

Hitachi Storage Replication Adapter Software VMware vCenter Site Recovery Manager Deployment Guide

FASTFIND LINKS

[Document Organization](#)

[Product Version](#)

[Getting Help](#)

[Contents](#)

Copyright © 2009 Hitachi Data Systems Corporation,
ALL RIGHTS RESERVED

Notice: No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Hitachi Data Systems Corporation (hereinafter referred to as "Hitachi Data Systems").

Hitachi Data Systems reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. Hitachi Data Systems products and services can only be ordered under the terms and conditions of Hitachi Data Systems' applicable agreements. All of the features described in this document may not be currently available. Refer to the most recent product announcement or contact your local Hitachi Data Systems sales office for information on feature and product availability.

This document contains the most current information available at the time of publication. When new and/or revised information becomes available, this entire document will be updated and distributed to all registered users.

Hitachi is a registered trademark of Hitachi, Ltd. in the United States and other countries. Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd. in the United States and other countries.

ESCON, IBM, and z/OS are registered trademarks of International Business Machines Corporation.

All other trademarks, service marks, and company names in this document are properties of their respective owners.



Contents

Preface	v
Intended Audience	vi
Product Version	vi
Document Revision Level	vi
Changes in This Release	vi
Document Organization	vi
Document Conventions	vii
Convention for Storage Capacity Values	vii
Getting Help	viii
Comments	viii
1 Planning for Deployment	1-1
Deployment Requirements	1-2
VMware Environment Requirements	1-2
Hitachi Software Requirements	1-2
Enable SPC-2 mode	1-3
Set Host Group Options for Hitachi AMS/WMS Systems	1-3
Running virtual machines from VMFSs/LUNs	1-4
Set Host Group Options for Hitachi AMS 2000 Family	1-13
Responsibilities	1-15
Customer Responsibilities	1-15
Hitachi Data Systems Responsibilities	1-15
Deployment Planning Tasks	1-15
2 Deployment	2-1
Verify the Hitachi Storage Replication Adapter version	2-2
Checking the version on a Windows Server	2-2
Checking the version on a Linux CCI Server	2-2
Upgrade to the Hitachi SRA 2.0	2-3
Upgrading the RAID Manager CCI	2-3
Upgrading the Storage Replication Adapter	2-4

Installing the SRA 2.0	2-4
Storage Replication Adapter 2.0 Options	2-5
RAID Manager CCI HORCM Configuration Considerations	2-5
Example of HORCM Configuration Files	2-6
Scenarios	2-9
Using TrueCopy or Hitachi Universal Replicator with ShadowImage	2-9
Using TrueCopy or Hitachi Universal Replicator Only	2-10
Mixing	2-11
RAID Mgr CCI HORCM Mixed Scenario Configuration Considerations. . .	2-11
Creating ShadowImage Pairs	2-15
Environment Variables	2-15
Setting Environment Variables on the SRM Host	2-15
Setting Environment Variables on a UNIX Host	2-16
Configuring Array Managers in Site Recovery Manager	2-16
When CCI Resides on the Windows SRM Server	2-17
When CCI resides on a Linux Server	2-17
Recovering from a Failover.	2-18
Recovering Replication on USP, NSC, USP V and USP VM	2-19
Reverse Replication, Protected site on-line	2-19
Reverse Replication, Protected site off-line.	2-19
Recovering replication	2-19
Troubleshooting the SRA 2.0	2-20
Error Messages on SRM Log Files	2-20
Errors in XML received from SRM	2-20
RAID Manager command Errors in rmsra.exe	2-21
Configuration and Status errors	2-23
Multiple Error Codes	2-24
Failure to launch scripts	2-25
UNIX CCI Server	2-25
Windows CCI Server	2-26
Test failover errors	2-26
Collecting Information Before Contacting Customer Support	2-28
SRM/SRA local configuration.	2-28
SRM/SRA remote configuration	2-29



Preface

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

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

This preface includes the following information:

- [Intended Audience](#)
- [Product Version](#)
- [Document Revision Level](#)
- [Document Organization](#)
- [Document Conventions](#)
- [Convention for Storage Capacity Values](#)
- [Getting Help](#)
- [Comments](#)

Intended Audience

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

This document assumes the following:

- The user has a working knowledge of Hitachi Data Systems storage management tools including Hitachi Command Control Interface (CCI) software.
- The user has an understanding of Windows systems, and if a Linux server is intended for use as a CCI server, working knowledge of Linux system administration.

Product Version

This document applies to the Storage Replication Adapter version 2.0, which has a subcomponent RMSRA (RAID Manager Storage Replication Adapter) version 01.00.08.

Document Revision Level

Revision	Date	Description
MK-09RM6745-00	April 2009	Initial release
MK-09RM6745-01	May 2009	This revision supersedes revision 00.

Changes in This Release

The following new information is included in this release of the document:

- Added instructions for enabling SPC-2 Mode.





Document Organization

The following table provides an overview of the contents and organization of this document. Click the [chapter title](#) in the left column to go to that chapter. The first page of each chapter provides links to the sections in that chapter.

Chapter	Description
Chapter 1, Planning for Deployment	This chapter describes the pre-requisites for deployment of the VMware vCenter Site Recovery Manager with the Storage Replication Adapter.
Chapter 2, Deployment	This chapter provides instructions for the deployment of the Storage Replication Adapter (RMSRA).

Document Conventions

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

Icon	Meaning	Description
	Note	Calls attention to important and/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 (e.g., disruptive operations).
	WARNING	Warns the user of severe conditions and/or consequences (e.g., destructive operations).

Convention for Storage Capacity Values

Physical storage capacity values (e.g., disk drive capacity) are calculated based on the following values:

- 1 KB = 1,000 bytes
- 1 MB = 1,000² bytes
- 1 GB = 1,000³ bytes
- 1 TB = 1,000⁴ bytes
- 1 PB = 1,000⁵ bytes

Logical storage capacity values (e.g., logical device capacity) are calculated based on the following values:

- 1 KB = 1,024 bytes
- 1 MB = 1,024 KB or 1,024² bytes
- 1 GB = 1,024 MB or 1,024³ bytes
- 1 TB = 1,024 GB or 1,024⁴ bytes
- 1 PB = 1,024 TB or 1,024⁵ bytes
- 1 block = 512 bytes

Getting Help

If you need to call the Hitachi Data Systems Support Center, 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 message(s) displayed on the host system(s)
- The exact content of any message(s) displayed on the Storage Navigator.
- The service information messages (SIMs), including reference codes and severity levels, displayed by Storage Navigator.

See [Collecting Information Before Contacting Customer Support on page 2-28](#) for more information.

The Hitachi Data Systems customer support staff is available 24 hours a day, seven days a week. If you need technical support, please call:

- United States: +1 (800) 446-0744
- Outside the United States: +1 (858) 547-4526

Comments

Please send us your comments on this document:

doc.comments@hds.com

Include the document title, number, and revision, and refer to specific section(s) and paragraph(s) whenever possible.

Thank you! (All comments become the property of Hitachi Data Systems Corporation.)

Planning for Deployment

The Hitachi Storage Replication Adapter is the linkage between the VMware vCenter Site Recovery Manager (SRM) application and the Command Control Interface/RAID Manager software that is used to manage data replication and data protection operations. This new release of the Hitachi Storage Replication Adapter supports the Universal Storage Platform family and extends platform coverage to the Advanced Modular Storage family and Advanced Modular Storage 2000 family.

This chapter describes the pre-requisites for deployment of the VMware vCenter Site Recovery Manager with the Storage Replication Adapter. The following topics are discussed:

- ❑ [Deployment Requirements](#)
- ❑ [Responsibilities](#)
- ❑ [Deployment Planning Tasks](#)

Deployment Requirements

This section describes the requirements to be completed before installing the Hitachi Storage Replication Adapter.

The Hitachi Command Control Interface version 01-23-03/07 or later is required. Supported Operating systems include:

- Windows
- Linux
- Solaris
- Solaris/x86
- HP-UX
- AIX

The RAID Manager Storage Replication Adapter (RMSRA) version 01.00.08 is required.

VMware Environment Requirements

Before installing the Hitachi Storage Replication Adapter 2.0, the following VMware software must be installed on both sites:

- VMware vCenter Server, previously named VirtualCenter
- VMware vCenter Site Recovery Manager

Hitachi Software Requirements

Before completing the Site Recovery Manager deployment, the following Hitachi software license keys must be installed:

1. On USP, NSC, USP V or USP VM storage systems:
 - a. Remote replication using TrueCopy and/or Universal Replicator
 - b. Optional: local replication on the recovery site using ShadowImage or Copy-on-Write
2. On AMS family of storage processors:
 - a. Remote replication using TrueCopy or TrueCopy Extended
 - b. Optional: when using TrueCopy, ShadowImage or Copy-on-Write may be utilized for the recovery site. TrueCopy Extended Distance is not supported on AMS 200 or WMS 100.



NOTE: On Hitachi Adaptable Modular Storage, Hitachi Workgroup Modular Storage F/W version 08-60/C or higher is required.

3. For all Hitachi storage, the Hitachi Command Control Interface must be installed on both sites. This may be installed on either Windows or UNIX systems. If Windows is used it must be installed on the same server as the VMware vCenter Site Recovery Manager.

Enable SPC-2 mode

The Host Connection Mode 2 parameter “SPC-2 Mode” needs to be enabled for VMware vCenter Site Recovery Manager and Hitachi Storage Replication Adapter 2.0. It can, but is unnecessary, be enabled for a VMware Virtual Infrastructure environment (VMware ESX/ESXi Server, VMware vCenter Server) without using VMware vCenter Site Recovery Manager and Hitachi Storage Replication Adapter 2.0.



CAUTION! Do not enable SPC-2 Mode when ESX hosts are actively issuing I/O (i.e. when virtual machines are powered on) on the VMFSs mapped to the host group(s).

Set Host Group Options for Hitachi AMS/WMS Systems

Perform the following steps to set the Host Group Options.

1. Set the following Host Group Options for Hitachi Adaptable Modular Storage Systems (AMS/WMS), as shown in [Figure 1-1](#).
 - Platform: Solaris
 - Alternate Path: not specified
 - Failover: SunCluster
 - Host Connection Mode 1: Standard Mode
 - Host Connection Mode 2: all disabled

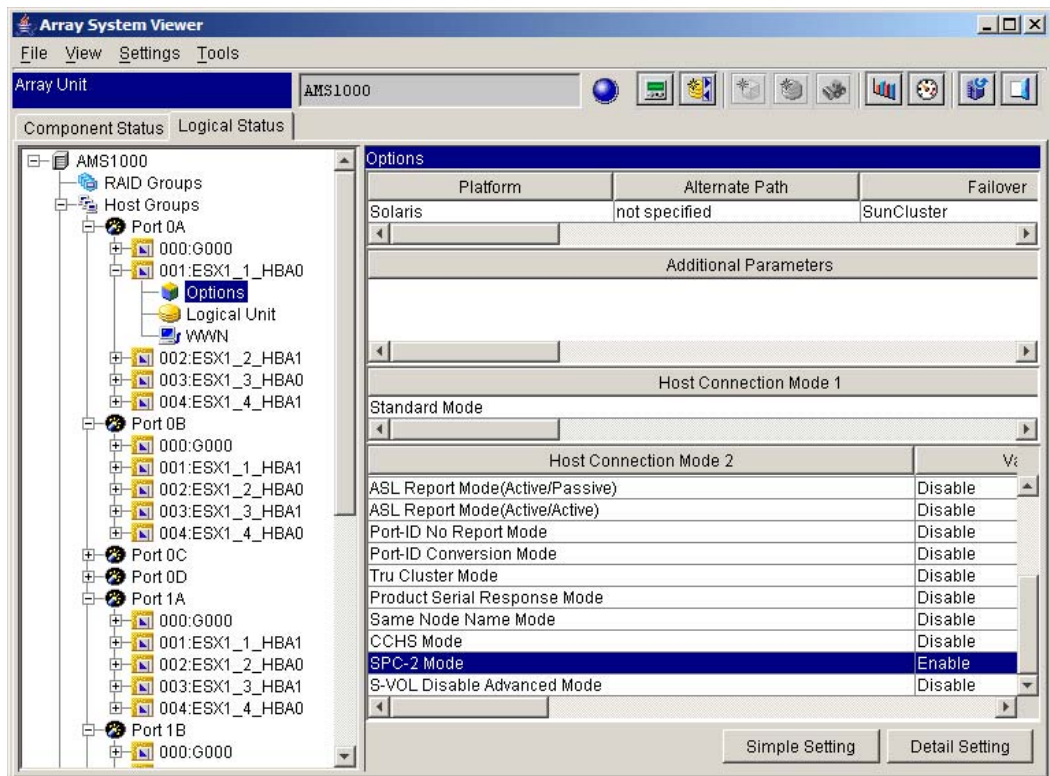


Figure 1-1: Host Group Options for AMS/WMS systems

2. Set the SPC-2 Mode parameter to **Enable** for VMware vCenter Site Recovery Manager and Hitachi Storage Replication Adapter 2.0.

