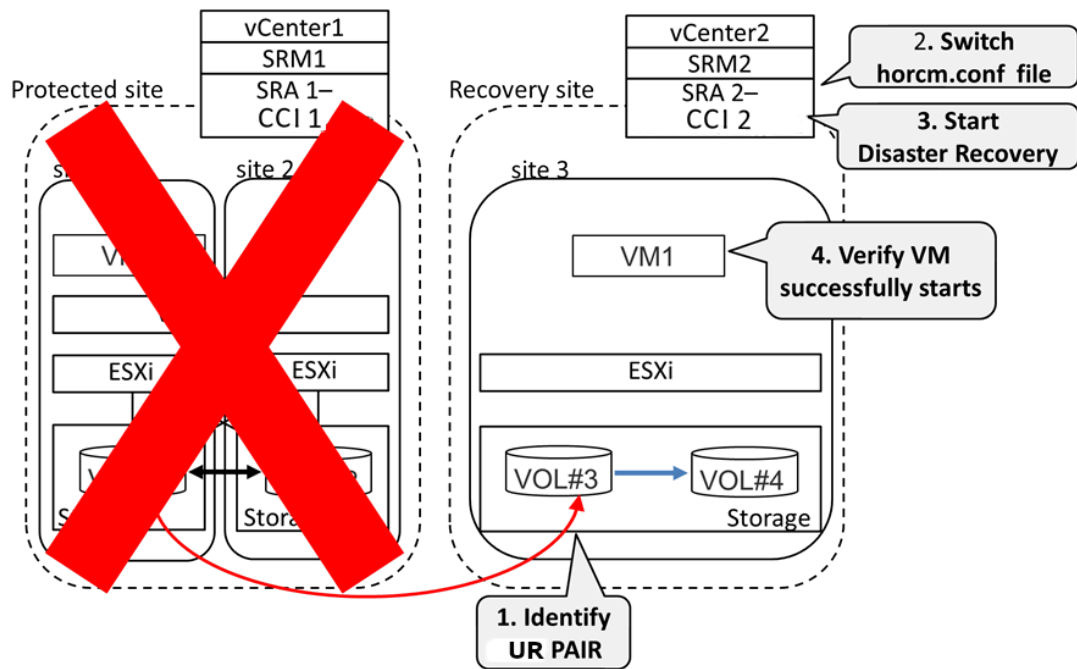
1. Identify the UR pair that is used at Site 3.
2. When the pair is different from the UR pair that is described in the configuration definition file of SRM2, switch to the configuration definition file of the UR pair that is identified in 1.
3. Execute Recovery Plan (Disaster Recovery) with SRM2.
4. Confirm that VM is started normally at Site 3.

Flow of failback by using GAD+UR+SRM

With GAD+UR+SRM, after failover is performed, the system migrated to Recovery site (Site3) can be restored to Protected site by performing failback after Protected site (both Site 1 and Site 2) is recovered.

The following shows the flow of failback from Site 3 to Site 1 of GAD+ UR+SRM.
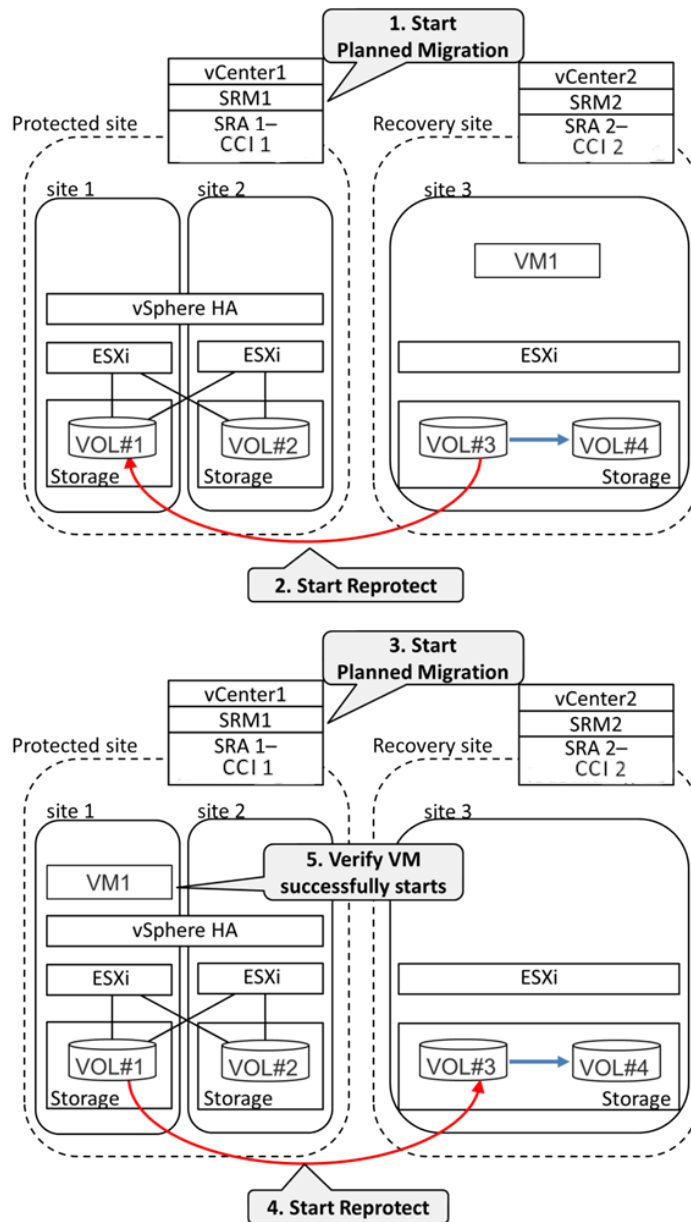
1. **Execute Recovery Plan (Planned Migration) from SRM1.**

2. **Perform Reprotect from SRM1.**

   This creates a UR pair of Site 3 (primary site) and Site 1 (secondary site). The data at Site 3 is copied to Site 1.

3. **Execute Recovery Plan (Planned Migration) from SRM1.**

4. **Perform Reprotect from SRM1.**

   This creates a UR pair of Site 1 (primary site) and Site 3 (secondary site). The data at Site 1 is copied to Site 3.

