Implementing VMware Site Recovery Manager with Hitachi Enterprise Storage Systems

Using the Hitachi Storage Replication Adapter

Technical Brief

By Bob Ingram and Jeff Maaks

October 2008
Executive Summary

Complex distance recovery solutions traditionally require customized, site-specific scripting. Testing these solutions also often requires multiple steps, each separately and manually executed. Hitachi Data Systems and VMware now offer a compelling solution that provides user-friendly site recovery testing and failover for VMware environments. The solution integrates VMware host-side intelligence and robust, market proven storage system-based replication from Hitachi Data Systems.

VMware’s Site Recovery Manager (SRM) is a host-based graphical user interface (GUI) application with intelligence about VMware virtual machines and virtual disks and the association of virtual machines and storage. The integration component connecting VMware SRM to the Hitachi storage system–based replication is called the Hitachi Storage Replication Adapter (SRA). The SRA allows Hitachi enterprise storage system customers to take advantage of the disaster recovery capabilities of SRM.

This document describes the configuration details required to deploy the SRA within an SRM environment using Hitachi replication. It serves as a supplementary implementation guide, describing how to deploy SRM on an existing distance replication solution.

For best results use Acrobat Reader 8.0.
## Contents

**Replication Requirements and Recommendations**
- Supported Storage Systems and Replication Architecture ........................................................................ 2
- Preparing for Data Replication Operations .................................................................................................. 2
- Preparing CCI for Pair Operations ............................................................................................................... 2
- LUN Numbering Scheme Recommendations .............................................................................................. 4

**Installing the Storage Replication Adapter**
- Verifying the SRA ........................................................................................................................................ 5
- Verifying the SRA in the SRM GUI ................................................................................................................ 10

**VMware SRM Failback**
- Manual Configuration for Recovery .............................................................................................................. 15
- Protected Site Cleanup .................................................................................................................................. 16

**Additional Reference Materials**
- VMware Documentation ................................................................................................................................. 17
- Hitachi Documentation .................................................................................................................................. 17
Implementing VMware Site Recovery Manager with Hitachi Enterprise Storage Systems

Using the Hitachi Storage Replication Adapter

Technical Brief

By Bob Ingram and Jeff Maaks

Complex distance recovery solutions traditionally require customized, site-specific scripting. Testing these solutions also often requires multiple steps, each separately and manually executed. Hitachi Data Systems and VMware now offer a compelling solution that provides user-friendly site recovery testing and failover for VMware environments. The solution integrates VMware host-side intelligence and robust, market proven storage system-based replication from Hitachi Data Systems.

VMware’s Site Recovery Manager (SRM) is a host-based graphical user interface (GUI) application with intelligence about VMware virtual machines and virtual disks and the association of virtual machines and storage. The integration component connecting VMware SRM to Hitachi storage system-based replication is called the Hitachi Storage Replication Adapter (SRA). The SRA allows Hitachi enterprise storage system customers to take advantage of the disaster recovery capabilities of SRM.

This document describes the configuration details required to deploy the SRA within an existing SRM environment using Hitachi replication. It serves as a supplementary implementation guide, describing how to deploy SRM on an existing distance replication solution.

This document is intended for anyone who wants to implement SRM with Hitachi enterprise storage systems. It is written for experienced Microsoft® Windows system administrators who are familiar with virtual machine technology and data center operations. This document assumes familiarity with VMware Virtual Infrastructure, including ESX Server 3.x, VirtualCenter Server 2.5 and the VI Client, and also assumes that these technologies and SRM are already installed. Readers also need working knowledge of storage network technology, specifically Hitachi enterprise-class Fibre Channel storage and how Virtual Infrastructure interacts with it.

A full analysis to determine the specific bandwidth and redundancy requirements of the environment you intend to replicate must be conducted by Hitachi Data Systems Global Solutions Services in its Remote Copy Planning and Design Service. This service provides you with a high-level design for your distance replication solution and a detailed analysis of workload and performance characteristics to help you support potentially expensive bandwidth decisions.
Replication Requirements and Recommendations

A number of requirements must be addressed in a storage replication environment before you deploy the Storage Replication Adapter within SRM. At a minimum, VirtualCenter and SRM must be installed and configured (with a copy of SRM installed on both the protected and recovery sites). In addition, follow the best practice recommendations in this document to ensure successful deployment and maintenance of the replication environment.

Supported Storage Systems and Replication Architecture

The SRA is designed to work with Hitachi enterprise-class storage systems, specifically the Hitachi Universal Storage Platform™, Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform VM and Hitachi Network Storage Controller.