Running virtual machines from VMFSs/LUNs

The procedure described below may also be used if you want to run virtual machines from VMFSs/LUNs that have been replicated or copied using Hitachi Universal Replicator, TrueCopy, TrueCopy Extended Distance, ShadowImage, Copy-on-Write, or when virtualizing storage systems with a Hitachi Universal Storage Platform V or VM storage system.

Once an LU is formatted with the VMFS by an ESX host, it writes a signature to the disk using information contained in SCSI inquiry page 83, including:

- Serial number of the storage system
- Internal LU ID (LDKC:CU:LDEV, LDEV)
- External LU ID (host LUN)

Whenever an ESX host has access to a VMFS, it reads and compares the signature with its current view. If it does not match, the host disables access to the VMFS (not the LU) by default and generates a warning similar to the following in the event log and on the ESX Server console:

ALERT: LVM: 4941: vmhba0:0:1:1 may be a snapshot: disabling access. See resignaturing section in the SAN config guide.

Enabling SPC-2 Mode changes the information provided in the SCSI inquiry page 83, and VMware ESX/ESXi hosts will therefore treat the LU as a "snapshot" LU.

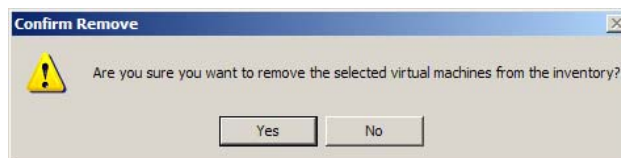
Perform the following steps:

1. Shutdown Virtual Machines.

Shut down all virtual machines on all VMFSs mapped to the host group(s) where SPC-2 Mode needs to be enabled.

2. Remove Virtual Machines from Inventory.

Remove all affected virtual machines from VMware inventory. Use VMware Virtual Infrastructure Client to connect to either the ESX/ESXi host directly or to VMware vCenter Server. Right click on each virtual machine and choose Remove from Inventory.



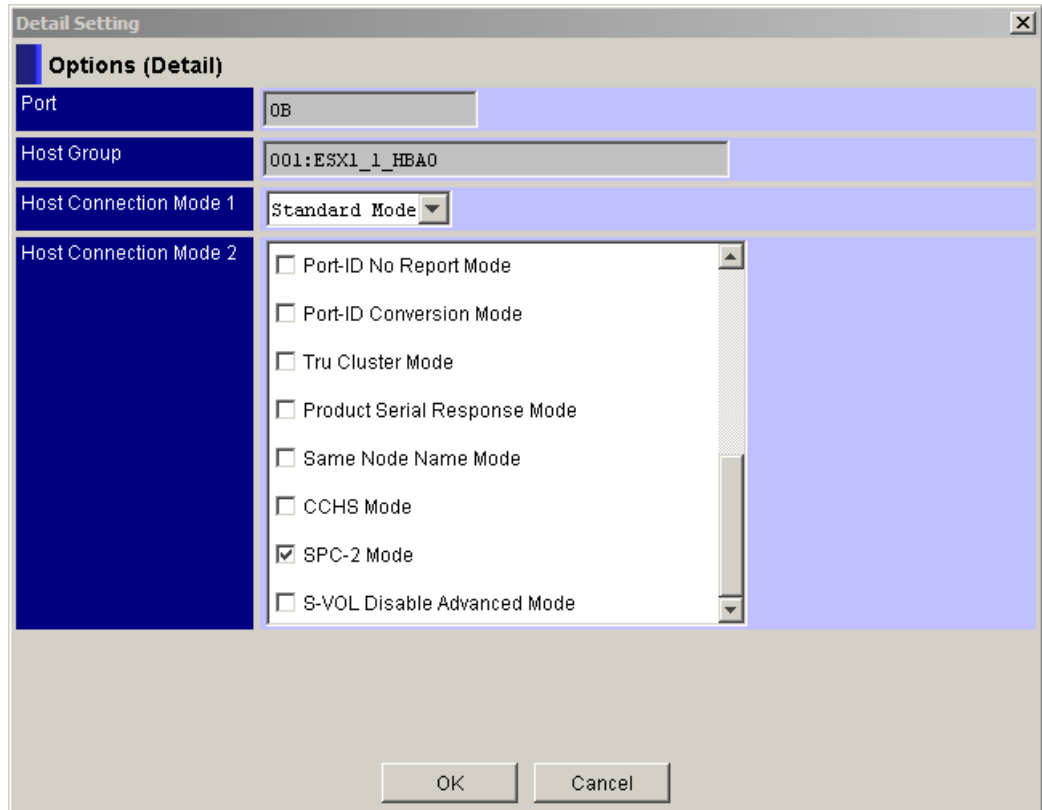
3. Enable SPC-2 Mode.

In Storage Navigator Modular highlight the Options of the host group, and click on Detail Setting.

Place a check next to SPC-2 Mode, and click OK.

Alternatively you may use Storage Navigator Modular Command Line Interface to enable SPC-2 Mode using the following command:

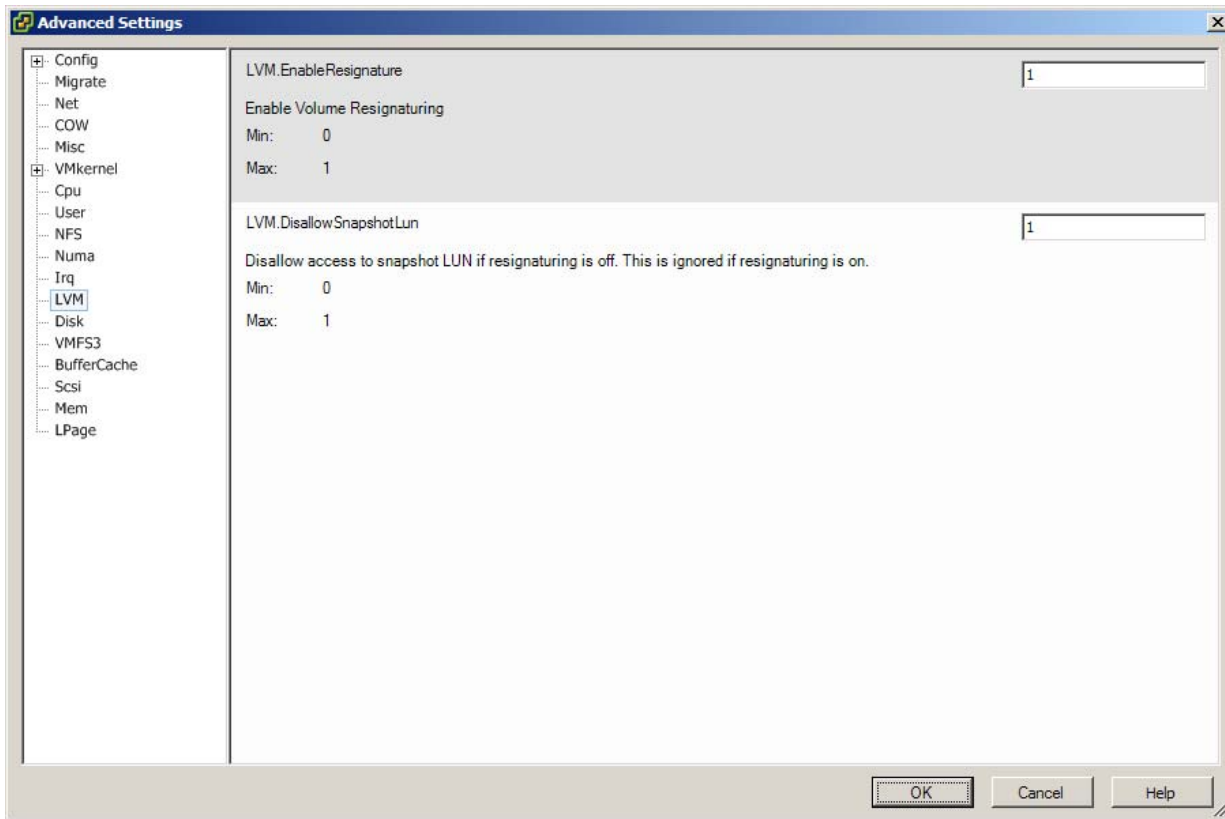
auhgopt -unit unit_name -set -SPC2 ctl_no port_no group_no enable



4. Enable Resignature.

On one ESX/ESXi host only (per VMFS), choose Host Configuration, Advanced Settings, LVM and set the LVM.EnableResignature parameter to 1, and click OK to enable resignaturing.

esxcfg-advcfg --set 1 /LVM/EnableResignature



5. Rescan Storage

Choose Host Configuration, select Storage Adapters from the Hardware list and click Rescan, then link. When a dialog box pops up, add a check mark to the *Scan for New Storage Devices* check box, and click OK.

6. Refresh Storage.

Choose Host Configuration, Storage and click on the blue Refresh link.

All VMFSs should now be visible. The datastore (Identification) has been renamed to "snap-xxxxxxx-<original datastore name>".

The screenshot displays the vSphere Host Configuration Manager interface. The top navigation bar includes tabs for Summary, Virtual Machines, Resource Allocation, Performance, Configuration, Users & Groups, Events, and Permissions. The left sidebar shows the Hardware and Software sections. The main content area is divided into Storage and Details panels.

Storage Table:

Identification	Device	Capacity	Free	Type
SAN_2_6	vmhba0:0:6:1	511.75 GB	511.13 GB	vmfs3
snap-00000002-SAN_1_1	vmhba0:0:11:1	511.75 GB	502.38 GB	vmfs3
snap-00000002-SAN_1_2	vmhba0:0:12:1	511.75 GB	511.13 GB	vmfs3
snap-00000002-SAN_1_3	vmhba0:0:13:1	511.75 GB	510.13 GB	vmfs3
snap-00000002-SAN_1_4	vmhba0:0:14:1	511.75 GB	510.13 GB	vmfs3
snap-00000002-SAN_1_5	vmhba0:0:15:1	511.75 GB	510.13 GB	vmfs3
snap-00000002-SAN_1_6	vmhba0:0:16:1	511.75 GB	511.13 GB	vmfs3

Details for SAN_2_3:

- Location: /vmfs/volumes/46b1c9f7-f2...
- Capacity: 511.75 GB
- Used: 634.00 MB
- Free: 511.13 GB

Path Selection:

Path Selection	Properties	Extents
Most Recently Used	Volume Label: SAN_2_3	vmhba0:0:3:1 512.00 ...
	Datastore Name: SAN_2_3	Total Formatted Capacity 511.75 ...

Paths:

Total:	4
Broken:	0
Disabled:	0

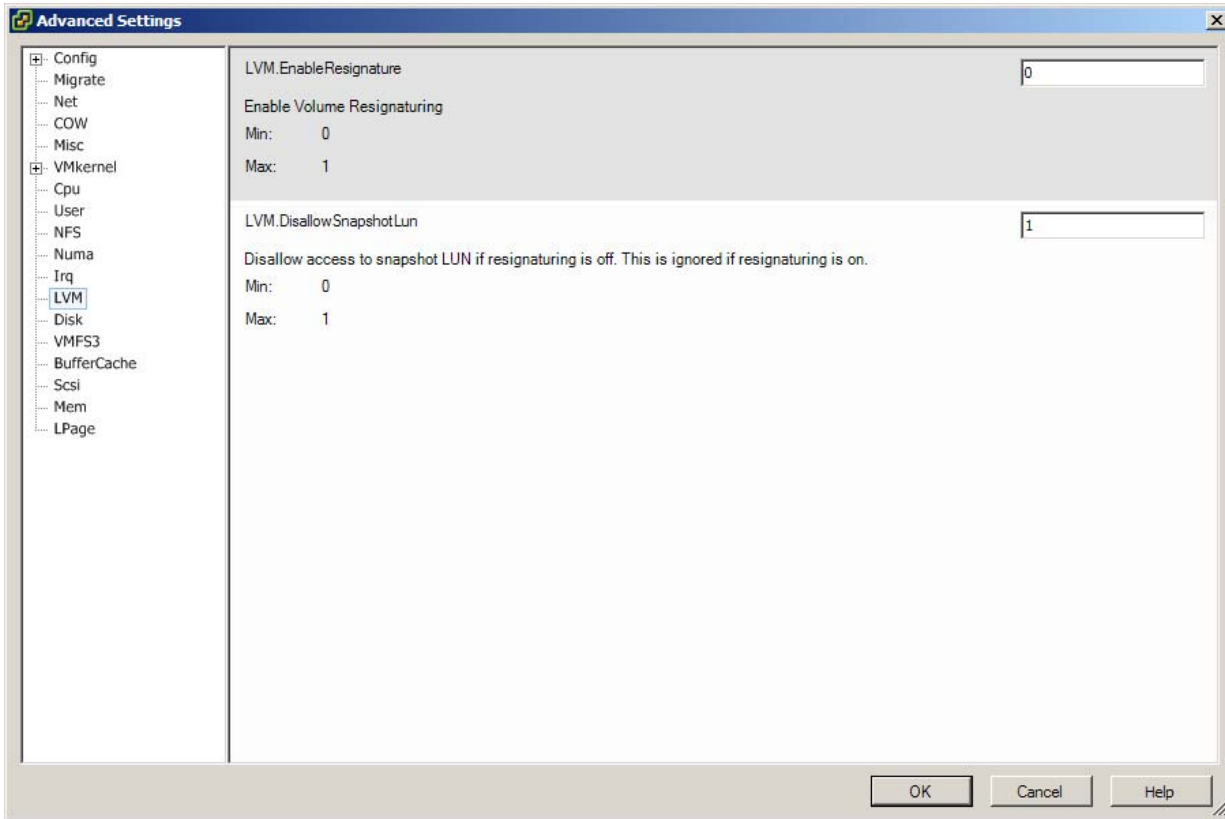
Formatting:

File System:	VMFS 3.21
Block Size:	1 MB

7. Disable Resignature.

Choose Host Configuration, Advanced Settings, LVM and set the LVM.EnableResignature parameter back to its default of 0, and click OK.

esxcfg-advcfg --set 0 /LVM/EnableResignature



8. Rename the Datastores.

Rename the datastores to its old or original names and choose Host Configuration, Storage, and click the blue Refresh link on each of the remaining ESX hosts (cluster members) with access to the affected VMFSs to make sure every ESX/ESXi host has been successfully updated.