5. **Confirm that VM is started normally at Site 1.**

GAD+UR+SRM does not support failback from Site 3 to Site 2.

GAD+UR+SRM restrictions

- SRM cannot simultaneously handle both the UR PAIR and the Delta UR PAIR. The PAIR handled by SRM is determined by the definition of horcm.conf which SRA-CCI uses. So horcm.conf files for CCI have to be changed and CCI instances used by SRM have to be restarted manually, when making SRM handle Delta UR PAIR. For example, if Delta resync happens and the Delta UR PAIR becomes the new UR PAIR, horcm.conf files for CCI have to be changed and CCI instances have to be restarted manually.

- SRM does not have a function to build a GAD+UR configuration. So if a disaster happens and a rebuild of GAD+UR configuration is required, users must operate pairs manually via CCI or Device Manager - Storage Navigator to rebuild the GAD+UR configuration.

- For information about the procedure for planned Failover with SRM to Site3, contact customer support.

- SRM may have to be reinstalled and may have to be reconfigured before failback. This restriction is not particular to GAD+UR+SRM. Refer to SRM Admin guide for details.

- Failback is supported when all of the conditions below are satisfied.

  1. The site pair between SRMs has been reestablished without reinstalling or reconfiguring SRMs after a disaster.
  2. Status of the site pair is normal.
  3. GAD pairs and Delta UR pairs are SMPL as shown below.
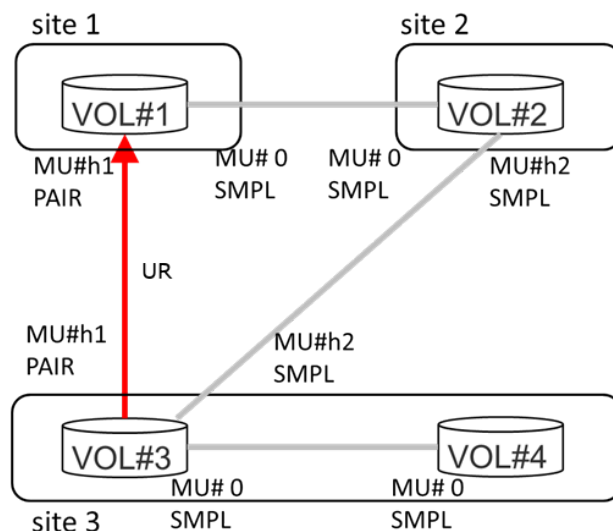
GAD+UR+SRM operations

GAD+UR+SRM operations include failover and failback among the protected and recovery sites.

System configuration example for GAD+UR+SRM

The following describes an example of a system configuration that is created with GAD+UR +SRM. The contents of the configuration definition file and the output results of commands that are described in this chapter are those when an environment is created based on the example of the configuration described in this section.
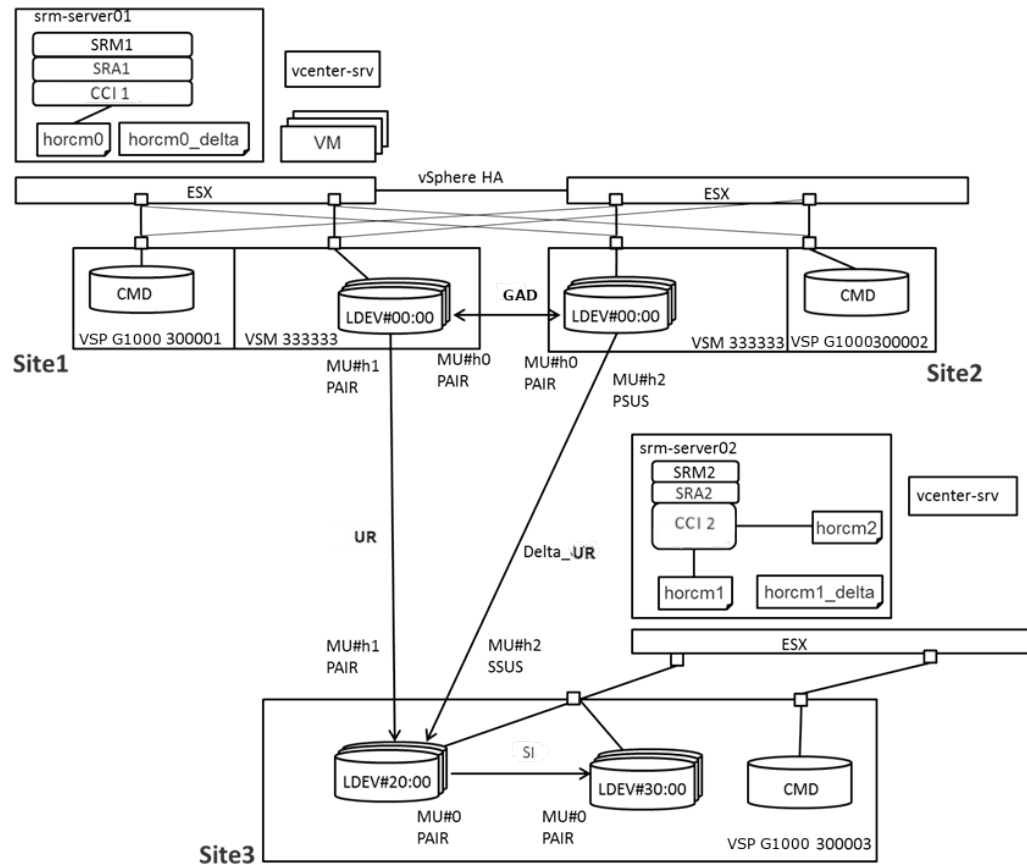
Example of storage system configuration

Table 5 Storage System

Site	Model	Serial Number
Site 1	VSP G1000	300001
Site 2	VSP G1000	300002
Site 3	VSP G1000	300003

Table 6 Resource Group

Resource Group Name	Virtual Storage Machine		Site
	Model	**Serial Number**	
meta_resource	VSP G1000	300001 (Site 1) 300002 (Site 2) 300003 (Site 3)	Site 1 Site 2 Site 3
HA_VSM	VSP G1000	333333	Site 1, Site 2