The supported storage replication environment consists of remote copy capabilities between primary and secondary sites using either Hitachi TrueCopy® Synchronous or Hitachi Universal Replicator remote replication software. In addition, the secondary site must contain a Hitachi ShadowImage® Heterogeneous Replication in-system software copy of all LUNs, cascaded from the TrueCopy or Universal Replicator secondary volume. Define only VMware volumes that are used for the SRM environment for these remote and in-system replications. For test and recovery purposes, the ShadowImage S-VOLs are used. The remote copy S-VOLs are not affected and are available for continuous replication (during a test) and allow resyncing to the ShadowImage S-VOLs if a problem is encountered during recovery procedures.

Preparing for Data Replication Operations

The SRA used in SRM uses Hitachi RAID Manager/Command Control Interface (CCI) to control remote and in-system data replication. The CCI application must be installed on the primary SRM server and the secondary SRM server, and it must have access to the appropriate command devices.

Preparing CCI for Pair Operations

Hitachi Open Remote Copy Manager (HORCM) is an interface on the host between CCI command-line utilities and the command device on the storage system. HORCM must be configured as a service that runs under Windows and has its own configuration file. The HORCM file is used for host management of the storage system copy pairs and defines the devices in ShadowImage, TrueCopy and Universal Replicator pairs.

The HORCM configuration needs to be completed so that TrueCopy or Universal Replicator pairs are created between the primary and secondary sites. In addition, the secondary site must contain a ShadowImage copy of all LUNs, configured with consistency groups, cascaded from the TrueCopy or Universal Replicator secondary volume.

ShadowImage consistency group configuration is critical because the ShadowImage pairs are split during active I/O. Failure to utilize consistency groups can create inconsistent data during failover test or actual failover.
Figure 1 shows the configuration required for an example LUN.

Figure 1. Single LUN Replication Configuration Example

If multiple ShadowImage copies are required on the remote site for other purposes (such as a backup solution), configure them separately in their own HORCM instances.

Starting HORCM as a Windows Service

Each HORCM instance for the SRA must be started as a Windows service. Following is an example of HORCM0_run.txt and the steps required to start HORCM0 as a Windows service. Perform these steps on both the primary and secondary servers, including HORCM1 on the secondary server (changing the HORCM and HORCMINST references from 0 to 1 as appropriate).

Sample HORCM0_run.txt

```plaintext
# **** For INSTANCE# X, change to HORCMINST=X as needed ****
START:
set HORCMINST=0
set HORCC_LOG=STDERROUT
set HORCM_EVERYCLI=1
C:\HORCM\etc\horcmstart.exe
exit 0
```
Follow these steps to start HORCM as a Windows service.

1. Customize the sample script file \( \text{HORCM0.run.txt} \) according to the HORCM instance.
   
   For more information, see the descriptions in the \( \text{HORCM0.run.txt} \) file.

2. Register the HORCM instance as a service using the following command:
   
   \[ C:\HORC\tool\>svce\exe /S=HORCM /A=C:\HORC\tool\svce\exe.exe \]

**LUN Numbering Scheme Recommendations**

When creating LDEVs and LUNs to be used for replication, choose a numbering scheme that is easy to understand and can scale with your environment (see Table 1). This is not strictly required if a distance replication solution is already in place, but it can greatly assist in documentation, maintenance and troubleshooting of the environment.

**Table 1. Example Numbering Scheme**

<table>
<thead>
<tr>
<th>LUN and Replication Software</th>
<th>CU Number (Hex)</th>
<th>LDEV Number (Hex)</th>
<th>LUN Number (Hex)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hitachi TrueCopy® Synchronous P-VOL on protected site storage system</strong></td>
<td>00</td>
<td>00-0E</td>
<td>00-0E</td>
</tr>
<tr>
<td><strong>TrueCopy S-VOL and Hitachi ShadowImage® Heterogeneous Replication P-VOL</strong></td>
<td>01</td>
<td>00-0E</td>
<td>10-1E</td>
</tr>
<tr>
<td><strong>ShadowImage S-VOL</strong></td>
<td>02</td>
<td>00-0E</td>
<td>20-2E</td>
</tr>
</tbody>
</table>

In this example, CU 00 is used for all TrueCopy P-VOLs, CU 01 is used for TrueCopy S-VOLs that are also ShadowImage P-VOLs, and CU 02 is used for ShadowImage S-VOLs. This numbering scheme makes it easy to identify the devices using Hitachi Device Manager software.

