Deploy VMware Site Recovery Manager 5.5 with VMware vSphere 5.5 on Hitachi Virtual Storage Platform G1000

Reference Architecture Guide

By Michael Nakamura (Hitachi Data Systems), Tsuyoshi Inoue (Hitachi, Ltd.)

April 23, 2014
Feedback

Hitachi Data Systems welcomes your feedback. Please share your thoughts by sending an email message to SolutionLab@hds.com. To assist the routing of this message, use the paper number in the subject and the title of this white paper in the text.
# Table of Contents

**Solution Overview** ............................................................................................................. 3
VMware vCenter Site Recovery Manager Operations ........................................... 5

**Key Solution Components** ................................................................................................. 11
- Hitachi Virtual Storage Platform G1000 ................................................................. 11
- Hitachi Compute Blade 500 ....................................................................................... 11
- Hitachi TrueCopy Heterogeneous Remote Replication Bundle ................................... 11
- Hitachi Universal Replicator .................................................................................... 12
- Hitachi ShadowImage® Heterogeneous Replication ............................................... 13
- VMware vSphere 5.5 ..................................................................................................... 13
- VMware vCenter Site Recovery Manager 5.5 ............................................................. 14

**Solution Design** ....................................................................................................................... 15
- Compute Infrastructure ........................................................................................... 15
- SAN Infrastructure .................................................................................................. 19
- Storage Infrastructure ............................................................................................. 21

**Engineering Validation** .......................................................................................................... 29
- Test Methodology ...................................................................................................... 29
- Test Results ............................................................................................................... 29

**Conclusion** ............................................................................................................................... 30

**Configuring the Hitachi ShadowImage Pair** ........................................................................ 31
- horcm1.conf ............................................................................................................. 31
- horcm2.conf ............................................................................................................. 32
Deploy VMware Site Recovery Manager 5.5 with VMware vSphere 5.5 on Hitachi Virtual Storage Platform G1000

Reference Architecture Guide

Virtualizing a data center with VMware vSphere provides several benefits to IT infrastructures.

- Reduce capital expenses through server consolidation.
- Reduce operating expenses through automation that allows the data center to run more efficiently.
- Protect critical applications running on a central infrastructure with features such as VMware High Availability, which reduces planned and unplanned downtime.

Expanding data centers across multiple locations provides an opportunity to increase these layers of protection beyond a single data center.

VMware vCenter Site Recovery Manager is a business continuity and disaster recovery solution. It integrates vSphere infrastructures with array-based replication to either of the following:

- A traditional two-site design, with a protected site and recovery site
- A multi-site design, with multiple protected sites pointing to a single recovery site

The multi-site design provides higher levels of recovery point objectives (RPO) and recovery time objectives (RTO) when compared to traditional backup and recovery solutions.

Using an automated recovery plan, a production data center site can failover to a disaster recovery site in an organized and validated manner.

Remote data replication is a key function in building out stable and reliable disaster recovery environments. Although data replication can be performed at the server level, perform this function more efficiently within the storage infrastructure.
Hitachi Virtual Storage Platform G1000 is an integral piece in building out a robust business continuity and disaster recovery solution. VMware vCenter Site Recovery Manager integrates tightly with Virtual Storage Platform family using Hitachi Storage Replication Adapter. The advanced functionalities found in Virtual Storage Platform G1000 fulfill the requirements of a virtual infrastructure and provide reliable protection by managing data replication across data centers.

This paper is for IT administrators charged with the storage, deployment, or administration of VMware vSphere infrastructures on Hitachi Virtual Storage Platform G1000 and Hitachi Compute Blade 500. It assumes familiarity with storage area network (SAN)-based storage systems, VMware vSphere, Hitachi data replication technologies, and common IT storage practices.

---

**Note** — Testing of this configuration was in a lab environment. Many things affect production environments beyond prediction or duplication in a lab environment. Follow the recommended practice of conducting proof-of-concept testing for acceptable results in a non-production, isolated test environment that otherwise matches your production environment before your production implementation of this solution.
Solution Overview

This reference architecture uses a VMware infrastructure backed by Hitachi hardware and software to create two data centers. The following components create a business continuity and disaster recovery solution to protect a VMware vSphere virtualized data center:

- **Hitachi Compute Blade 500** — Enterprise-class server platform, containing internal Fibre Channel and network switch modules, that provides dense compute resources and high I/O throughput
- **Hitachi Virtual Storage Platform G1000** — High performance and highly scalable storage solution
- **Brocade 6510 Fibre Channel Switch** — SAN connectivity to the storage network for the data center
- **VMware vSphere 5.5** — Virtualization technology providing the infrastructure for the data center
- **VMware vCenter Site Recovery Manager 5.5** — Disaster recovery solution for protecting the vSphere virtual infrastructure
- **Hitachi Storage Replication Adapter 2.01.4** — Adapter for integrating VMware Site Recovery Manager with the Virtual Storage Platform family

Figure 1 on page 4 is an overview of the VMware vSphere environment.
Figure 1
VMware vCenter Site Recovery Manager Operations

These are the operations performed by VMware vCenter Site Recovery Manager.

The operations below leverage the Hitachi Storage Replication Adapter in conjunction with either of the following Hitachi storage-based replication technologies:

- Hitachi TrueCopy Synchronous Remote Replication bundle
- Hitachi Universal Replicator

The examples below use Hitachi TrueCopy.

Recovery

In a normal state, where replicating the primary site datastores to the recovery site, the ESXi host cannot mount the recovery site datastores as they are in a read-only state. This means the replicated protected virtual machines cannot register to the recovery site ESXi host.

Because of this, VMware vCenter Site Recovery Manager creates and registers placeholder virtual machine files to reserve a place in the vCenter inventory of the recovery site for the protected virtual machines. For your environment, configure the Management VM datastore on the recovery site ESXi host to store the placeholder virtual machine files.

The recovery operation for Site Recovery Manager has two options:

- Planned migration
- Disaster recovery

Depending on the selected option, built-in verification steps run prior to executing the recovery process. At the storage replication level, three steps occur for both options:

- Recovery process initiates a replication split.
- Primary site volume (P-VOL) becomes read-only.
- Recovery site volume (S-VOL) becomes read/write.

Figure 2 on page 6 shows the pair state after a recovery process has run.
Reprotect

After performing a recovery, the recovery site ESXi host has write access to the replicated volume (S-VOL) and starts the virtual machines on the recovery site. This state does not protect the virtual machines.

Once the primary site is back up, the reprotect operation of VMware vCenter Site Recovery Manager reverses the role of the two sites. The primary site protects the recovery site.

At the storage replication level, three steps occur:

- Recovery site volume converts to a primary volume (P-VOL).
- Primary site volume converts to secondary volume (S-VOL).
- Hitachi TrueCopy replication initiates from recovery site to primary site.

Figure 3 shows the pair state after running a reprotect process.
Recovery (Failback) and Reprotect

When ready to resume normal operations, failback is required to migrate back the production workload to the primary site.

Essentially, the failback process works the same as another recovery operation, except it works in the reverse direction from the initial recovery process.

At the storage replication level, three steps occur:

- Recovery process initiates a replication split.
- Recovery site volume (P-VOL) becomes read-only.
- Primary site volume (S-VOL) becomes read/write.

Figure 4 shows the pair state after recovery (failback) process has run.

SRM-initiated Failback

<table>
<thead>
<tr>
<th>Test</th>
<th>Cleanup</th>
<th>Recovery</th>
<th>Reprotect</th>
<th>Cancel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Site SRM</td>
<td>Recovery Site SRM</td>
<td>HORCM0 DKC1</td>
<td>HORCM1 DKC2</td>
<td>TrueCopy</td>
</tr>
</tbody>
</table>

| S-VOL R/W | P-VOL R/W |

Figure 4

After successfully completing the failback, run reprotect to initiate storage replication again. This ensures protection of the virtual machines and returns the environment to its original state.

At the storage replication level, three steps occur:

- Primary site volume converts back to a primary volume (P-VOL).
- Recovery site volume converts back to secondary volume (S-VOL).
- Hitachi TrueCopy replication initiates from primary site to recovery site.
Figure 5 shows the pair state after running the final reprotect.

**SRM-initiated Reprotect**

<table>
<thead>
<tr>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test</td>
</tr>
<tr>
<td>Cleanup</td>
</tr>
<tr>
<td>Recovery</td>
</tr>
<tr>
<td>Reprotect</td>
</tr>
<tr>
<td>Cancel</td>
</tr>
</tbody>
</table>

![Diagram of SRM-initiated Reprotect](image)

**Figure 5**

**Test Recovery**

VMware vCenter Site Recovery Manager provides a feature to test recovery plans without disrupting ongoing operations at either site. This uses a locally replicated copy of the recovery site volume. Add this optional function to the existing configuration by creating another replication LUN on the storage system of the recovery site.