Table 7 UR Pair

Pair Group Name	Primary Site	Primary Volume	Secondary Site	Secondary Volume	Mirror ID(MU#)	Status
UR	Site 1	00:00:00 00:00:01 00:00:02	Site 3	00:20:00 00:20:01 00:20:02	h1	PAIR
DELTA_UR	Site 2	00:00:00 00:00:01 00:00:02	Site 3	00:20:00 00:20:01 00:20:02	h2	PSUS (Site 2) SSUS (Site 3)

Table 8 GAD Pair

Pair Group Name	Primary Site	Secondary Site	LDEV ID	Mirror ID(MU#)	Status
GAD	Site 1	Site 2	00:00:00 00:00:01 00:00:02	h0	PAIR

Table 9 SI Pair

Pair Group Name	Site	Primary Volume	Secondary Volume	Mirror ID(MU#)	Status
SI	Site 3	00:20:00 00:20:01	00:30:00 00:30:01 00:30:02	0	PAIR

Appendix B: Configuration with GAD, UR, and SRM

Pair Group Name	Site	Primary Volume	Secondary Volume	Mirror ID(MU#)	Status
		00:20:02			

Table 10 Port

Site	Port name	Attribute
Site 1	CL3-A	TAR
Site 1	CL5-A	TAR
Site 1	CL7-A	MCU
Site 1	CL2-B	RCU
Site 1	CL4-B	MCU
Site 1	CL5-B	RCU
Site 2	CL3-A	RCU
Site 2	CL4-A	TAR
Site 2	CL5-A	RCU
Site 2	CL6-A	TAR
Site 2	CL7-A	MCU
Site 2	CL1-B	MCU
Site 3	CL1-A	TAR
Site 3	CL7-A	MCU
Site 3	CL3-A	RCU
Site 3	CL7-B	MCU
Site 3	CL3-B	RCU

Example of server configuration

Table 11 SRM server

#	IP address	Use
1	10.213.54.140	Management of Protected site
2	10.213.54.141	Management of Recovery site

Table 12 CCI

#	Initial instance	Use
CCI 1	horcm0.conf	Storage operation at Protected site
CCI 2	horcm1.conf	Storage operation at Recovery site
	horcm2.conf	SI/HTI pair operation at Recovery site

Table 13 Configuration definition file at Protected site

Instance Number	Configuration definition file	Use
0	horcm0.conf	UR pair operation
	horcm0_delta.conf	UR pair operation for Delta Resync

Table 14 Configuration definition file at Recovery site

Instance Number	Configuration definition file	Use
1	horcm1.conf	UR pair operation
	horcm1_delta.conf	UR pair operation for Delta Resync
2	horcm2.conf	SI/HTI pair operation

Configuration definition

The following shows examples of configuration definition files. These examples use the In-Band method, in which the host (connected by FC or iSCSI) issues commands to the command device in the storage system. GAD+UR+SRM operations can also be performed by using the Out-of-Band method, in which a LAN-attached host issues commands to the virtual command device in the SVP of the storage system.

To use the In-Band method, make sure to define a command device (CMD) on meta_resource. For details, see the *Command Control Interface User and Reference Guide*.

horcm0.conf

```
HORCM_MON#ip_address    service       poll(10ms)     timeout(10ms)
10.213.54.140    31001        1000          3000
```

Appendix B: Configuration with GAD, UR, and SRM

```
HORCM_CMD
#dev_name
\\.\CMD-300001

HORCM_VCMD
333333

HORCM_LDEV#GRP        DEV           SERIAL     LDEV#      MU#
UR     UR_dev1     333333     00:00      h1
UR     UR_dev2     333333     00:01      h1
UR     UR_dev3     333333     00:02      h1

HORCM_INSTP
#GPR      IP ADR          PORT#         PID
UR      10.213.54.141     31002          12
```

horcm0_delta.conf

```
HORCM_MON
#ip_address     service         poll(10ms)      timeout(10ms)
10.213.54.140    31001          1000           3000

HORCM_CMD
#dev_name
\\.\CMD-300002

HORCM_VCMD
333333

HORCM_LDEV
#GRP       DEV           SERIAL       LDEV#      MU#
UR     UR_dev1     333333     00:00      h2
UR     UR_dev2     333333     00:01      h2
UR     UR_dev3     333333     00:02      h2

HORCM_INSTP
#GPR      IP ADR          PORT#         PID
UR      10.213.54.141     31002          11
```

Confirm that the target storage specified by `horcm0.conf` is at Site 1 and the used MU number is h1. Confirm that the target storage specified by `horcm0_delta.conf` is at Site 2 and the used MU number is h2.

horcm1.conf

```
HORCM_MON
#ip_address     service         poll(10ms)      timeout(10ms)
10.213.54.141    31002          1000           3000

HORCM_CMD
```

```
#dev_name
\\.\CMD-300003

HORCM_LDEV
#GRP     DEV          SERIAL     LDEV#     MU#
UR    UR_dev1    300003     20:00     h1
UR    UR_dev2    300003     20:01     h1
UR    UR_dev3    300003     20:02     h1

SI    SI_dev1      300003     20:00     0
SI    SI_dev2      300003     20:01     0
SI    SI_dev3      300003     20:02     0

HORCM_INST
#GPR     IP ADR        PORT#
SI    10.213.54.141    31003

HORCM_INSTP
#GPR     IP ADR        PORT#      PID
UR    10.213.54.140    31001       12
```

horcm1_delta.conf

```
HORCM_MON
#ip_address    service       poll(10ms)    timeout(10ms)
10.213.54.141    31002      1000          3000

HORCM_CMD
#dev_name
\\.\CMD-300003

HORCM_LDEV
#GRP         DEV          SERIAL     LDEV#     MU#
UR        UR_dev1    300003     20:00     h2
UR        UR_dev2    300003     20:01     h2
UR        UR_dev3    300003     20:02     h2

SI        SI_dev1      300003     20:00     0
SI        SI_dev2      300003     20:01     0
SI        SI_dev3      300003     20:02     0

HORCM_INST
#GPR     IP ADR        PORT#
SI    10.213.54.141    31003

HORCM_INSTP
#GPR     IP ADR        PORT#      PID
UR    10.213.54.140    31001       11
```

Appendix B: Configuration with GAD, UR, and SRM

Confirm that the target storage specified by `horcm1.conf` is at Site 3 and the used MU number is h1. Confirm that the target storage specified by `horcm1_delta.conf` is at Site 3 and the used MU number is h2.