In addition, the LUN numbers allow easy identification of the LUN’s role using VirtualCenter. By identifying the LUN number first, you can increment the first digit of the LUN number to identify the TrueCopy S-VOL and increment again to identify the ShadowImage S-VOL.

Figure 1 illustrates that the TrueCopy P-VOL is easily mapped to the TrueCopy S-VOL. The ShadowImage P-VOL is easily mapped to the ShadowImage S-VOL. All of the numbering is visible using VMware Virtual Center, Hitachi Storage Command Suite and CCI.

Large production environments might need larger offsets to allow for scaling of LDEVs and LUNs. This is only an example.
Installing the Storage Replication Adapter

Download the SRA from the VMware Web site. The SRA is available as an InstallShield installer, which installs the Perl scripts in `scripts\SAN\Hitachi Storage Replication Adapter` folder under the SRM installation directory (typically `C:\Program Files\VMware\Site Recovery Manager`).

Verifying the SRA

The following scripts for testing the SRA functionality and Windows setup are included in the SRA installation:

- `test_da.bat` – Tests `discoverArrays.pl`
- `test_dl.bat` – Tests `discoverLuns.pl`
- `test_failstart.bat` – Starts `failover.pl`
- `test_failstop.bat` – Stops `failover.pl`

The test batch files simulate SRM by piping XML input into each relevant Perl script. The XML used for input is stored in a text file and each XML input file must be edited prior to testing. The path to the version of Perl installed by VMware and the path to the CCI commands must be added to the Windows system path for the batch files to function correctly.

After configuring the storage system replication (distance and in-system on the remote side), verify that the SRA Perl scripts work before attempting to configure SRM. First, verify that the discovery scripts work by executing `test_da.bat` and `test_dl.bat`. Next, attempt to manually test the failover by executing the `test_failstart.bat` and then `test_failstop.bat`. These test scripts are detailed in the following sections.

Verify Storage System Discovery

test_da.bat is the batch file to test whether `discoverArrays.pl` is working. `test_da.bat` uses the following input XML to test `discoverArrays.pl`.

discoverArrays.xml Contents

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<Command>
  <Name>discoverArrays</Name>
  <ConnectSpec>
    <Name>Hitachi Array</Name>
    <Address>0</Address>
  </ConnectSpec>
  <OutputFile>C:\Temp\discarrays.xml</OutputFile>
  <LogLevel>Trivia</LogLevel>
</Command>
```
You might need to edit the following lines:

- `<Address>` – Set to the HORCM instance number (use the primary instance on both sides)
- `<OutputFile>` – Set to the location where the XML output is to be placed; if this line is changed, the `test_da.bat` file must also be changed

After CCI is running, the pairs are defined and `discoverArrays.xml` is edited, run `test_da.bat` to verify the `discoverArrays.pl` script. Various logging information is echoed to the console as the script executes. The last data echoed to the console is the contents of the file as specified in `<OutputFile>`. Something similar to the following appears on the console:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Response>
    <ArrayList>
        <Array id="10033">
            <Model>USP V / USP VM</Model>
            <Product>Universal Storage Platform</Product>
            <StoragePortList>
                <StoragePort id="50060e800427314d" type="FC"/>
            </StoragePortList>
        </Array>
    </ArrayList>
    <ReturnCode>0</ReturnCode>
</Response>
```

Ensure that the storage system ID and serial number match. More complex environments with multiple storage systems have one `<Array>` block per storage system. Also, ensure that the `<Model>` and `<Product>` lines are correct. If CCI is working, these data elements are all correct. If CCI is not working, it is obvious from the logging information echoed to the console as the script runs.

Ensure that the `<StoragePort>` lines match the ports with replication LUNs for VMware. One `<StoragePort>` line exists per storage port controlling replication on the storage system. If any ports are missing, the likely cause is that CCI cannot see any replicated LUNs on those ports. The storage port WWNs can be found via Device Manager.

Ensure that your CCI `horcm.conf` file is correct. You can manually verify this by running `raidqry -g` to get the list of pairs seen by this CCI instance, then running `pairdisplay -g <group> -few -fx CLI -l0` command for each group (adjust the `-l0` parameter as appropriate for the desired HORCM instance number). The port WWN for this storage system is in the fourth column of the first line for each pair set in the `pairdisplay` output. Execute this script on both the primary and secondary sites.
Verify LUN Discovery

test_dl.bat is the batch file to test whether discoverLuns.pl is working. For this test script, the XML input file is discoverLuns.xml.