Hitachi ShadowImage Heterogeneous Replication bundle creates an in-system asynchronously replicated pair between the Hitachi TrueCopy secondary volume (S-VOL) and the new LUN.

Figure 6 provides a diagram of the relationship between the TrueCopy and ShadowImage pairs.

![Diagram of Test Recovery](image)

**Figure 6**
Figure 6 on page 8 shows the following:

- The TrueCopy secondary volume (S-VOL) becomes the ShadowImage primary volume (P-VOL).
- A Hitachi Open Remote Copy Manager (HORCM) instance (horcm2) manages the ShadowImage secondary volume (S-VOL).

Both volumes are read-only. The ESXi host for the recovery site cannot access them.

When initiating the test recovery process, the replicated virtual machines attaches to one of the following:

- A non-production VMware vSphere virtual switch
- A private network specified in the recovery plan to avoid network conflicts with the protected virtual machines running on the primary site

At the storage replication level, two steps occur:

- Test recovery process initiates a replication split of the ShadowImage pair.
- Recovery site ShadowImage replicated volume (S-VOL) is made read/write.

Figure 7 shows the pair state after the test recovery process has run.

![SRM-initiated Test Recovery Diagram]

Figure 7
This configuration allows the recovery site ESXi host to power on the replicated virtual machines safely without disrupting the TrueCopy replication. This provides the administrator with a tangible method for testing and validating the disaster recovery process.

For more details around the configuration of the ShadowImage relationship, see “Configuring the Hitachi ShadowImage Pair,” starting on page 31.

**Cleanup**

After running a test recovery operation, the cleanup process returns the recovery site ESXi host to its original state. This powers off the replicated virtual machines and restores the placeholder virtual machines.

At the storage replication level, two steps occur:

- On the recovery site, the Hitachi ShadowImage replicated volume (S-VOL) becomes read-only.
- Cleanup process resumes ShadowImage replication.

Figure 8 shows the pair state after the cleanup process has run.
Key Solution Components

The following are descriptions of the components used in this reference architecture.

Hitachi Virtual Storage Platform G1000

Hitachi Virtual Storage Platform G1000 provides an always-available, agile, and automated foundation that you need for a continuous infrastructure cloud. This delivers enterprise-ready software-defined storage, advanced global storage virtualization, and powerful storage.

Supporting always-on operations, Virtual Storage Platform G1000 includes self-service, non-disruptive migration and active-active storage clustering for zero recovery time objectives. Automate your operations with self-optimizing, policy-driven management.

Virtual Storage Platform G1000 supports Oracle RAC and VMware Metro Storage Cluster.

Hitachi Compute Blade 500

Hitachi Compute Blade 500 combines the high-end features with the high compute density and adaptable architecture you need to lower costs and protect investment. Safely mix a wide variety of application workloads on a highly reliable, scalable, and flexible platform. Add server management and system monitoring at no cost with Hitachi Compute Systems Manager, which can seamlessly integrate with Hitachi Command Suite in IT environments using Hitachi storage.

The Hitachi Compute Blade 500 chassis contains internal Fibre Channel and network switches for the high availability requirements of Hitachi Unified Compute Platform for VMware vSphere.

Hitachi TrueCopy Heterogeneous Remote Replication Bundle

For synchronous replication up to 190 miles (300 km), Hitachi TrueCopy Synchronous Remote Replication provides a no-data-loss, rapid restart solution. Real-time copies are the same as the originals. This reduces recovery time to minutes.

Synchronous replication provides very fast recovery time (low RTO) and good data currency (low RPO) between Hitachi storage systems.
Hitachi Universal Replicator

Hitachi Universal Replicator for Hitachi Virtual Storage Platform G1000 is an advanced technology for asynchronously replicating data hosted on Virtual Storage Platform family models.

Asynchronous replication maintains a remote copy of data without having a performance impact on the primary data. In asynchronous replication, the system considers an input-output update operation complete when confirming the update at the primary site.

Hitachi Virtual Storage Platform G1000 manages the process of replicating the changes to the secondary site.

Hitachi Universal Replicator uses disk-based journaling and an optimized replication engine to reduce resource consumption and costs while increasing performance and operational resilience. The strengths of Hitachi Universal Replicator are two key technical innovations: performance optimized, disk based journaling and a pull-style replication engine.