It might be necessary to go to Datastores in VMware vCenter and remove any references left to the old or original datastore names before renaming them.

The screenshot shows the VMware vCenter interface for configuring storage. The top navigation bar includes Summary, Virtual Machines, Resource Allocation, Performance, Configuration, Users & Groups, Events, and Permissions. The left sidebar has Hardware and Software sections. The main area is titled 'Storage' and contains a table of datastores, a 'Details' section for the selected 'SAN_2_1' datastore, and a 'Properties...' link.

Identification	Device	Capacity	Free	Type
SAN_1_6	vmhba0:0:16:1	511.75 GB	511.13 GB	vmfs3
SAN_2_1	vmhba0:0:1:1	511.75 GB	511.13 GB	vmfs3
SAN_2_2	vmhba0:0:2:1	511.75 GB	511.13 GB	vmfs3
SAN_2_3	vmhba0:0:3:1	511.75 GB	511.13 GB	vmfs3
SAN_2_4	vmhba0:0:4:1	511.75 GB	511.13 GB	vmfs3
SAN_2_5	vmhba0:0:5:1	511.75 GB	511.13 GB	vmfs3
SAN_2_6	vmhba0:0:6:1	511.75 GB	511.13 GB	vmfs3

Details for SAN_2_1:

- Capacity: 511.75 GB
- Location: /vmfs/volumes/46b1c9b6-6...
- Used: 634.00 MB
- Free: 511.13 GB

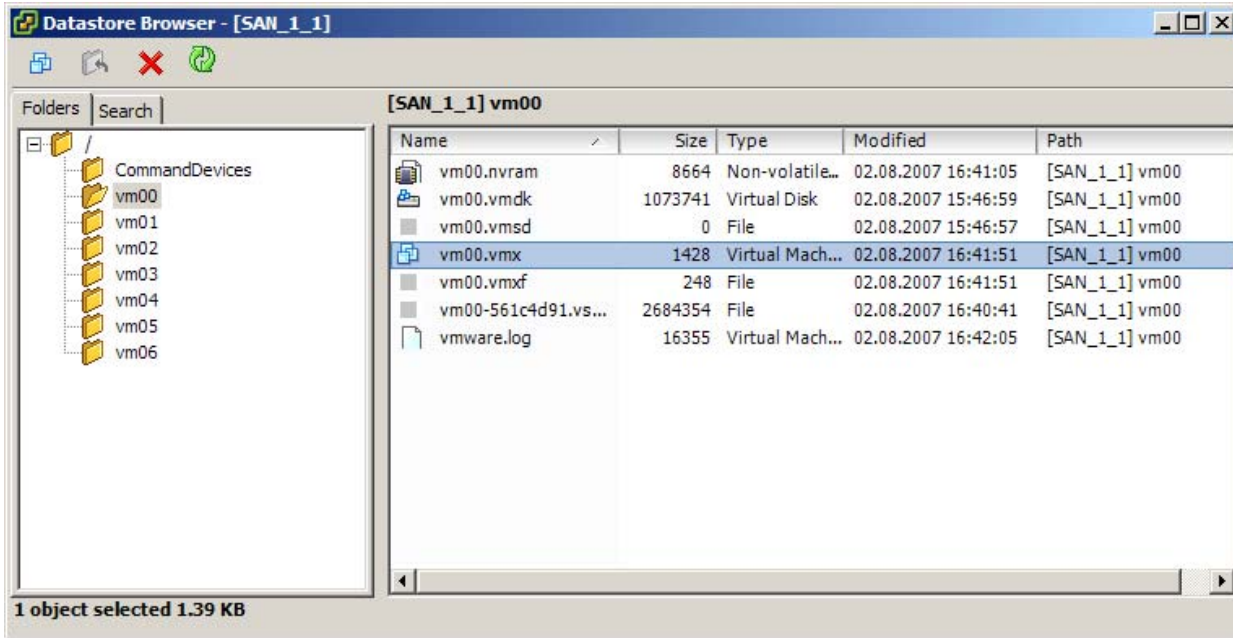
Path Selection	Properties	Extents
Most Recently Used	Volume Label: SAN_2_1	vmhba0:0:1:1 512.00 ...
	Datastore Name: SAN_2_1	Total Formatted Capacity 511.75 ...

Paths	Formatting
Total: 4	File System: VMFS 3.21
Broken: 0	Block Size: 1 MB
Disabled: 0	

9. Re-register Virtual Machines.

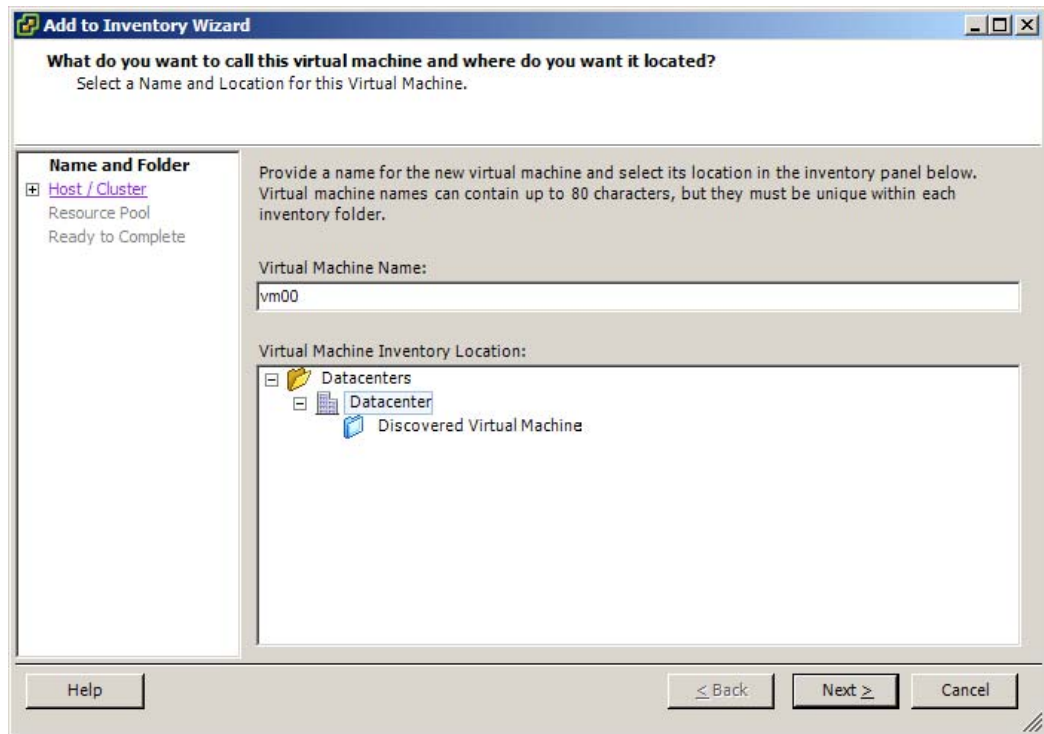
Browse each datastore for .vmx files (virtual machine configuration files) and re-register each affected virtual machine by right-clicking on the .vmx file and choosing Add to Inventory.

Command line tools (COS, Remote CLI) can be used to automate or script this process (e.g. `vmware-cmd -s register /vmfs/.../vm00/vm00.vmx`)



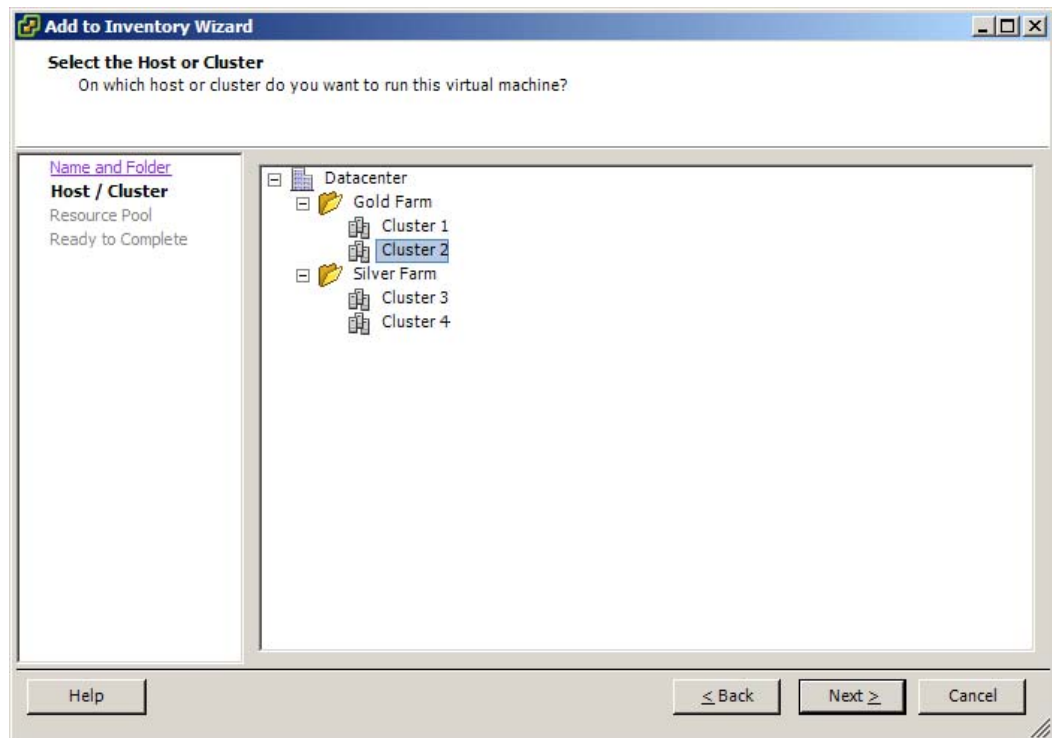
10. Add to Inventory Wizard.

Provide a name for the virtual machine and select its location in the inventory panel.



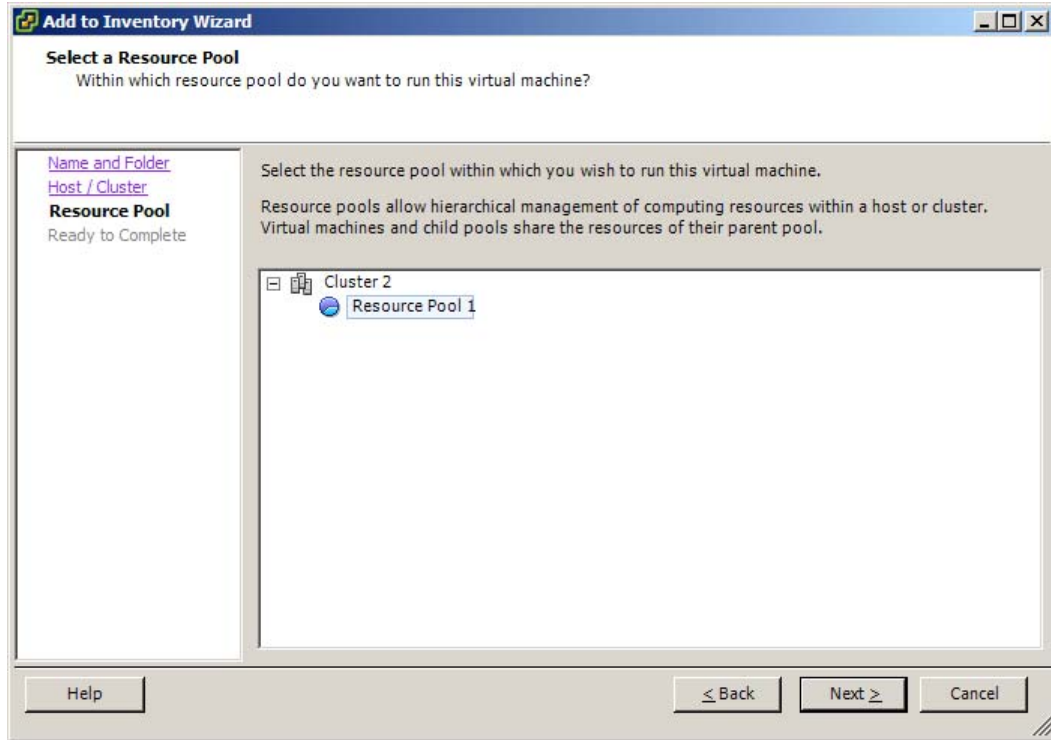
11. Select the Host or Cluster.