discoverLuns.xml Contents

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<Command>
  <Name>discoverLuns</Name>
  <ConnectSpec>
    <Name>Hitachi Array</Name>
    <Address>0</Address>
  </ConnectSpec>
  <ArrayId>10033</ArrayId>
  <OutputFile>C:\Temp\discluns.xml</OutputFile>
  <LogLevel>Trivia</LogLevel>
</Command>
```

You might need to edit the following lines:

- `<Address>` – Set to the HORCM instance number
- `<ArrayId>` – Set to the serial number of the storage system to be tested (use the primary storage system’s serial number when testing the script on the protected site, and use the secondary storage system’s serial number when testing on the recovery site)
- `<OutputFile>` – Set to the location where the XML output is to be placed; if this line is changed, the test_dl.bat file must also be changed

For test_dl.bat, the output XML is similar to the following:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Response>
  <LunList arrayId="10033">
    <Lun id="173" wwn="60:06:0E:80:04:27:31:00:00:00:27:31:00:00:01:73">
      <Peer>
        <ArrayKey>25017</ArrayKey>
        <ReplicaLunKey>73</ReplicaLunKey>
      </Peer>
    </Lun>
    <Lun id="174" wwn="60:06:0E:80:04:27:31:00:00:00:27:31:00:00:01:74">
      <Peer>
        <ArrayKey>25017</ArrayKey>
      </Peer>
    </Lun>
  </LunList>
</Response>
```
Ensure that the <Lun> entries match information found by running a `pairdisplay -g <group> -few -fx -CLI` command for each group controlled by the indicated storage system serial number on the <LunList> line (which corresponds to the storage system ID as defined in `discoverLuns.xml`). Execute this script on both the primary and secondary sites.

**Verify Initiation of Failover Test**

The `test_failStart.bat` script tests the `failover.pl` script, specifically the `testFailover start` command. This script is only run from the secondary site, so ensure that you are on the correct server before beginning. For this script, the XML input file is `testFailoverStart.xml`.

**testFailoverStart.xml Contents**

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<Command>
  <Name>failover</Name>
  <Action>start</Action>
  <ConnectSpec>
    <Name>Hitachi Array</Name>
    <Address>0</Address>
  </ConnectSpec>
  <ArrayId>25017</ArrayId>
</Command>
```
You might need to edit the following lines:

- `<Address>` – Set to the HORCM instance number
- `<ArrayId>` – Set to the serial number of the secondary storage system
- `<ReplicaLunKey>` – Set to the LDEV number (in hex) for each TrueCopy S-VOL and ShadowImage P-VOL LUN in a pair group to test
- `<OutputFile>` – Set to the location where the XML output is to be placed; if this line is changed, the `test_failstart.bat` file must be changed as well

For `test_failstart.bat`, the output XML is similar to the following:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Response>
  <ReplicaLunList>
    <ReplicaLun key="74" wwn="60:06:0E:80:04:27:31:00:00:61:B9:00:00:00:78">
      <Number>37</Number>
    </ReplicaLun>
  </ReplicaLunList>
  <ReturnCode>0</ReturnCode>
</Response>
```

Ensure that the `<ReplicaLun>` entries match information found by running the command `pairdisplay -g <group> -few -fx -CLI` for each group containing the LUNs defined in the `testFailoverStart.xml` file. The key entry must match the input LUN key, and the WWN attribute corresponds to the ShadowImage S-VOL for the requested LUN to failover. The `<Number>` entry corresponds to the ShadowImage S-VOL. Also, scroll back a few lines in the script output and look for the `pairsplit` command and ensure it operates on the correct pair group or groups and returns 0 (for success).

**Verify Completion of Failover Test**

The `test_failStop.bat` script tests the `failover.pl` script, specifically the `testFailoverStop` command. This script is only run from the secondary site, so ensure that you are on the right server before beginning. For this script, the XML input file is `testFailoverStop.xml`.
**testFailoverStop.xml Contents**

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<Command>
  <Name>failover</Name>
  <Action>start</Action>
  <ConnectSpec>
    <Name>Hitachi Array</Name>
    <Address>0</Address>
  </ConnectSpec>
  <ArrayId>25017</ArrayId>
  <ReplicaLunKeyList>
    <ReplicaLunKey>74</ReplicaLunKey>
  </ReplicaLunKeyList>
  <OutputFile>C:\Temp\teststart.xml</OutputFile>
  <LogLevel>Trivia</LogLevel>
</Command>

You might need to edit the following lines:

- `<Address>` – Set to the HORCM instance number
- `<ArrayId>` – Set to the serial number of the secondary storage system
- `<ReplicaLunKey>` – Set to the LDEV number (in hex) for each TrueCopy S-VOL and ShadowImage P-VOL LUN in a pair group to test

*test_failstop.bat* has no output XML. Review the script output to ensure that the *pairresync* command operates on the correct pair group or groups and returns 0 (for success).