`horcm2.conf`

```
HORCM_MON
#ip_address        service     poll(10ms)     timeout(10ms)
10.213.54.141      31003         1000             3000

HORCM_CMD
#dev_name
\\.\CMD-300003

HORCM_LDEV
#GRP          DEV          SERIAL      LDEV#      MU#
SI          SI_dev1        300003      30:00      0
SI          SI_dev2        300003      30:01      0
SI          SI_dev3        300003      30:02      0

HORCM_INST
#dev_group      ip_address      service
SI          10.213.54.141       31002
```

Confirm in `horcm2.conf` that the LDEV# of HORCM_LDEV is the same as the LDEV ID of the SI secondary volume at Site 3.

Test Failover from Site 1 and / or Site 2 to Site 3

In Test Failover with GAD+UR+SRM, the Recovery plan test can be performed by starting VM at Site 3 without stopping the system that is running at Protected site.

Test Failover can be performed when each site has the following status.

#	Site1	Site2	Site3
1	Active	Active	Active
2	Fail	Active	Active
3	Active	Fail	Active

This section uses #1 as an example, but Test Failover to Site 3 can be performed in all cases (See).

Before Test Failover starts
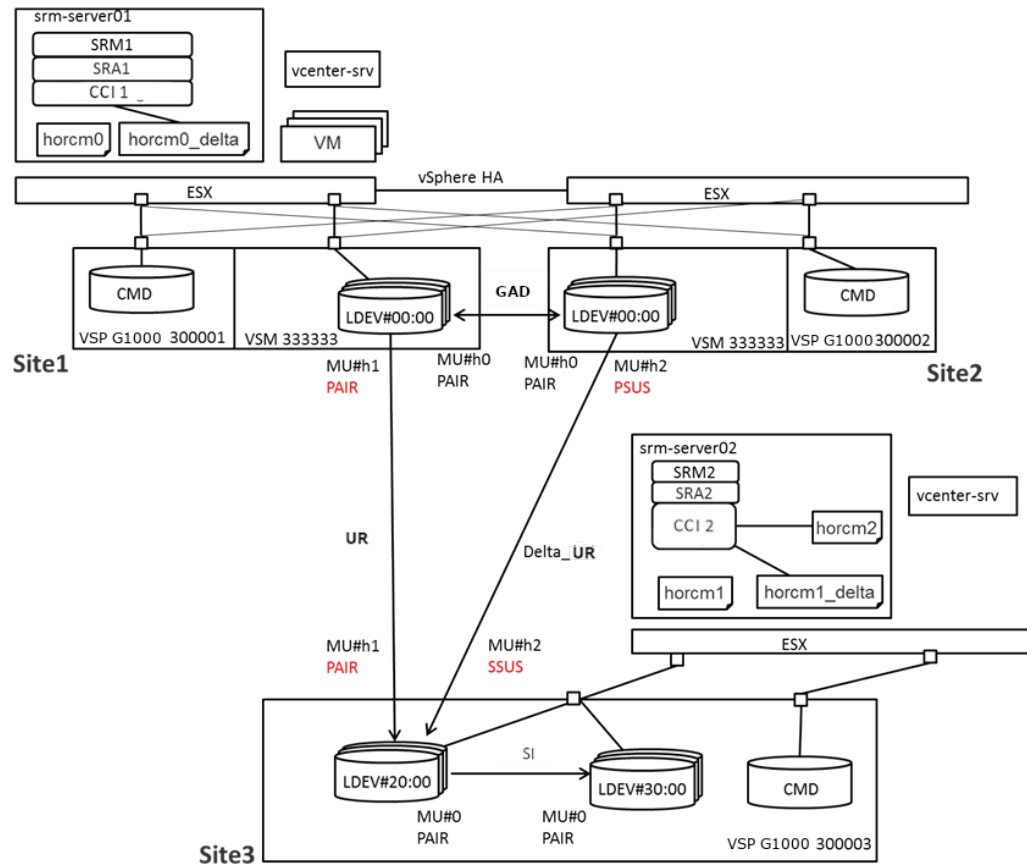
CCI 1(Protected site)

```
c:\HORCM\etc>pairdisplay.exe -g UR -IH0 -fx
Group   PairVol(L/R) (Port#,TID, LU),Seq#,LDEV#.P/S,Status,Fence,Seq#,P-
LDEV# M
UR     UR_dev1(L) (CL4-A-0,23,   0)333333    0.P-VOL PSUS ASYNC ,300003
2000 -
UR     UR_dev1(R) (CL1-A-0,26,   0)300003  2000.S-VOL SSUS ASYNC ,-----
1000 -
UR     UR_dev2(L) (CL4-A-0,23,   1)333333    1.P-VOL PSUS ASYNC ,300003
2001 -
UR     UR_dev2(R) (CL1-A-0,26,   1)300003  2001.S-VOL SSUS ASYNC ,-----
1001 -
UR     UR_dev3(L) (CL4-A-0,23,   2)333333    2.P-VOL PSUS ASYNC ,300003
2002 -
UR     UR_dev3(R) (CL1-A-0,26,   2)300003  2002.S-VOL SSUS ASYNC ,-----
1002 -
```

CCI 2(Recovery site)

```
c:\HORCM\etc>pairdisplay -g UR -IH1 -fx
Group   PairVol(L/R) (Port#,TID, LU),Seq#,LDEV#.P/S,Status,Fence,Seq#,P-
LDEV# M
```