Select the Host or Cluster where you want the virtual machine to run.



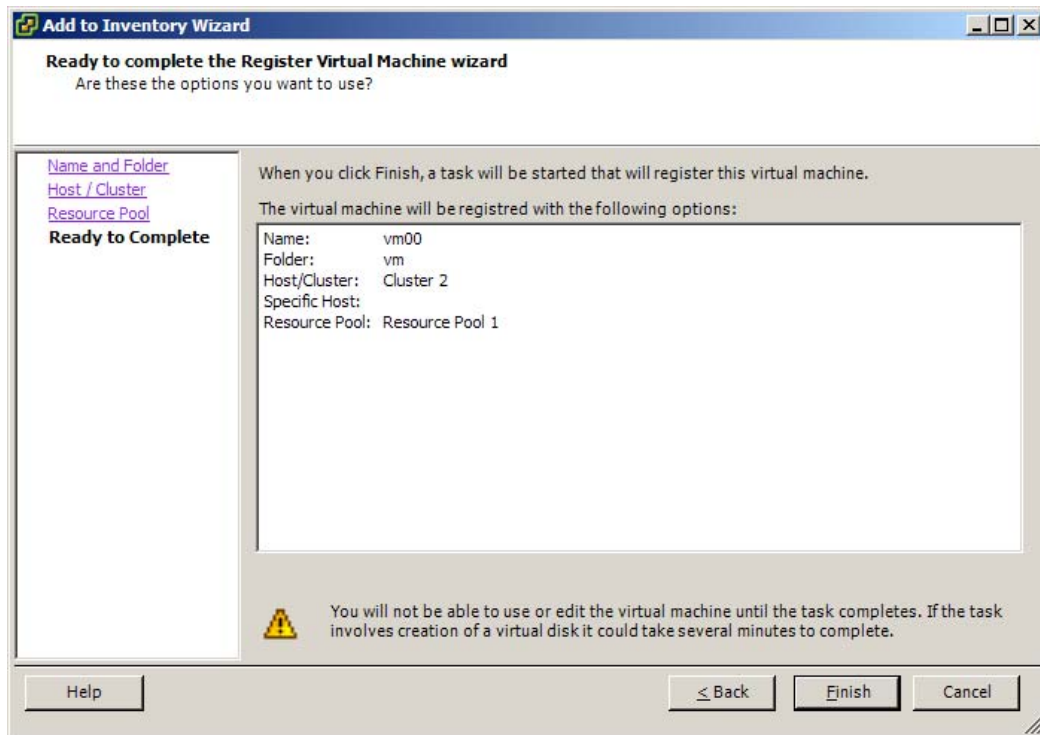
12. Select a Resource Pool.

Select the resource pool where you want to run the virtual machine.



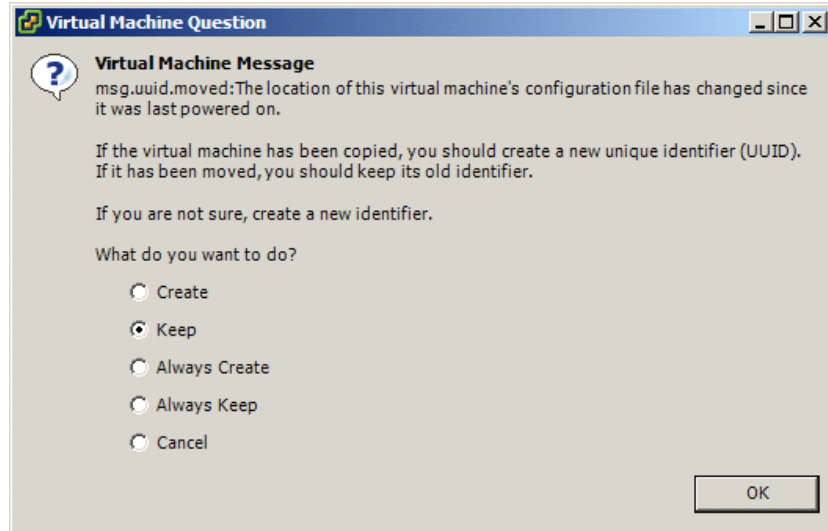
13. Finalize.

Click Finish. The virtual machine should now appear in the inventory view.



14. Start the Re-registered Virtual Machine.

Choose Keep and click OK.



15. Repeat these steps for every VMFS.

Set Host Group Options for Hitachi AMS 2000 Family

Set the following Host Group Options for the Hitachi Adaptable Modular Storage Systems 2000, as shown in [Figure 1-2](#).

- Platform: VMware
- Middleware: not specified
- Common Setting: Standard Mode
- Additional Setting: all disabled (unchecked)

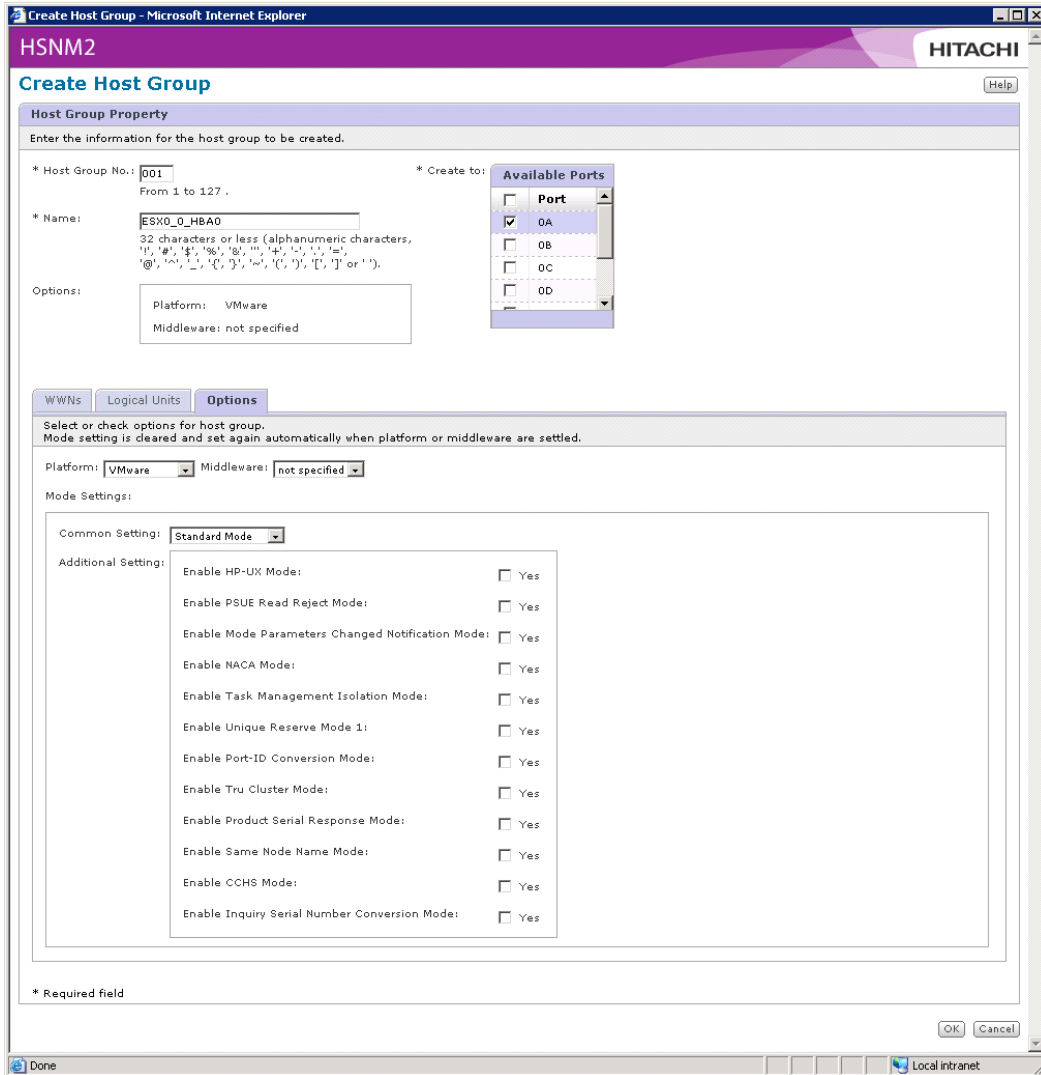


Figure 1-2: Host Group Options for Hitachi Adaptable Modular Storage 2000 Family

Responsibilities

The responsibilities for installation planning are shared by the customer and the Hitachi Data Systems account team. The required installation planning tasks must be scheduled and completed to ensure successful and efficient deployment of the Storage Replication Adapter 2.0.

Customer Responsibilities

You are responsible for providing customer-supplied hardware required for the Storage Replication Adapter.

Hitachi Data Systems Responsibilities

Your Hitachi Data Systems account team will assist you throughout the installation planning process.

The Hitachi Data Systems account team is responsible for:

- Assisting you as needed during the installation planning process for your specific site and operational configuration
- Coordinating Hitachi Data Systems resources to ensure a successful installation and configuration

Deployment Planning Tasks

You, the customer, are responsible for performing the following tasks, with assistance as needed from the Hitachi Data Systems account team, to prepare for deployment of the VMware vCenter Site Recovery Manager:

1. **Read this document** carefully to understand the installation requirements for the VMware vCenter Site Recovery Manager and Storage Replication Adapter.
2. **Provide the customer-supplied hardware** required for installation and configuration.
3. **Work with your Hitachi Data Systems account team** during the deployment planning process.

Deployment

This chapter provides instructions for the deployment of the RAID Manager Storage Replication Adapter (RMSRA, or simply SRA). The following topics are discussed:

- ❑ [Verify the Hitachi Storage Replication Adapter version](#)
- ❑ [Upgrade to the Hitachi SRA 2.0](#)
- ❑ [Installing the SRA 2.0](#)
- ❑ [Storage Replication Adapter 2.0 Options](#)
- ❑ [RAID Manager CCI HORCM Configuration Considerations](#)
- ❑ [Scenarios](#)
- ❑ [Creating ShadowImage Pairs](#)
- ❑ [Environment Variables](#)
- ❑ [Configuring Array Managers in Site Recovery Manager](#)
- ❑ [Recovering from a Failover](#)
- ❑ [Troubleshooting the SRA 2.0](#)

Verify the Hitachi Storage Replication Adapter version

The CCI comes with an earlier version of the Storage Replication Adapter. You will need to verify which version is installed on your system. The following topics are covered in this section:

- ❑ [Checking the version on a Windows Server](#)
- ❑ [Checking the version on a Linux CCI Server](#)

Checking the version on a Windows Server

If you are running CCI on a Windows server, follow these steps to check the Storage Replication Adapter version:

1. Log in to the Windows server that is running SRM and CCI as an administrator.
2. Open a command prompt window.
3. Navigate to the c:\HORCM\etc folder.
4. Issue the following command:

```
rmsra -h
```

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

```
Ver&Rev: 01.00.04
```

5. Navigate to the C:\Program Files\VMware\VMware Site recovery Manager\scripts\SAN\RMHTC folder.
6. Issue the following command:

```
rmsra -h
```

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

```
Ver&Rev: 01.00.08
```

7. If the version numbers do not match or do not exist, as in the examples in this procedure, copy the rmsra.exe file from the RMSRA directory to the c:\HORCM\etc directory.

If both version numbers match and are equal to or greater than version 01.00.08, no action is needed.

Checking the version on a Linux CCI Server

1. Log in to the Linux CCI server as root.
2. Navigate to the /HORCM/usr/bin directory.
3. Issue the following command to display the version number of RMSRA that was installed with CCI:

```
./rmsra -h
```

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

Ver&Rev: 01.00.04

4. Using FTP, copy the `rmsra.linux` file from the SRA installation folder on the Windows SRM server to the `/HORCM/usr/bin` directory on the Linux server that is running CCI.
5. Issue the following command to make the `rmsra.linux` file executable:

```
chmod +x rmsra.linux
```

6. Issue the following command to display the version number of RMSRA that was installed with the SRA:

```
./rmsra.linux -h
```

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

Ver&Rev: 01.00.08

7. If the `rmsra.linux` version is newer than the `rmsra` version, or does not exist, as in the example in this procedure, rename the `rmsra.linux` file to `rmsra`.

If the `rmsra` version is newer than the `rmsra.linux` version, no action is needed.

Upgrade to the Hitachi SRA 2.0

You will need to perform an upgrade to the Hitachi Storage Replication Adapter 2.0 if the Storage Replication Adapter 1.0 is already installed.

The following topics are discussed in the section:

- [Upgrading the RAID Manager CCI](#)
- [Upgrading the Storage Replication Adapter](#)

Upgrading the RAID Manager CCI

The RAID Manager CCI needs to be upgraded to 01-23-03/06 or later. Check the version of your install by executing any CCI command using the `-h` option. For example:

```
raidscan -h
```

Perform the following steps if the CCI is an older version.