**Verifying the SRA in the SRM GUI**

Use the SRM GUI to verify connection to the storage systems as shown in Figure 2.

1. Log in to VirtualCenter on the protected site and go to the **Site Recovery** section.
2. Under **Array Managers**, click **Configure**.
Figure 2. Site Recovery Manager GUI
3. Click **Add** to reach the **Add Array Manager** screen as shown in Figure 3.

*Figure 3. Add Array Manager Screen*
4. Enter the HORCM instance for the protected site (typically 0) and click **OK**.

   After a brief delay while `discoverArrays.pl` is executing, the information for the protected site displays.

5. Verify that the SRA appears in the resulting screen (see Figure 4) and that the LUN Count field correctly represents the desired configuration.

   **Figure 4. Configure Array Managers Screen**

6. Click **Next** to perform the same steps for the recovery site, entering the HORCM instance controlling both the remote replication pairs and the local replication pairs (typically instance 0).

   After a brief delay while `discoverArrays.pl` is executing, the information for the recovery site displays.
7. Verify that the SRA appears in the resulting screen (see Figure 5) and that the LUN Count field correctly represents the desired configuration and click **Next** to complete the configuration.

*Figure 5. Configure Array Managers Screen – Recovery Site*

Storage Replication Adapter implementation is now complete. Your next step is to configure Site Recovery Manager.
VMware SRM Failback

After SRM fails over, you need to configure the original recovery site to act as the protected site, as shown in Figure 6.

*Figure 6. Failback Replication Configuration*

**Manual Configuration for Recovery**

This failback method assumes that the hardware on the original protected site is replaced and that new supported storage subsystems and new ESX Servers are in place.

1. Create the HORCM configuration according to the “Preparing CCI for Pair Operations” section following Figure 2.

   Use consistency groups for all LUNs that require application consistency.

2. Install SRM as described in the “Preparing CCI for Pair Operations” section.

3. Establish protection groups from the acting protected site.

4. Establish a recovery plan from the acting recovery site.

5. Test the recovery plan.

6. Shut down all applications and virtual machines on the acting protected site.

7. Execute a failover from the acting recovery site.

8. Verify that all virtual machines and applications are running properly.

Recovery is now complete. Applications can be returned to production.
Protected Site Cleanup

1. Delete all TrueCopy or Universal Replicator pairs.

2. Delete all ShadowImage pairs.

3. Browse to the datastore where the placeholder virtual machines are stored.

4. Delete all folders containing the placeholder virtual machines.

   All failed over datastores are now named with a prefix of `snap` and a number. These datastores can optionally be renamed using their original names.

5. On the acting protected site, delete all virtual machines from the disk.

6. Re-establish SRM for the protected site protection following the instructions in VMware’s `Administration Guide for Site Recovery Manager 1.0` and the “Preparing CCI for Pair Operations” section of this document.
Additional Reference Materials

For more information about related topics, see the following documents.

VMware Documentation

- Administration Guide for Site Recovery Manager 1.0 — Provides a conceptual overview as well as reference information about SRM prerequisites, system requirements, installation and licensing, configuring virtual machines, protected and recovery sites, recovery plans, testing and running failover, failback scenarios, adding users, procedural checklists and terminology.

- Site Recovery Manager 1.0 Release Notes — Provides last-minute information about Site Recovery Manager version 1.0.

- Site Recovery Manager Compatibility Matrixes — Lists server, client, database and guest operating system version compatibilities for Site Recovery Manager.

- Getting Started with Site Recovery Manager — Provides a high-level overview of Site Recovery Manager.

- Site Recovery Manager Evaluator Guide — Provides a conceptual overview and step-by-step workflows describing planning for using SRM, setting up protected and recovery sites, testing failover, the failover and failback process, alarms and status monitoring and a discussion of roles and privileges.

Hitachi Documentation


The following documentation is available to registered partners and customers on the Hitachi Data Systems Customer Support portal:


- Hitachi Universal Storage Platform V and Hitachi Universal Storage Platform VM Hitachi TrueCopy™ User’s Guide


- Hitachi TagmaStore® Universal Storage Platform and Network Storage Controller Universal Replicator User and Reference Guide

- Hitachi Universal Storage Platform V/VM Configuration Guide for VMware™ ESX Server Host Attachment