Appendix B: Configuration with GAD, UR, and SRM

```
UR      UR_dev1(L) (CL1-A-0,26,   0)300003  2000.S-VOL SSUS ASYNC ,-----
1000 -
UR      UR_dev1(R) (CL4-A-0,23,   0)333333    0.P-VOL PSUS ASYNC ,300003
2000 -
UR      UR_dev2(L) (CL1-A-0,26,   1)300003  2001.S-VOL SSUS ASYNC ,-----
1001 -
UR      UR_dev2(R) (CL4-A-0,23,   1)333333    1.P-VOL PSUS ASYNC ,300003
2001 -
UR      UR_dev3(L) (CL1-A-0,26,   2)300003  2002.S-VOL SSUS ASYNC ,-----
1002 -
UR      UR_dev3(R) (CL4-A-0,23,   2)333333    2.P-VOL PSUS ASYNC ,300003
2002 -

c:\HORCM\etc>pairdisplay -g SI      SI -IM1 -fx
Group   PairVol(L/R) (Port#,TID, LU-M) ,Seq#,LDEV#.P/S,Status, Seq#,P-
LDEV# M
SI      SI_dev1(L)  (CL1-A-0,26,   0-0 )300003  2000.P-VOL PAIR,300003
3000 -
SI      SI_dev1(R)  (CL1-A-0,26,   3-0 )300003  3000.S-VOL PAIR,-----
2000 -
SI      SI_dev2(L)  (CL1-A-0,26,   1-0 )300003  2001.P-VOL PAIR,300003
3001 -
SI      SI_dev2(R)  (CL1-A-0,26,   4-0 )300003  3001.S-VOL PAIR,-----
2001 -
SI      SI_dev3(L)  (CL1-A-0,26,   2-0 )300003  2002.P-VOL PAIR,300003
3002 -
SI      SI_dev3(R)  (CL1-A-0,26,   5-0 )300003  3002.S-VOL PAIR,-----
2002 -
```

Operational procedure of Test Failover

The following describes the operational flow of Test Failover.

1. Check the MU number that is used by the UR pair at Site 3 from CCI 2, and check if Site 1 or Site 2 is a UR PAIR.

   The journal status(JNLS) of secondary UR volumes should be SJNN. In this example, MU#1 is used by the UR pair.

   ```
   c:\HORCM\etc>raidcom get journal -IH1 -fx
   JID MU CTG  JNLS  AP  U(%)   Q-Marker   Q-CNT   D-SZ(BLK)   Seq# Num
   LDEV#
   001  1  1  SJNN   1   1    2a05ea1f    1184    20213760   300002   1
   322
   001  2  0  SJNS   1   1    2a05ec65     922    20213760   300002   1
   322
   ```

2. If the MU numbers that are described in the horcm files running at both Protected site and Recovery site are different from the MU number that is identified in Step 1, switch to the horcm file of the corresponding MU number.

CCI 1 (Protected site)

```
c:\HORCM\etc>type c:\windows\horcm0.conf
(omitted)
HORCM_LDEV
#GRP      DEV          SERIAL      LDEV#      MU#
UR    UR_dev1    333333      00:00      h2
UR    UR_dev2    333333      00:01      h2
UR    UR_dev3    333333      00:02      h2
(omitted)
```

CCI 2 (Recovery site)

```
c:\HORCM\etc>type c:\windows\horcm1.conf
(omitted)
HORCM_LDEV
#GRP      DEV          SERIAL      LDEV#      MU#
UR    UR_dev1    300003    20:00      h2
UR    UR_dev2    300003    20:01      h2
UR    UR_dev3     300003    20:02      h2
(omitted)
```

   a. Stop the CCI instance.

       CCI 1 (Protected site)

```
c:\HORCM\etc>horcmshutdown 0
inst 0:
HORCM Shutdown inst 0 !!!
```

       CCI 2 (Recovery site)

```
c:\HORCM\etc>horcmshutdown 1
inst 1:
HORCM Shutdown inst 1 !!!
```

   b. Change the file name of the configuration definition file.

       CCI 1 (Protected site)

```
C:\HORCM\etc>ren C:\WINDOWS\horcm0.conf horcm0_tmp.conf
C:\HORCM\etc>ren C:\WINDOWS\horcm0_delta.conf horcm0.conf
C:\HORCM\etc>ren C:\WINDOWS\horcm0_tmp.conf horcm0_delta.conf
```

       CCI 2 (Recovery site)

```
c:\HORCM\etc>ren C:\WINDOWS\horcm1.conf horcm1_tmp.conf
c:\HORCM\etc>ren C:\WINDOWS\horcm1_delta.conf horcm1.conf
c:\HORCM\etc>ren C:\WINDOWS\horcm1_tmp.conf horcm1_delta.conf
```

   c. Start the CCI instance.

Appendix B: Configuration with GAD, UR, and SRM

CCI 1 (Protected site)

```
c:\HORCM\etc>horcmstart 0
starting HORCM inst 0
HORCM inst 0 starts successfully.
```

CCI 2 (Recovery site)

```
c:\HORCM\etc>horcmstart 1
starting HORCM inst 1
HORCM inst 1 starts successfully.
```

3. Execute Test Recovery Plan from SRM2 at Site 3.

4. Confirm that VM is started normally at Site 3.

   Use VM to perform necessary operations, such as checking system operations after failover.

5. Perform Clean up from SRM2 at Site 3 and restore it to the initial status.

   For SRM operations, refer to "VMware Site Recovery Manager Documentation Center".

Failover from Site 1 or Site 2 to Site 3

When failures occur at both Site1 and Site 2, the user can migrate the system to Site 3 by performing failover at Site 3.

Failover can be performed when failures occur at both Site 1 and Site 2.