Following are the key characteristics of the Universal Replicator software:

- **Replication across any distance without significant negative effect on host performance** — Hitachi Universal Replicator has been successfully used in replication configurations that span thousands of miles.

- **No acknowledgment dependencies from secondary site** — Hitachi Universal Replicator replicates to a remote site without the affect on performance of waiting for acknowledging each individual record. Instead, Hitachi Universal Replicator manages the remote relationship at a controller level. During a disruption of communication to the remote unit or while exceeding the capability of the replication circuit, Hitachi Universal Replicator retains a replicated write data in local journals, then updates the write data when the condition is corrected.

There is a potential for some data lag between remote and primary sites, particularly at longer distances. Manage the recovery point objective with the configuration of the data communication lines. When input-output activity at the primary site exceeds the capacity of the communication channel, the data is staged and moved to the secondary site in the same order as it was written at the primary site.
Hitachi ShadowImage® Heterogeneous Replication

Hitachi ShadowImage® Heterogeneous Replication is a storage-based hardware solution that creates RAID-protected duplicate volumes within the Hitachi Virtual Storage Platform family. ShadowImage Heterogeneous Replication primary volumes (P-VOLs) contain the original data. Up to nine secondary volumes (S-VOLs) can be created as copies.

On Hitachi Virtual Storage Platform G1000, use ShadowImage Heterogeneous Replication to implement clones, a full copy of the primary data. The clone is available for use by secondary applications. The unique value of working with a clone is that any operation on the clone has no effect on the primary data.

Detailed information on using Shadow Image Heterogeneous Replication is in *Hitachi Command Control Interface User and Reference Guide* (MK-90RD7010).

VMware vSphere 5.5

VMware vSphere 5.5 is a virtualization platform that provides a data center infrastructure. It features vSphere Distributed Resource Scheduler (DRS), high availability, and fault tolerance.

Use of the round robin multipathing policy in vSphere 5.5 distributes the load across multiple host bus adapters (HBAs) and multiple storage ports. Use of DRS with Hitachi Dynamic Provisioning automatically distributes loads on the ESX host and across the back end of the storage system.

VMware vSphere 5.5 has the following components:

- **ESXi 5.5** — This is a hypervisor that loads directly on a physical server. It partitions one physical machine into many virtual machines that share hardware resources.

- **vCenter Server** — This allows management of the vSphere environment through a single user interface. With vCenter, there are features available such as vMotion, Storage vMotion, Distributed Resource Scheduler, high availability, and fault tolerance.

For more information, see the [VMware vSphere](https://www.vmware.com) website.
VMware vCenter Site Recovery Manager 5.5

VMware vCenter Site Recovery Manager 5.5 is a disaster recovery solution that helps to reduce planned and unplanned downtime of a vSphere infrastructure. It enables automated site recovery and migration processes. This can leverage the built-in vSphere Replication for hypervisor-based replication to cover a wide range of required recovery time and data currency.

This reference architecture focuses on using Site Recovery Manager with storage-based replication technologies such as Hitachi TrueCopy Heterogeneous Remote Replication bundle and Hitachi Universal Replicator. This use provides a centralized management of recovery plans. Tight integration between storage arrays, VMware vCenter, VMware vCenter Site Recovery Manager, and the Hitachi Storage Replication Adapter ensure a coordinated recovery for large, business critical environments.

For more information, see VMware vCenter Site Recovery Manager on the VMware website.
Solution Design

This reference architecture is for a virtualized data center protected by VMware Site Recovery Manager. It uses the hardware and software components described in “Key Solution Components,” starting on page 11, to build the following infrastructures:

- Compute
- Storage area network
- Storage infrastructure

The architecture uses a synchronous and asynchronous storage replication model in a Site Recovery Manager environment to illustrate support for different recovery point objective (RPO) requirements.

Compute Infrastructure

This describes the compute infrastructure used in this reference architecture.

- Hardware components
  - Hitachi Compute Blade 500
  - VMware vSphere 5.5
- Disaster recovery and replication control components
  - VMware vCenter Site Recovery Manager (SRM) 5.5
  - Hitachi Storage Replication Adapter 2.01
  - Command control interface
Hitachi Compute Blade 500

A Hitachi Compute Blade 500 hosts the VMware vSphere 5.5 infrastructure. Table 1 shows the hardware configuration with two server blades.