1. Remove the HORCM services on the Site Recovery Manager server by issuing the following commands:

```
cd \HORCM\tool
net stop HORCM<X>
svcxexe /S=HORCM<X> /D
```

2. Upgrade the CCI according to the installation steps in Chapter 3 of the *Hitachi Command Control Interface User and Reference Guide*.
3. Replace the HORCM services by issuing the following command:

```
C:\HORCM\tool\svcxexe /S=HORCM<X> /A=C:\HORCM\Tool\svcxexe.exe
<X> is the HORCM instance number.
```

Upgrading the Storage Replication Adapter

Follow these steps to upgrade from Storage Replication Adapter version 1.0 to version 2.0:

1. Open the Windows **Control Panel**.
2. Click **Add or Remove Programs**.
3. Select *Hitachi Storage Replication Adapter 1.0* from the list of currently installed programs.
4. Click **Remove**.
5. Open an Explorer window.
6. Navigate to the folder **C:\Program Files\VMware\VMware Site Recovery Manager\scripts\SAN**
7. Right-click on the Hitachi Storage Replication Adapter folder and click **Delete**.
8. Install the Storage Replication Adapter 2.0. See [Installing the SRA 2.0](#).

Installing the SRA 2.0

Download the Storage Replication Adapter from the VMware website once the Site Recovery Manager has been installed. After the Storage Replication Adapter is downloaded it is installed on the Site Recovery Manager servers on both the protected site and recovery site. In addition the RMSRA executable on the RAID Manager CCI installation will need to be updated.

1. Select the file RMHTCSRA.exe that was downloaded from VMware.
2. Verify the location of your VMware vCenter Site Recovery Manager Installation (change the installation folder if necessary).
3. Click **Install**.
4. When the install finishes, click **Finish**.
5. After the Storage Replication Adapter is installed, the Site Recovery Manager service will need to be restarted.
 - a. Right click on **My Computer** and select **Manage**.
 - b. Click on **Services and Application** then select **Services**.
 - c. Locate **VMware Site Recover Manager** and click **Restart**.

Storage Replication Adapter 2.0 Options

Storage Replication Adapter 2.0 can be configured to utilize either the TrueCopy/Hitachi Universal Replicator S-VOL or an additional snapshot volume for the purpose of testing failover without disrupting primary replication. This snapshot can be taken on the recovery site only with ShadowImage or Copy-on-Write. The Storage Replication Adapter 2.0 searches for a snapshot volume at mirror unit MU#0 by examining the HORCM pair groups and the status of these pairs. For a mirror unit other than MU#0, the environment variable RMSRATMU can be set.

If you use the TrueCopy or Hitachi Universal Replicator S-VOL (this is the S-VOL of the primary replication between protection site and recovery site) for testing failover, the failover test disrupts the remote replication. In addition, during the resynchronisation between the protection site and the recovery site after test failover, changes are applied from a bitmap and are out of order. The consistency of the S-VOL is compromised during this time and a real failover is not possible if a failure on the P-VOL occurs. Test failovers in this scenario are best done during an application outage.

If a mirror unit other than MU#0 is set, and a snapshot does not exist at that mirror unit, the TrueCopy or Hitachi Universal Replicator pairs are used for testing failover.

RAID Manager CCI HORCM Configuration Considerations

Keep these considerations in mind when creating the TrueCopy, Hitachi Universal Replicator or TrueCopy Extended pairs as well as the optional ShadowImage or Copy-on-Write pairs.

- If you use ShadowImage software, the mirror unit number must be implicitly specified in the horcm<X>.conf file.
- ShadowImage S-VOLS should be configured using horcmX+1.conf.
- ShadowImage must be created using the following command options:

```
paircreate -g <grp> -m grp -fq quick -v<l/r>
```

- If Copy-on-Write is used, do not use the -fq quick option.
- -m grp creates a consistency group for all LUNs in the pair group.
- -fq quick allows for ShadowImage quick split.
- ShadowImage S-VOLs must be mapped on the same Fibre Channel port as the P-VOLs.

ESX derives the UUID of the datastore from the WWN of the LU. Because this WWN is different if the S-VOL is on a different Fibre Channel port, the UUID does not match and the datastore is not attached to the virtual machine. As a workaround, place a dummy ShadowImage S-VOL on the P-VOL port to describe this port to ESX.

- If TrueCopy sync is used, the fence level must be set to **data** to ensure that **horctakeover** succeeds. Use the following command to set the fence level:

paircreate -g <grp> -vl -f data

- A fence level of data should be utilized when using TrueCopy for remote replication:

paircreate -g <grp> -f data -vl

Example of HORCM Configuration Files

It is best practice to name the devices the same as the datastore contained on the LU. [Figure 2-1](#) illustrates the device naming conventions and [Figure 2-2](#), [Figure 2-3](#) show code samples.

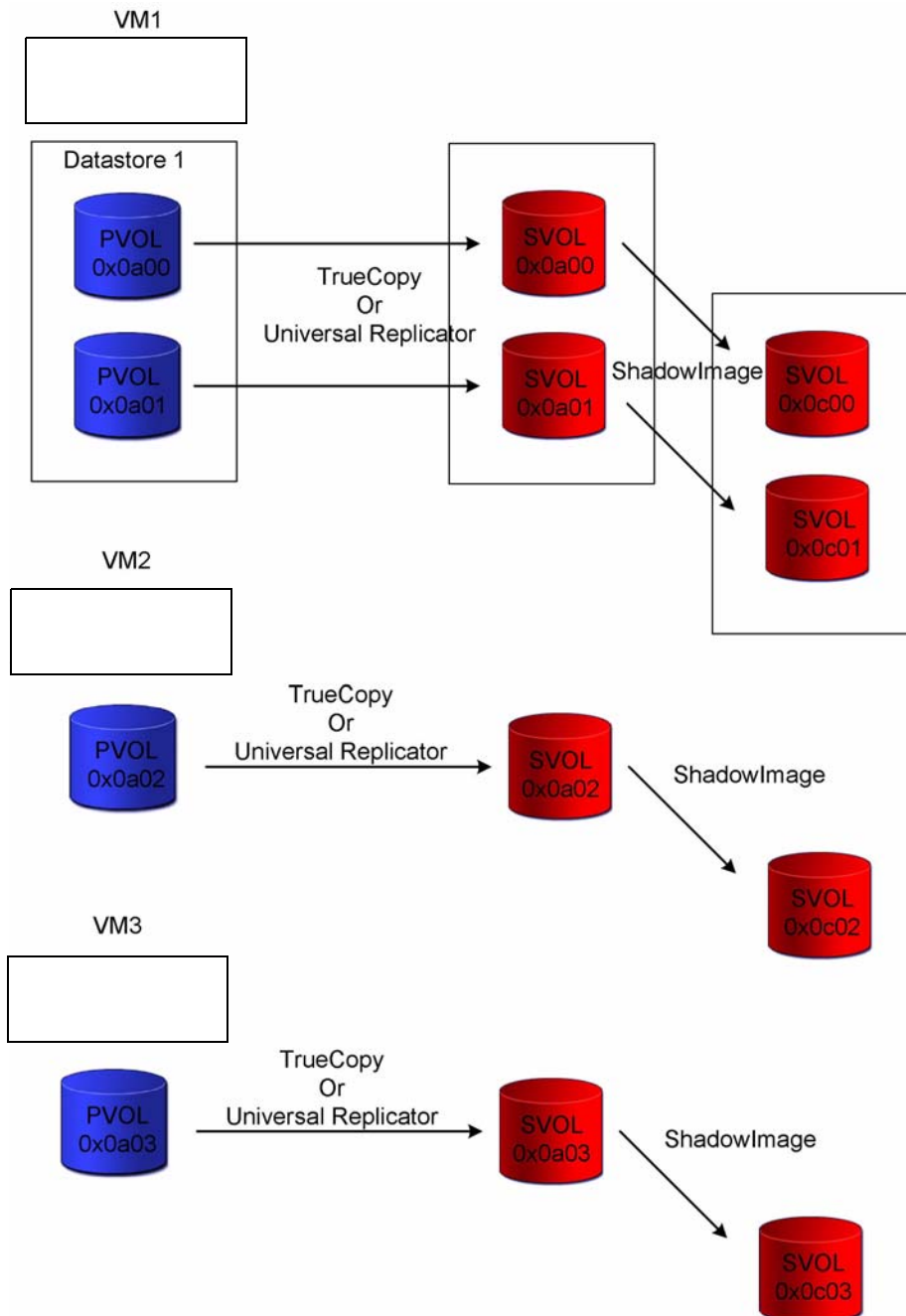


Figure 2-1: Device Naming Conventions

```

#UnitID 0 (Serial#10033)
#set HORCMINST=0
HORCM_MON
#ip_address      service      poll(10ms)      timeout(10ms)
rm-srm-protected horcm0      1000            4000

HORCM_CMD
#dev_name
\\.\CMD-10033

HORCM_LDEV
#group      P-VOL      #serial  S-VOL
VM1      VM_1_Dev_1      10033  0x0A00
VM1      VM_1_Dev_2      10033  0x0A01
VM2      VM_2            10033  0x0A03
VM3      VM3            10033  0x0A04

HORCM_INST
#group      device      instance
VM1      rm-srm-recovery  horcm1
VM2      rm-srm-recovery  horcm1
VM3      rm-srm-recovery  horcm1

#UnitID 0 (Serial#10226)
#set HORCMINST=1
HORCM_MON
#ip_address      service      poll(10ms)      timeout(10ms)
rm-srm-recovery  horcm1      1000            4000

HORCM_CMD
#dev_name
\\.\CMD-10226
HORCM_LDEV
#HUR LDEVs
#group      Device      serial#  LDEV
VM1      VM1_Dev_1      10226  0x0a00
VM1      VM1_Dev_2      10226  0x0a01
VM2      VM2            10226  0x0a03
VM3      VM3            10226  0x0a04

#SI SRM LDEVs
#group      Device      serial#  LDEV  MU
SI-VM1      SI-VM1_Dev_1  10226  0x0a00  0
SI-VM1      SI-VM1_Dev_2  10226  0x0a01  0
SI-VM2      SI_VM2        10226  0x0a03  0
SI-VM3      SI_VM3        10226  0x0a04  0

HORCM_INST
VM1      rm-srm-protected  horcm0
VM2      rm-srm-protected  horcm0
VM3      rm-srm-protected  horcm0
SI-VM1      rm-srm-recovery  horcm2
SI-VM2      rm-srm-recovery  horcm2
SI-VM3      rm-srm-recovery  horcm2

```

Figure 2-2: Relationship between Protected Site C:\windows\horcm0.conf and Recovery Site C:\windows\horcm1.conf

```

#UnitID 0 (Serial#10226)
HORCM_MON
#ip_address      service      poll(10ms)      timeout(10ms)
rm-srm-recovery  horcm2       1000            4000

HORCM_CMD
#dev_name        dev_name      dev_name
\\.\CMD-10226

HORCM_LDEV
#SI SRM LDEVs
#group           Device              serial#  LDEV
SI-VM1           SI-VM1_Dev_1       10226   0x0c00
SI-VM1           SI-VM1_Dev_2       10226   0x0c01
SI-VM2           SI_VM2              10226   0x0c03
SI-VM3           SI_VM3              10226   0x0c04

HORCM_INST
#group           device            instance
SI-VM1           rm-sra-recovery  horcm1
SI-VM2           rm-sra-recovery  horcm1
SI-VM3           rm-sra-recovery  horcm1

```

Figure 2-3: Recovery Site C:\windows\horcm2.conf

ShadowImage devices must contain the MU parameter; in this case MU#0 is used. If MU#1 or MU#2 are used, the variable RMSRATMU must be set using the following command:

```
setx RMSRATMU 1 /m
```



NOTE: The SRM server must be rebooted after this command is issued.

This HORCM instance must be the primary instance number plus 1. In this example, the primary instance number is 1 and the secondary instance number is 2.

Scenarios

With the Hitachi Storage Replication Adapter 2.0, remote replication on enterprise storage subsystems can be done using TrueCopy or Hitachi Universal Replicator. With Adaptable Modular Storage subsystems, remote replication can be done using TrueCopy or TrueCopy Extended. However, only TrueCopy supports ShadowImage or Copy-on-Write while TrueCopy Extended Distance does not allow either ShadowImage or Copy-on-Write. Local replication on the recovery site can be done using ShadowImage or Copy-on-Write on either class of subsystem. For Adaptable Modular Storage subsystems only one ShadowImage or Copy-on-Write pair may be in PAIR status at one time and only with TrueCopy. The ShadowImage or Copy-on-Write copy provides the ability to test failover without disrupting the primary replication.

Using TrueCopy or Hitachi Universal Replicator with ShadowImage

SRM can utilize a ShadowImage copy or Copy-on-Write for test failover. This additional point-in-time (PIT) copy allows the TrueCopy or Hitachi Universal Replicator copy to remain in sync during the test failover; facilitating testing of the disaster recovery plan without interruption of protection. The recovery point objective remains the same during test failover.

To execute a test failover using a ShadowImage copy, create a ShadowImage copy using MU 0 and include this in the HORCM configuration as seen in [Figure 2-2 on page 2-7](#). By default, RMSRA executes the test failover on the ShadowImage copy. [Figure 2-4](#) shows an example of using TrueCopy or Universal Replicator in conjunction with ShadowImage.