Before failover starts
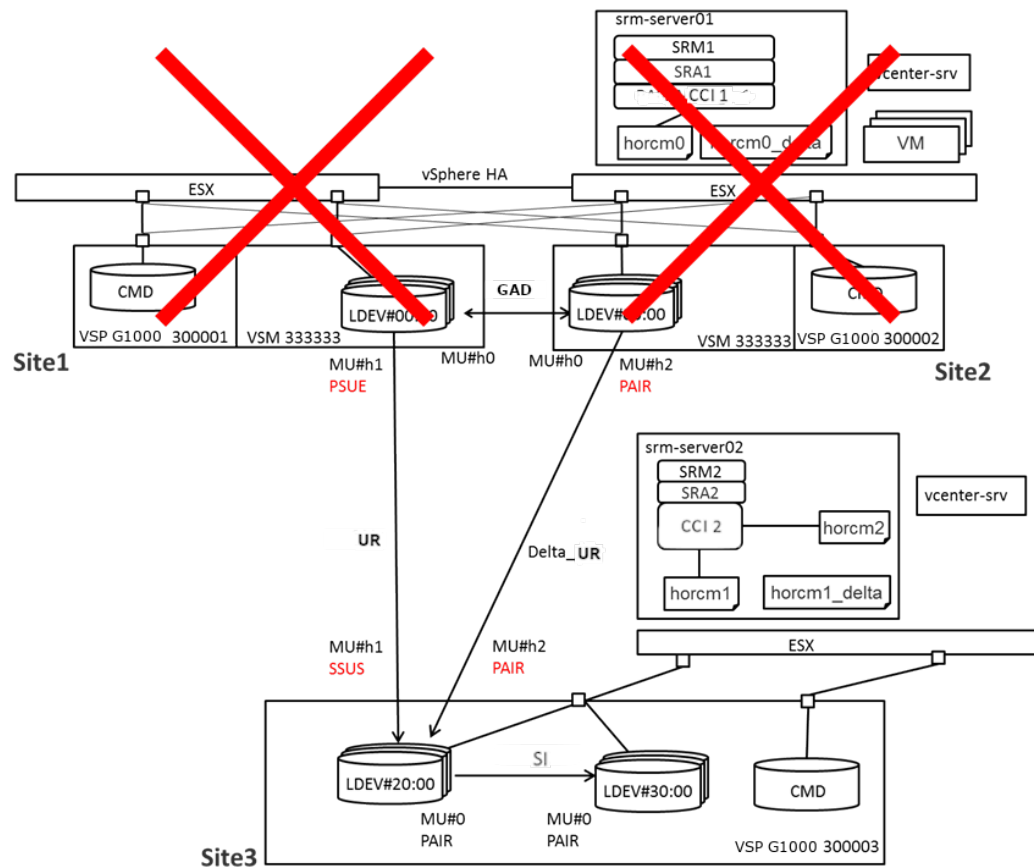
CCI 1 (Protected site)

```
c:\HORCM\etc>pairdisplay -g UR -IH0 -fx
Group   PairVol(L/R) (Port#,TID, LU),Seq#,LDEV#.P/S,Status,Fence,Seq#,P-
LDEV# M
UR     UR_dev1(L) (CL3-A-0, 0,   0)333333   0.P-VOL PSUE ASYNC ,300003
2000 -
UR     UR_dev1(R) (CL1-A-0,26,   0)300003  2000.S-VOL SSUS ASYNC ,-----    0 -
UR     UR_dev2(L) (CL3-A-0, 0,   1)333333   1.P-VOL PSUE ASYNC ,300003
2001 -
UR     UR_dev2(R) (CL1-A-0,26,   1)300003  2001.S-VOL SSUS ASYNC ,-----    1 -
UR     UR_dev3(L) (CL3-A-0, 0,   2)333333   2.P-VOL PSUE ASYNC ,300003
2002 -
UR     UR_dev3(R) (CL1-A-0,26,   2)300003  2002.S-VOL SSUS ASYNC ,-----    2 -
```

CCI 2 (Recovery site)

```
c:\HORCM\etc>pairdisplay -g UR -IH1 -fx
Group   PairVol(L/R) (Port#,TID, LU),Seq#,LDEV#.P/S,Status,Fence,Seq#,P-
LDEV# M
UR     UR_dev1(L) (CL1-A-0,26,   0)300003  2000.S-VOL SSUS ASYNC ,-----    0
-
UR     UR_dev1(R) (CL3-A-0, 0,   0)333333   0.P-VOL PSUE ASYNC ,300003
```

```
2000 -
UR    UR_dev2(L) (CL1-A-0,26,   1)300003  2001.S-VOL SSUS ASYNC ,-----    1
-
UR    UR_dev2(R) (CL3-A-0, 0,   1)333333     1.P-VOL PSUE ASYNC ,300003
2001 -
UR    UR_dev3(L) (CL1-A-0,26,   2)300003  2002.S-VOL SSUS ASYNC ,-----    2
-
UR    UR_dev3(R) (CL3-A-0, 0,   2)333333     2.P-VOL PSUE ASYNC ,300003
2002 -

c:\HORCM\etc>pairdisplay -g SI -IM1 -fx
Group   PairVol(L/R) (Port#,TID, LU-M) ,Seq#,LDEV#.P/S,Status, Seq#,P-
LDEV# M
SI      SI_dev1(L)  (CL1-A-0,26,   0-0 )300003  2000.P-VOL PAIR,300003
3000 -
SI      SI_dev1(R)  (CL1-A-0,26,   3-0 )300003  3000.S-VOL PAIR,-----
2000 -
SI      SI_dev2(L)  (CL1-A-0,26,   1-0 )300003  2001.P-VOL PAIR,300003
3001 -
SI      SI_dev2(R)  (CL1-A-0,26,   4-0 )300003  3001.S-VOL PAIR,-----
2001 -
SI      SI_dev3(L)  (CL1-A-0,26,   2-0 )300003  2002.P-VOL PAIR,300003
3002 -
SI      SI_dev3(R)  (CL1-A-0,26,   5-0 )300003  3002.S-VOL PAIR,-----
2002 -
```

Operational procedure of Failover

The following shows the operational flow of Test Failover.