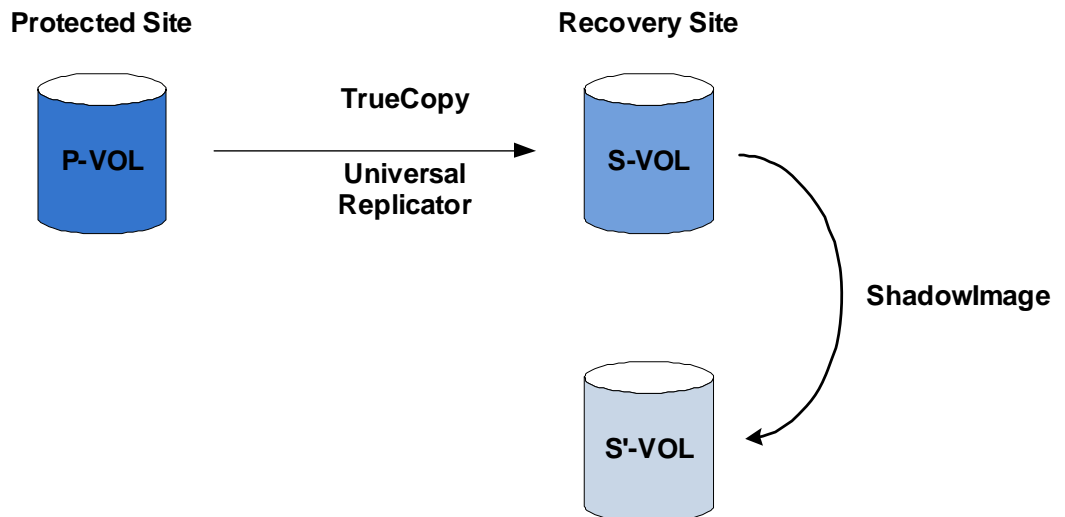


Figure 2-4: TrueCopy or Universal Replicator use with ShadowImage

Using TrueCopy or Hitachi Universal Replicator Only

Site Recovery Manager can utilize the TrueCopy or Hitachi Universal Replicator S-VOL for test failover and failover without the additional ShadowImage volume on the recovery site. In this case, during test failover the recovery site S-VOL is not available for failover. In addition, updates are applied from the bitmap and out of order during resynchronization of the replication after test failover is complete. The S-VOL is not available for failover until these updates are complete. [Figure 2-5](#) shows an example where TrueCopy or Universal Replicator is used alone.

Test failover utilizes the remote replication S-VOL if one or more of the following conditions are met:

- The storage processor does not contain a ShadowImage license
- The variable RMSRATMU is set to a ShadowImage MU that does not exist

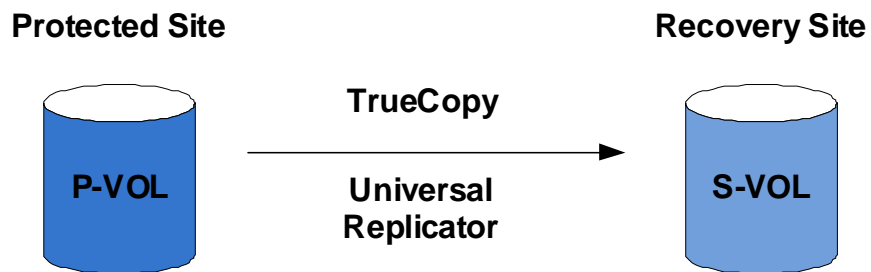


Figure 2-5: Using True Copy or Universal replicator only

For more information, see [Environment Variables on page 2-15](#).

Mixing

Figure 2-6 shows a scenario in which Virtual Machine 1 has a service level agreement (SLA) of 6/24 and a planned outage every week. Test failover can be executed during this planned outage and therefore an additional ShadowImage copy is not required. Virtual Machine 2 has an SLA of 7/24 and cannot suffer a planned outage for testing failover. Testing failover on Virtual Machine 2 is critical to meeting the SLA.

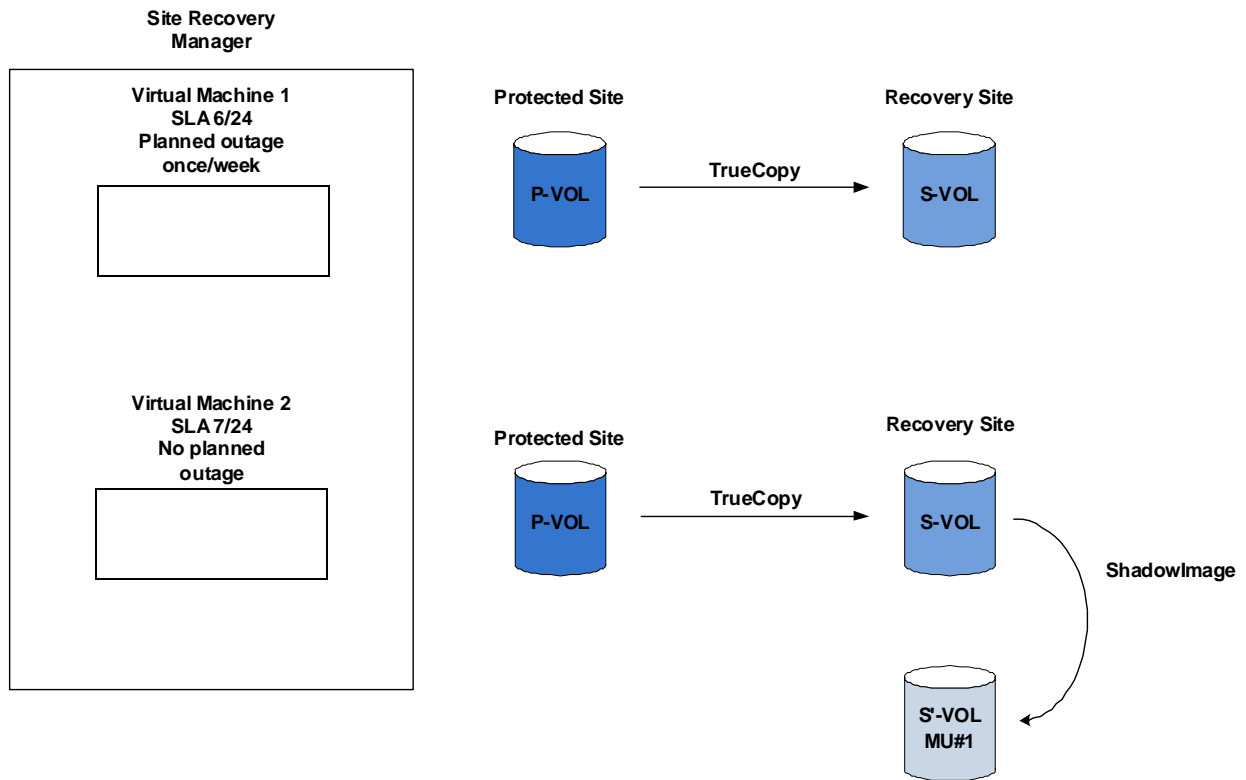


Figure 2-6: Mixing scenario with different hosts

RAID Mgr CCI HORCM Mixed Scenario Configuration Considerations

Refer to Figure 2-7, Figure 2-8, Figure 2-9 and keep these considerations in mind when using this mixed mode configuration:

- Virtual Machine 1 contains a TrueCopy pair group.
- Virtual Machine 2 contains a TrueCopy pair group and a ShadowImage pair group using MU#1.

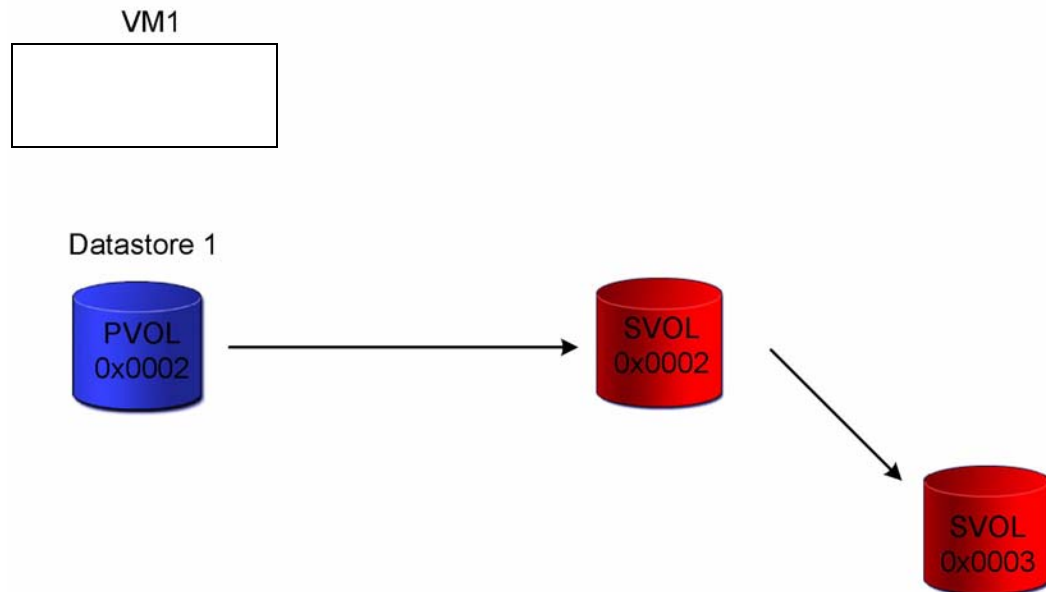
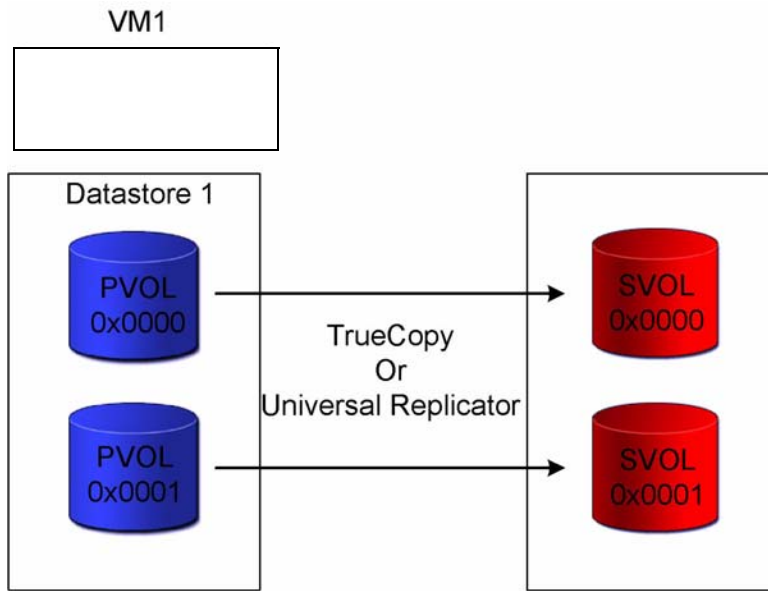


Figure 2-7: Device Naming Conventions

```

#/******Local Host *****/
HORCM_MON
#ip_address    service    poll(10ms)  timeout(10ms)
rm-srm-protected horcm0    1000      3000

#/******For HORCM_CMD *****/
HORCM_CMD
#dev_name
\\.\CMD-10226

#/****** For HORCM_LDEV *****/
HORCM_LDEV
#dev_group  dev_name  Serial#  LDEV#  MU#
VM1        Datastore1-1  10226  0x0000
VM1        Datastore1-2  10226  0x0001
VM2        Datastore2    10226  0x0002

#/****** For HORCM_INST*****/
HORCM_INST
#dev_group  ip_address  service
VM1         rm-srm-recovery horcm1
VM2         rm-srm-recovery horcm1

```

```

#/******Local Host *****/
HORCM_MON
#ip_address  service  poll(10ms)  timeout(10ms)
srm-recovery horcm1    1000      3000

#/******For HORCM_CMD *****/
HORCM_CMD
#dev_name
\\.\CMD-10033

#/****** For HORCM_LDEV *****/
HORCM_LDEV
#dev_group  dev_name  Serial#  LDEV#  MU#
VM1        Datastore1    10033  00:00
VM2        Datastore2    10033  00:01
SI-VM2     SI-Datastore2  10033  00:01  1

#/****** For HORCM_INST*****/
HORCM_INST
#dev_group  ip_address  service
VM1         srm-protected horcm0
VM2         srm-protected horcm0
SI-VM2     srm-recovery horcm2

```

Figure 2-8: Relationship between Protected Site HORCM C:\windows\horcm0.conf and Recovery Site HORCM C:\windows\horcm1.conf

```

#/******Local Host *****/
HORCM_MON

#ip_address  service  poll(10ms)  timeout(10ms)
srm-recovery horcm2  1000      3000

#/******For HORCM_CMD *****/
HORCM_CMD

#dev_name
\\.\CMD-10033

#/****** For HORCM_LDEV *****/
HORCM_LDEV

#dev_group  dev_name  Serial#  LDEV#  MU#
SI-VM2     SI-Datastore2  10033  00:02

#/****** For HORCM_INST*****/
HORCM_INST

#dev_group  ip_address  service
SI-VM2      srm-recovery  horcm1

```

Figure 2-9: Recovery Site HORCM C:\windows\horcm2.conf

Creating ShadowImage Pairs

Follow these requirements when creating the ShadowImage pairs for deployment on Storage Replication Adapter 2.0:

- ShadowImage software must use consistency groups using the command option **-m grp**
- Split mode must be set to *quick* using the command option **-fq quick**
- Use the following command to create the local replication pairs

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

- If Copy-on-Write is used, do not use the **-fq quick** option

Environment Variables

The Storage Replication Adapter 2.0 must be configured to look for MU#1 for the ShadowImage copy. If Storage Replication Adapter 2.0 looks for MU#1 on virtual machine 1 during testFailover and does not find it, the TrueCopy pair is suspended and used for testFailover. If Storage Replication Adapter 2.0 looks for MU#1 and locates it at HORCM instance <X>+1, the ShadowImage copy is suspended and used for the test failover.



NOTE: The ShadowImage S-VOL must be presented on the same Fibre Channel port as the ShadowImage P-VOL or the UUID on the datastore changes. ESX cannot attach it to the shadow virtual machine for test failover unless the UUID matches.

Setting Environment Variables on the SRM Host

Follow these steps to set the environment variables on the SRM host:

1. Issue the following command to set the SplitReplication parameter to equal true:

```
setx SplitReplication true /m
```

2. Issue the following command to set the RMSRATMU parameter to 1:

```
setx RMSRATMU 1 /m
```

3. Reboot the SRM host.
4. Verify that the variables are set correctly using the **Set** command.
5. Optional setting: If CCI is installed to another drive (e.g. E:), then use the HORCMROOTD variable:

```
setx HORCMROOT E: /m
```

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

```
setx RMSRATOV 120 /m
```

If CCI is installed on the SRM host, no more changes are required. Follow the steps in the next section if CCI is installed on a UNIX host.

Setting Environment Variables on a UNIX Host

SRM will telnet as root to the UNIX host to execute RMSRA commands. Use the root user profile to set these variables, that is, `/root/.bash_profile`, in 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 utilized for testing.

Configuring Array Managers in Site Recovery Manager

The VMware vCenter Site Recovery Manager Array Manager (i.e. the Hitachi Storage Replication Adapter 2.0) configuration varies depending on the location of CCI/RAID Manager.

If the Windows version of CCI/RAID Manager is used it has to be installed on the VMware vCenter Site Recovery Manager on both sites; the protection site, and the recovery site. This means VMware vCenter Site Recovery Manager, Hitachi Storage Replication Adapter 2.0, and CCI/RAID Manager have to be installed on the same server running Windows, and the Hitachi Storage Replication Adapter 2.0 will communicate locally with the CCI/RAID Manager. See [When CCI Resides on the Windows SRM Server on page 2-17](#).

If the UNIX version of CCI/RAID Manager is used the VMware vCenter Site Recovery Manager Array Manager (i.e. the Hitachi Storage Replication Adapter 2.0) can be configured to remotely communicate (via telnet) with the CCI/RAID Manager instance(s). See [When CCI resides on a Linux Server on page 2-17](#). In this latter case only, the VMware vCenter Site Recovery Manager and the Hitachi Storage Replication Adapter have to be installed on the same server, and CCI/RAID Manager may run on separate (remote) UNIX host(s). This would allow to run a centralized UNIX CCI/RAID Manager host instead of running UNIX CCI/RAID Manager hosts for each site, protection site, and recovery site. Hitachi Data Systems does not recommend running a centralized CCI/RAID Manager host for redundancy reasons.

When CCI Resides on the Windows SRM Server

Follow these steps to configure the array manager when CCI resides on the SRM server:

1. Enter the display name that describes the configuration.
2. Select **Hitachi Storage Replication Adapter 2.0** from the drop down menu.
3. In the Alias field, enter **HORCMINST=<instance_number>**.

For example, if your HORCM instance is 0, enter **HORCMINST=0**.

4. Enter any information in the Username and Password fields and click **Connect**.

These fields are required, but are not used for local HORCM configurations. A dummy user name and password can be entered.

The SRM function **discoverArrays** runs. The storage processor serial number appears under Array ID, and the microcode version appears under Model.

5. Click **OK**.

The SRM function **discoverLuns** runs and identifies the number of replicated LUs in the HORCM instance. In addition the LDEV number (in decimal) and the Peer Array serial number are discovered. In the display shown under Replicated Array Pairs: only the Peer Array serial number is shown.

6. Configure the recovery site using steps 1 through 5 above for the protected site.



NOTE: A green check mark appears when **discoverLuns** determines that the configuration is correct. If any discrepancies between the LUs replicated are discovered, the check mark does not appear. In this case, check the HORCM configuration for errors.

7. Click **Next**.
8. In the window **Review Replicated Datastores** click the plus (+) signs and double check that the correct replicated LDEV numbers are listed with the correct Datastores.

When CCI resides on a Linux Server

Before you can use Storage Replication Adapter 2.0 on a Linux server, the following conditions must be met:

- The Linux server must accept root login via telnet.
- The telnet server must be installed and configured.



NOTE: Secure shell is not supported. The following variables need to be set if the Linux host is Suse Linux which does not recognize the "network" as terminal type:

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

```
setx RMSRA_TEL_RESPTS vt100 /m
```

Enter the display name that describes the configuration.

1. Select Hitachi Storage Replication Adapter 2.0 from the drop down menu.
2. In the Alias field, enter HORCMINST=<instance_number>@<IP Address of the CCI server>.

For example, if your HORCM instance is 0 on CCI server 172.17.17.100, enter HORCMINST=0@172.17.17.100.

3. Enter the root user information in the **Username** and **Password** fields and click Connect.

The SRM function **discoverArrays** runs. The storage processor serial number appears under Array ID, and the microcode version appears under Model.

4. Click OK.

The SRM function discoverLuns runs and identifies the number of replicated LUs in the HORCM instance. In addition the LDEV number (in decimal) and the Peer Array serial number are discovered. In the display shown under **Replicated Array Pairs:**, only the Peer Array serial number is shown.

5. Configure the recovery site for the protected site using Steps 1 through 5 from the previous section [When CCI Resides on the Windows SRM Server on page 2-17](#).



NOTE: A green check mark appears when discoverLuns determines that the configuration is correct. If any discrepancies between the LUs replicated are discovered, the check mark does not appear. In this case, check the HORCM configuration for errors.

6. Click **Next**.
7. In the window **Review Replicated Datastores** click the plus (+) signs and double check that the correct replicated LDEV numbers are listed with the correct Datastores.

Recovering from a Failover

To recover from a failover, the roles of the Protected site and Recovery site are reversed. Before Site Recovery Manager can be configured in the reverse direction, remote replication must be reversed. Methods for this vary according to the storage processor type and the conditions that caused the failover.

Recovering Replication on USP, NSC, USP V and USP VM

These storage systems reverse the remote replication when failover occurs. In some cases no action is needed, in others a pairresync operation may be required.

Reverse Replication, Protected site on-line

If the Protected site storage processor remains on line, the replication will be automatically reversed by the failover operation. Check the status of the remote replication using *pairdisplay -g <grp>*. If the status is PAIR, no action is needed.

Reverse Replication, Protected site off-line

If the protected site was off-line during the failover operation, resynchronization of the remote replication may be required.

Check the remote replication pair status using the *pairdisplay -g <grp>* command.

1. If the status is PAIR, no action is needed.
2. If the status is PSUE or SSWS, a pair resync operation is required.
 - a. From the Recovery site CCI server issue the command *pairresync -g <grp> -swaps*. See the CCI manual for more details.
 - b. Wait for status of PAIR using the command *pairevtwait -g <grp> -s pair -t <timeout value?>*. See the CCI manual for more details.
3. If the status is SMPL, a paircreate operation is needed.
 - a. Issue the paircreate command as shown in [RAID Manager CCI HORCM Configuration Considerations on page 2-5](#) of this document.
 - b. Wait for status of PAIR using the command *pairevtwait -g <grp> -s pair -t <timeout value?>*. See the CCI manual for more details.

Recovering replication

The AMS family of arrays will require that the remote replication be deleted and recreated in the reverse direction. Issue a *pairsplit -g <grp> -S* to delete the pairs. Issue the paircreate command as shown in [RAID Manager CCI HORCM Configuration Considerations on page 2-5](#) of this document.

Troubleshooting the SRA 2.0

This section provides information to help you troubleshoot configuration problems.

Error Messages on SRM Log Files

RMSRA generates the following error messages in order to identify the cause of a failure as “[RMSRA]” in the SRM log files.

Remove the cause of the error by referring to the error messages of “[RMSRA]” and “SRM ERROR messages” in the SRM log files.

SRM log is located in the following directory:

C:\Documents and Settings\All Users\Application Data\VMware\VMware Site Recovery Manager\Logs\vmware*.log

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

Errors in XML received from SRM

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

- [Cause] A parameter in XML was input from SRM to the SRA, but it exceeds the defined length for the SRA specification.
- [Action to be taken] Please confirm if SRM received the appropriate parameters in XML from its own SRM log message.

[RMSRA][Time]: [command_main] : Parameter in XML was NOT enough.

- [Cause] A parameter in XML was input from SRM to the SRA but it could not be found in any parameters.
- [Action to be taken] Please confirm if SRM received the appropriate parameters in XML from its own SRM log message.

[RMSRA][Time]: [command_discoverLuns] : NO arrayId in XML.

- [Cause] A parameter in XML(discoverLuns) was input from SRM to the SRA but the array ID could not be found.
- [Action to be taken] Please confirm if SRM received the Array ID parameter in XML(discoverLuns) from its own SRM log message.

[RMSRA][Time]: [command_failover] : NO ReplicaLunKey in XML.

- [Cause] A parameter in XML(failover) was input from SRM to the SRA but RelplicaLunKey(LDEV# of TC_SVOL) could not be found.
- [Action to be taken] Confirm whether SRM was passed RelplicaLunKey parameter in XML(failover) from its own SRM log message.

[RMSRA][Time]: [command_testFailover] : Action in XML was NOT start/stop.

- [Cause] A parameter in XML(testFailover) was input from SRM to the SRA, but it could not be found "start/stop" as Action.
- [Action to be taken] Please confirm whether SRM received the "start/stop" parameter in XML(testFailover) from its own SRM log message.

[RMSRA][Time]: [command_testFailover] : NO ReplicaLunKey in XML.

- [Cause] A parameter in XML(testFailover) was input from SRM to the SRA but RelplicaLunKey(LDEV# of TC_SVOL) could not be found.
- [Action to be taken] Confirm whether SRM received the RelplicaLunKey parameter in XML(testFailover) from its own SRM log message.

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

- [Cause] A connection address in XML was input from SRM to the SRA but the HORCM instance #X could not be found.
- [Action to be taken] Check whether HORCM instance# is running or a connection address (Alias) specified in the Array Manager configuration is appropriate.

RAID Manager command Errors in rmsra.exe

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

- [Cause] A parameter in XML was input from SRM to the SRA, but it could not be created "XML OUTPUT file name".
- [Action to be taken] Please confirm whether SRM received the appropriate OutputFile in XML from its own SRM log message, or refer to the "system error message."

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

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

[RMSRA][Time]: ["Command line"] : popen : "system error message"

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

[RMSRA][Time]: [] : malloc : "system error message"

- [Cause] Couldn't retain the memory for executing a RM SRA.
- [Action to be taken] Increase the capacity of virtual memory of the whole system, or terminate unnecessary programs or daemon processes that are running simultaneously.

[RMSRA][Time]: [] : "Command line" failed with RC=XXX.

[Cause] The RAID Manager command (Command line) has failed with RC=XXX.

[Action to be taken] Remove the cause of the error after confirming with a RAID Manager error code and command error log messages output in this log file, as shown below.

```
-----  
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]:Please confirm if the group name exists in the configuration file of  
the local and remote host.  
-----
```

Configuration and Status errors

[RMSRA][Time]: [disarray_exe] : Unknown PWWN.

- [Cause] Couldn't find the Port WWN in the output of "pairedisplay -fw" command via discoverArrays.
- [Action to be taken] Confirm that the RAID Manager is the correct RMSRA supported version.

[RMSRA][Time]: [dislun_exe] : invalid arrayId (...).

- [Cause] A parameter in XML(discoverLuns) was input from SRM to the SRA, but it could not be found correct array ID.
- [Action to be taken] Confirm whether the SRM received an array ID parameter in XML(discoverLuns) from its own SRM log message.

[RMSRA][Time]: [dislun_exe] : Unknown PWWN.

- [Cause] Couldn't find the Port WWN in the output of "pairedisplay -fw" command via discoverLuns.
- [Action to be taken] Confirm that the RAID Manager is the correct RMSRA supported version.

[RMSRA][Time]: [failover_chk] : " Command line" -> P/S = ..., Status = ..., Fence =

- [Cause] The pair status of a target volume specified with failover is inappropriate status ('SMPL' or 'PVOL' or 'COPY').
- [Action to be taken] Confirm whether the volume status is set properly (TC is 'SVOL' and 'PAIR') using the pairedisplay command.

[RMSRA][Time]: [failover_chk] : The output of "Command line" is missing.

- [Cause] Couldn't find the correct format in the output of "Command line" command via failover.
- [Action to be taken] Confirm that the RAID Manager is the correct RMSRA supported version.