1. Check the MU number that is used by the UR pair at Site 3.

```
c:\HORCM\etc>raidcom get journal -IH1 -fx
JID MU CTG  JNLS  AP  U(%)    Q-Marker   Q-CNT  D-SZ(BLK)   Seq# Num
LDEV#
001  1   1  SJNS   1   0      2c9753a2       0   20213760   300002   1
322
001  2   0  SJNN   0   0      2c9753a2       0   20213760   300002   1
322
```

2. If the MU number that is described in the horcm file running at Site 3 is different from the MU number that is identified in Step 1., switch to the horcm file of the corresponding MU number.

```
C:\HORCM\etc>type C:\WINDOWS\horcm1.conf
(omitted)
HORCM_LDEV
#GRP            DEV            SERIAL  LDEV#   MU#
UR    UR_dev1        300003  20:00   h1
UR    UR_dev2        300003  20:01   h1
```

```
UR    UR_dev3        300003  20:02   h1
(omitted)
```

   a. Stop CCI instance 1 from CCI 2.

```
c:\HORCM\etc>horcmshutdown 1
inst 1:
HORCM Shutdown inst 1 !!!
```

   b. Change the file name of the configuration definition file of Site 3.

```
c:\HORCM\etc>ren C:\WINDOWS\horcm1.conf horcm1_tmp.conf
c:\HORCM\etc>ren C:\WINDOWS\horcm1_delta.conf horcm1.conf
c:\HORCM\etc>ren C:\WINDOWS\horcm1_tmp.conf horcm1_delta.conf
```

   c. Start CCI instance 1 from CCI 2.

```
c:\HORCM\etc>horcmstart 1
starting HORCM inst 1
HORCM inst 1 starts successfully.
```

3. Check the UR pair status and confirm that Delta Resync is not running.

   If the UR pair status is COPY, wait until the status is changed to PAIR.

```
c:\HORCM\etc>pairdisplay -g UR -IH1 -fx
Group   PairVol(L/R) (Port#,TID, LU),Seq#,LDEV#.P/S,Status,Fence,Seq#,
P-LDEV# M
UR    UR_dev1(L) (CL1-A-0,26,   0)300003  2000.S-VOL PAIR ASYNC ,-----
1000 -
UR    UR_dev1(R) (CL3-A-0, 0,   0)333333    0.P-VOL PSUE ASYNC ,
300003  2000 -
UR    UR_dev2(L) (CL1-A-0,26,   1)300003  2001.S-VOL PAIR ASYNC ,-----
1001 -
UR    UR_dev2(R) (CL3-A-0, 0,   1)333333    1.P-VOL PSUE ASYNC ,
300003  2001 -
UR    UR_dev3(L) (CL1-A-0,26,   2)300003  2002.S-VOL PAIR ASYNC ,-----
1002 -
UR    UR_dev3(R) (CL3-A-0, 0,   2)333333    2.P-VOL PSUE ASYNC ,
300003  2002 -
```

4. Execute Recovery plan (Disaster Recovery) from SRM2 at Site 3.

**5.** Confirm that VM is started normally at Site 3.

For SRM operations, refer to "VMware Site Recovery Manager Documentation Center".

Failback from Site 3 to Site 1

With GAD+UR+SRM, when failback is performed, the system that was migrated to Site 3 can be restored to Site 1.

Failback can be performed only when all sites are running without a failure and all the requirements for GAD+UR+SRM are met (See GAD+UR+SRM restrictions (on page 79)).

Before Failback starts
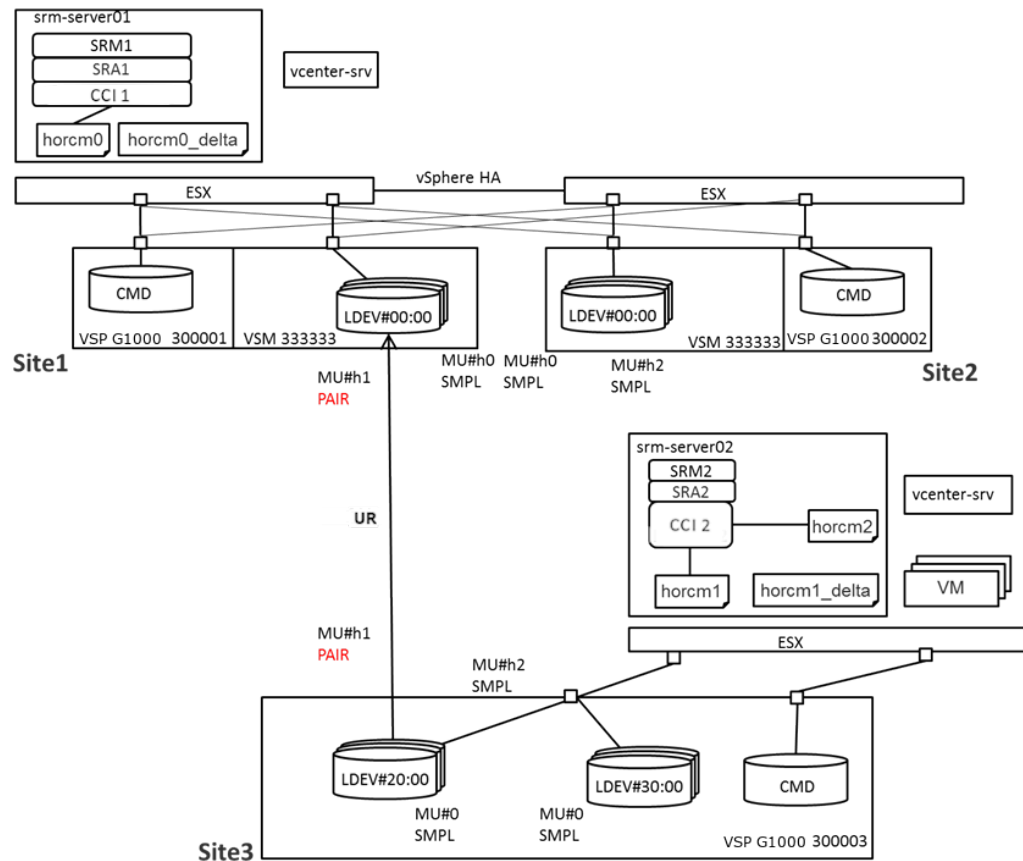
CCI 1(Protected site)

```
c:\HORCM\etc>pairdisplay -g UR -I0 -fcx
Group   PairVol(L/R) (Port#,TID, LU),Seq#,LDEV#.P/S,Status,Fence,   %,P-
LDEV# M
UR    UR_dev1(L) (CL3-A-0, 0,   0)333333    0.S-VOL PAIR ASYNC ,   0
2000 -
UR    UR_dev1(R) (CL1-A-0,26,   0)300003  2000.P-VOL PAIR ASYNC ,   0
0 -
UR    UR_dev2(L) (CL3-A-0, 0,   1)333333    1.S-VOL PAIR ASYNC ,   0
2001 -
UR    UR_dev2(R) (CL1-A-0,26,   1)300003  2001.P-VOL PAIR ASYNC ,   0
1 -
UR    UR_dev3(L) (CL3-A-0, 0,   2)333333    2.S-VOL PAIR ASYNC ,   0
2002 -
UR    UR_dev3(R) (CL1-A-0,26,   2)300003  2002.P-VOL PAIR ASYNC ,   0
2 -
```