[RMSRA][Time]: [testFailover_chk] : " Command line" -> P/S = ..., Status = ..., CTG =

- [Cause] The pair status of a target volume specified with testFailover is improperly set ('SMPL' or 'PVOL' or 'NOT PAIR' or NO CTG).
- [Action to be taken] Confirm that the volume status is set properly (ShadowImage is 'SVOL' and 'PAIR' with CTG) using the pairedisplay command.

[RMSRA][Time]: [testfailover_chk] : The output of "Command line" is missing.

- [Cause] Couldn't find the correct format in the output of "Command line" command via testFailover.
- [Action to be taken] Confirm that the RAID Manager is the correct RMSRA supported version.

[RMSRA][Time]: [failover_exe] : invalid arrayId (...).

- [Cause] A parameter in XML(failover) was input from SRM to the SRA, but it could not be found correct array ID.
- [Action to be taken] Confirm that the SRM received an array ID parameter in XML(failover) from its own SRM log message.

[RMSRA][Time]: [testfailover_exe] : invalid arrayId (...).

- [Cause] A parameter in XML(testFailover) was input from SRM to the SRA, but it could not be found correct array ID.
- [Action to be taken] Confirm that the SRM received an array ID parameter in XML(testFailover) from its own SRM log message.

Multiple Error Codes

RMSRA defines an error code by an "OR" flag of 32 bits so the user can identify multiple errors that happened to the transaction from XML data strings.

For example:

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

Table 2-1: Error Codes

Error Code	Description
0x000000XX	XX : exit code returned from RAID Manager command. Refer to the RAID Manager command error code
0x00000100	The volume is inappropriate property as "SMPL"
0x00000200	The volume is inappropriate property as "PVOL"
0x00000400	The volume is inappropriate property as "SVOL"
0x00000800	Undefined
0x00001000	The volume is inappropriate status as "COPY", etc...
0x00002000	The volume has NO CTgroup
0x00004000	Undefined
0x00008000	Undefined

Table 2-1: Error Codes

Error Code	Description
0x00010000	The pairedisplay command has NO PWWN
0x00020000	The pairedisplay command has NO LUN WWN
0x00040000	The pairedisplay command has NO support for SRA
0x00080000	Undefined
0x00100000	Memory allocation error
0x00200000	Popen() function of the system was returned with ERROR
0x00400000	System() function of the system was returned with ERROR
0x00800000	Undefined
0x01000000	Error in XML from SRM
0x02000000	Undefined
0x04000000	Undefined
0x08000000	Undefined
0x10000000	Undefined
0x20000000	Undefined
0x40000000	Undefined
0x80000000	Undefined

Failure to launch scripts

If VMware vCenter Site Recovery Manager array manager configuration fails to launch the Hitachi Storage Replication Adapter 2.0, an error message appears as shown in [Figure 2-10](#).

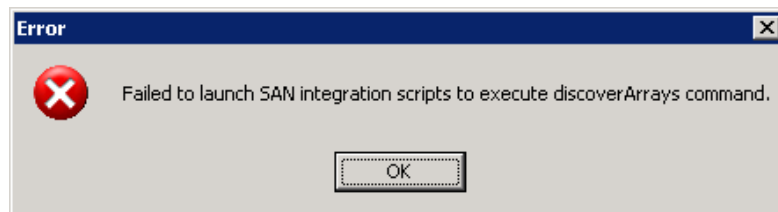


Figure 2-10: Error message

UNIX CCI Server

1. Check that the HORCM instance is running using the command **ps -ef | grep horcm**.
2. Check that telnet as root is allowed. From the SRM server, telnet to the CCI server as root.
3. Check that the correct version of rmsra is installed with the following command:

```
/HORCM/usr/bin/rmsra -h
```

```
Ver&Rev: 01.00.08
```

4. Check that the Alias is entered correctly HORCMINST=X@<CCI server IP>.

Windows CCI Server

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.

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>rmsra -h

Ver&Rev: 01.00.08

Test failover errors

If the Test Failover produces errors on Prepare storage as shown in the history screen in [Figure 2-11](#), perform the following steps.

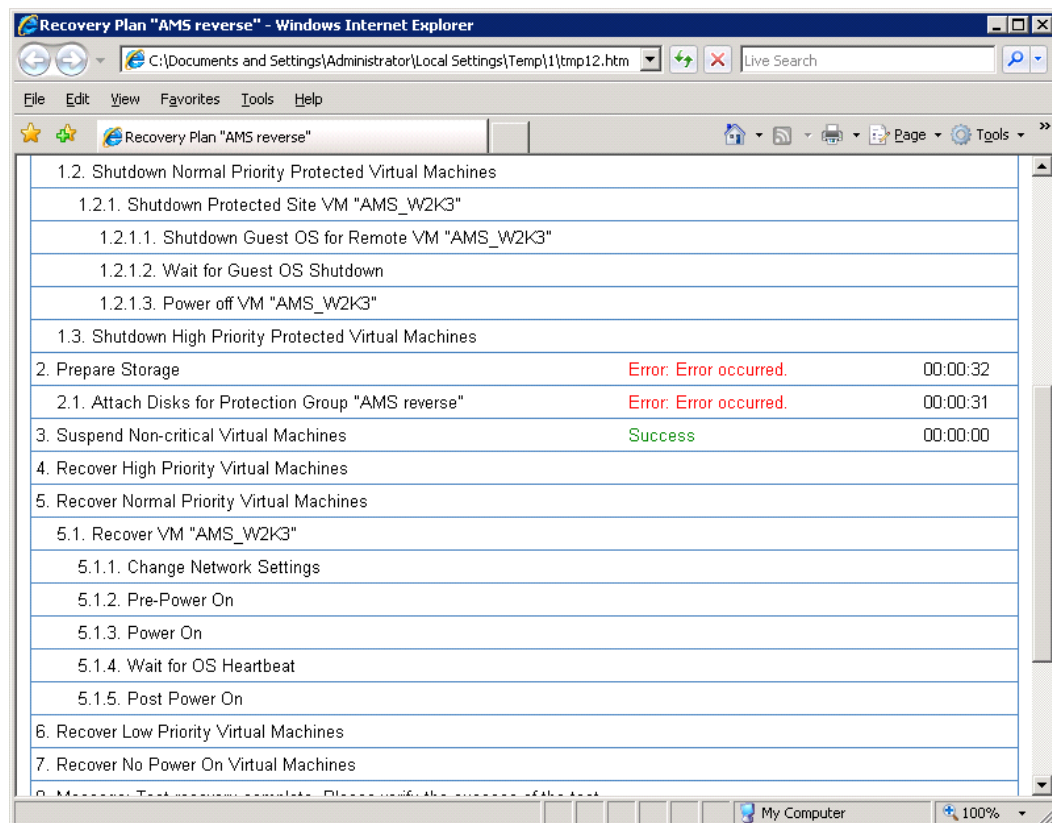


Figure 2-11: History Screen

1. Check the SRM log on the recovery site. Search for the XML code produced by the SRA.

```
[RMSRA][Fri Jan 23 05:41:44 2009]: [RMSRAVER] : 01.00.08
```

```
[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [XML_name] : testFailover
```

```
[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [XML_action] : start
```

```

[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [XML_con_name] : RAID
Manager Storage Replication Adapter

[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [XML_con_addr] :
HORCMINST=0@172.17.171.203

[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [XML_arrayId] : 87010011

[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [XML_rlunkey] : 0

[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [XML_split] : false

[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [XML_outfile] :
C:\WINDOWS\TEMP\vmware-SYSTEM\dr-sanprovider0

[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [XML_loglvl] : trivia

[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [RMSRATOV] : 60 sec

[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [RMSRATMU] : 1

[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [RMSRASPLIT] : false

[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [XML_IniPort] : iScsi-fc-all =>
id= 10:00:00:00:c9:48:50:68 type= fc

[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [XML_IniPort] : iScsi-fc-all =>
id= 10:00:00:00:c9:44:68:12 type= fc

[#6] [RMSRA][Fri Jan 23 05:41:44 2009]: [horcmconn_exe] : '/usr/bin/
raidqry -IH -l 1 >/dev/null' returned with RC=0 on HORCMINST=0.

[#6] COMMAND ERROR : EUserId for HORC[1] : root (0) Fri Jan 23
05:41:44 2009

[#6] CMDLINE : /usr/bin/raidqry -IH1 -l

[#6] ***** SYSTEM ERROR *****

[#6] P.P. : RAID Manager for Linux

[#6] Model : RAID-Manager/Linux

[#6] Ver&Rev: 01-23-03/06

[#6] Release: Production(GA)

```



NOTE: In this case there is no ShadowImage or Copy-on-Write utilized for test failover, therefore the SplitReplication parameter must be set to TRUE.

2. Check the above log and see that the [RMSRASPLIT] : false is set.
 - a. Change this to true both on the SRM server and if UNIX is used for CCI in the UNIX servers root profile. See section (X) above.
 - b. After corrections are made the test should complete and the XML will look like this example:

```

[RMSRA][Fri Jan 23 05:46:17 2009]: [RMSRAVER] : 01.00.08

[#6] [RMSRA][Fri Jan 23 05:46:17 2009]: [XML_name] : testFailover

```

```

[#6] [RMSRA][Fri Jan 23 05:46:17 2009]: [XML_action] : start
[#6] [RMSRA][Fri Jan 23 05:46:17 2009]: [XML_con_name] : RAID
Manager Storage Replication Adapter
[#6] [RMSRA][Fri Jan 23 05:46:17 2009]: [XML_con_addr] :
HORCMINST=0@172.17.171.203
[#6] [RMSRA][Fri Jan 23 05:46:17 2009]: [XML_arrayId] : 87010011
[#6] [RMSRA][Fri Jan 23 05:46:17 2009]: [XML_rlunkey] : 0
[#6] [RMSRA][Fri Jan 23 05:46:17 2009]: [XML_split] : true
[#6] [RMSRA][Fri Jan 23 05:46:17 2009]: [XML_outfile] :
C:\WINDOWS\TEMP\vmware-SYSTEM\dr-sanprovider0
[#6] [RMSRA][Fri Jan 23 05:46:17 2009]: [XML_loglvl] : trivia
[#6] [RMSRA][Fri Jan 23 05:46:17 2009]: [RMSRATOV] : 60 sec
[#6] [RMSRA][Fri Jan 23 05:46:17 2009]: [RMSRATMU] : 1
[#6] [RMSRA][Fri Jan 23 05:46:17 2009]: [RMSRASPLIT] : true
[#6] [RMSRA][Fri Jan 23 05:46:17 2009]: [XML_IniPort] : iScsi-fc-all =>
id= 10:00:00:00:c9:48:50:68 type= fc
[#6] [RMSRA][Fri Jan 23 05:46:17 2009]: [XML_IniPort] : iScsi-fc-all =>
id= 10:00:00:00:c9:44:68:12 type= fc
[#6] [RMSRA][Fri Jan 23 05:46:18 2009]: [horcmconn_exe] : '/usr/bin/
raidqry -IH -l 1>/dev/null' returned with RC=0 on HORCMINST=0.
[#6] COMMAND ERROR : EUserId for HORC[1] : root (0) Fri Jan 23
05:46:18 2009
[#6] CMDLINE : /usr/bin/raidqry -IH1 -l

```

Collecting Information Before Contacting Customer Support

Please collect the following information before contacting customer support.

SRM/SRA local configuration

On Windows where SRM is running, perform the following procedures.

1. Collect the SRM log file on Windows on both protection and recovery sites. Collect the following SRM log file including the error messages of "[RMSRA]" and "SRM ERROR messages" and the RAID Manager command error log.

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

2. Collect the outputs of the following command on HORCMINST=XX(instance# for SRA)
 - set
 - %HORCMROOT%\HORCM\etc\raidqry -l

- %HORCMROOT%\HORCM\etc\raidqry -g
- %HORCMROOT%\HORCM\etc\pairdisplay -IH -g ??? -CLI -I -fwe (where ??? is a group name shown by "raidqry -g")
- %HORCMROOT%\HORCM\etc\raidscan -IH -p port(i.e. cl1-a-0) -CLI (port where connecting to ESX server)

If ShadowImage is installed,

- %HORCMROOT%\HORCM\etc\pairdisplay -g ??? -CLI -I -few -m cas (where ??? is a group name shown by "raidqry -g")

SRM/SRA remote configuration

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

1. Collect the SRM log file on Windows on both protection and recovery site.

Collect the following SRM log file including the error messages of "[RMSRA]" and "SRM ERROR messages" and the RAID Manager command error log.

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

2. Collect the outputs of the following command on HORCMINST=XX(instance# for SRA) on remot UNIX

- env
- raidqry -l
- raidqry -g
- pairdisplay -IH -g ??? -CLI -I -fwe (where ??? is a group name shown by "raidqry -g")
- raidscan -IH -p port(i.e. cl1-a-0) -CLI (port where connecting to ESX sever)

If ShadowImage is installed,

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

Hitachi Data Systems

Corporate Headquarters

750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: +1 408 970 1000
www.hds.com
info@hds.com

Asia Pacific and Americas

750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: +1 408 970 1000
info@hds.com

Europe Headquarters

Sefton Park
Stoke Poges
Buckinghamshire SL2 4HD
United Kingdom
Phone: +44 1753 618000
info.eu@hds.com



MK-09RM6745-01