CCI 2(Recovery site)

```
c:\HORCM\etc>pairdisplay -g UR -I1 -fcx
Group   PairVol(L/R) (Port#,TID, LU),Seq#,LDEV#.P/S,Status,Fence,   %,P-
LDEV# M
UR    UR_dev1(R) (CL1-A-0,26,   0)300003  2000.P-VOL PAIR ASYNC ,    0
0 -
UR    UR_dev1(L) (CL3-A-0, 0,   0)333333     0.S-VOL PAIR ASYNC ,    0
2000 -
UR    UR_dev2(R) (CL1-A-0,26,   1)300003  2001.P-VOL PAIR ASYNC ,    0
1 -
UR    UR_dev2(L) (CL3-A-0, 0,   1)333333     1.S-VOL PAIR ASYNC ,    0
2001 -
UR    UR_dev3(R) (CL1-A-0,26,   2)300003  2002.P-VOL PAIR ASYNC ,    0
2 -
UR    UR_dev3(L) (CL3-A-0, 0,   2)333333     2.S-VOL PAIR ASYNC ,    0
2002 -

c:\HORCM\etc>pairdisplay -g SI -IM1 -fcx
Group   PairVol(L/R) (Port#,TID, LU-M) ,Seq#,LDEV#.P/S,Status,   % ,P-
LDEV# M
SI     SI_dev1(L)  (CL1-A-0,26,   0-0 )300003  2000.SMPL  ----,-----   ----
- -
SI     SI_dev1(R)  (CL1-A-0,26,   3-0 )300003  3000.SMPL  ----,-----   ----
- -
SI     SI_dev2(L)  (CL1-A-0,26,   1-0 )300003  2001.SMPL  ----,-----   ----
- -
SI     SI_dev2(R)  (CL1-A-0,26,   4-0 )300003  3001.SMPL  ----,-----   ----
- -
SI     SI_dev3(L)  (CL1-A-0,26,   2-0 )300003  2002.SMPL  ----,-----   ----
- -
SI     SI_dev3(R)  (CL1-A-0,26,   5-0 )300003  3002.SMPL  ----,-----   ----
- -
```

Operational procedure of Failback

The following shows the operational flow of Test Failback.

1. Check if the requirements of failback are met. For the requirements, see GAD+UR+SRM restrictions (on page 79). If the requirements are not met, contact customer support (See Contact Information (on page 9)) and perform failback without using SRM.

2. If the MU numbers that are described in the horcm files running at both Protected site and Recovery site are not h1, switch to the horcm file in which the MU number is h1.

CCI 1 (Protected site)

```
c:\HORCM\etc>type c:\windows\horcm0.conf
(omitted)
HORCM_LDEV
#GRP     DEV          SERIAL     LDEV#     MU#
```

```
UR          UR_dev1    333333     00:00      h2
UR          UR_dev2    333333     00:01      h2
UR          UR_dev3    333333     00:02      h2
(omitted)
```

CCI 2 (Recovery site)

```
c:\HORCM\etc>type c:\windows\horcm1.conf
(omitted)
HORCM_LDEV
#GRP    DEV          SERIAL     LDEV#     MU#
UR          UR_dev1     300003     20:00     h2
UR          UR_dev2     300003     20:01     h2
UR          UR_dev3      300003     20:02      h2
(omitted)
```

   a. Stop the RAID Manager instance.

      CCI 1 (Protected site)

```
c:\HORCM\etc>horcmshutdown 0
inst 0:
HORCM Shutdown inst 0 !!!
```

      CCI 2 (Recovery site)

```
c:\HORCM\etc>horcmshutdown 1
inst 1:
HORCM Shutdown inst 1 !!!
```

   b. Change the file name of the configuration definition file.

      CCI 1 (Protected site)

```
C:\HORCM\etc>ren C:\WINDOWS\horcm0.conf horcm0_tmp.conf
C:\HORCM\etc>ren C:\WINDOWS\horcm0_delta.conf horcm0.conf
C:\HORCM\etc>ren C:\WINDOWS\horcm0_tmp.conf horcm0_delta.conf
```

      CCI 2 (Recovery site)

```
C:\HORCM\etc>ren C:\WINDOWS\horcm1.conf horcm1_tmp.conf
C:\HORCM\etc>ren C:\WINDOWS\horcm1_delta.conf horcm1.conf
C:\HORCM\etc>ren C:\WINDOWS\horcm1_tmp.conf horcm1_delta.conf
```

   c. Start the CCI instance.

      CCI 1 (Protected site)

```
c:\HORCM\etc>horcmstart 0
starting HORCM inst 0
HORCM inst 0 starts successfully.
```

Appendix B: Configuration with GAD, UR, and SRM

CCI 2 (Recovery site)

```
c:\HORCM\etc>horcmstart 1
starting HORCM inst 1
HORCM inst 1 starts successfully.
```

3. Execute Recovery Plan (Planned Migration) from SRM1 at Protected site (Site 1, Site 2). If Protected site is recovered after Disaster Recovery, Recovery Plan (Planned Migration) needs to be executed according to the SRM requirement.

4. Perform Reprotect from SRM1 at Protected site (Site 1, Site 2).

   As a result of the Reprotect operation, a UR pair of Site 1 (primary site) and Site 3 (secondary site) is created, and the data at Site 1 is copied to Site 3.

5. Confirm that VM is started normally at Site 1.

6. Re-create a GAD pair and a UR pair by using Device Manager - Storage Navigator or CCI.

For SRM operations, refer to "VMware Site Recovery Manager Documentation Center".

Hitachi Vantara