Table 1. Hitachi Compute Blade 500 Configuration

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Detail Description</th>
<th>Version</th>
<th>Quantity</th>
</tr>
</thead>
</table>
| Hitachi Compute Blade 500 Chassis | ▪ 8-blade chassis  
▪ 2 Brocade 5460 Fibre Channel switch modules, each with 6 × 8 Gb/sec uplink ports  
▪ 2 Brocade VDX 6746 Ethernet switch modules, each with 8 × 10 Gb/sec uplink ports  
▪ 2 management modules  
▪ 6 cooling fan modules  
▪ 4 power supply modules | SVP: A0165-E-8205  
5460: FOS v7.0.2c | 1 |
| 520H B2 server blade | ▪ Half blade  
▪ 2 × 12-core Intel Xeon E5-2697 v2 processor, 2.70 GHz  
▪ 192 GB RAM  
▪ 16 × 16 GB DIMMs | BMC/EFI: 04-13 | 2 |

Each server blade has VMware ESXi 5.5 installed. This is the basis for simulating a primary and recovery virtualized data center site.

VMware vSphere 5.5

For this reference architecture, the entire primary and recovery sites are contained in respective VMware vSphere 5.5 infrastructures with the following components:

▪ Virtual infrastructure management
▪ Disaster recovery management
▪ Storage array replication management
▪ Protected/recovery virtual machine environment
Three resource pools were created in both vSphere 5.5 infrastructures to separate the virtual machines by functionality and type of protection:

- Management
- Sync Protected
- Async Protected

The management resource pool contained three virtual machines for the following functions:

- **Infrastructure Management** — Microsoft Windows Server 2012 virtual machine running VMware vCenter Server 5.5 for overall management of the virtualized infrastructure

- **Database** — Microsoft Windows Server 2012 virtual machine running Microsoft SQL Server 2012. This serves database instances for vCenter Server 5.5 and Site Recovery Manager 5.5

- **Disaster Recovery Management** — Microsoft Windows Server 2012 virtual machine running VMware Site Recovery Manager, Hitachi Storage Replication Adapter and command control interface. This handles the replication communication between the virtual and storage infrastructure as well as site-to-site communications between Site Recovery Manager instances to facilitate an integrated disaster recovery process.

The Sync Protected and Async Protected resource pools on the primary site consisted of several virtual machines running on their respective storage replicated VMFS primary volumes or P-VOLs.

The Sync Protected and Async Protected resource pools on the recovery site contained placeholder virtual machines created by Site Recovery Manager for mirroring the protected virtual machines of the primary site.

**Disaster Recovery and Replication Control Components**

Handling the virtual infrastructure disaster recovery and storage replication control is through the following software components installed on a virtual machine outlined in Table 2.

<table>
<thead>
<tr>
<th>Application</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Site Recovery Manager</td>
<td>5.5 Build 1315893</td>
</tr>
<tr>
<td>Hitachi Storage Replication Adapter</td>
<td>02.01.04</td>
</tr>
<tr>
<td>Command control interface</td>
<td>01-31-03/06</td>
</tr>
</tbody>
</table>

Installing VMware Site Recovery Manager is a prerequisite to installing the Hitachi Storage Replication Adapter. This is necessary to ensure that Site Recovery Manager can properly register the installed adapter.
Install and download the client plug-in from Site Recovery Manager server from the Manage Plug-ins menu in the vSphere client. Use this to configure and manage Site Recovery Manager.

Rescan the Storage Replication Adapter from the SRAs tab in the Array Managers interface of Site Recovery Manager. Use this to verify the installed Hitachi adapter version and supported array models.

Use command control interface from Hitachi to perform storage system operations by issuing commands to Hitachi Virtual Storage Platform G1000. There are command control interface components residing on the following:

- **Storage system** — Command devices and Hitachi TrueCopy or Hitachi Universal Replicator volumes (P-VOLs and S-VOLs)
- **Server** — Hitachi Open Remote Copy Manager (HORCM), configuration definition files (for example, horcm0.conf), and command control interface commands

Create command device logical volumes on the local and remote storage systems. Present these logical volumes as physical raw device mappings (RDM) to their respective Site Recovery Manager virtual machine.

Figure 9 on page 19 shows the overall architecture of the disaster recovery and replication control components in a vSphere environment.
SAN Infrastructure

This describes the SAN infrastructure used in this reference architecture.

Server to Storage SAN Design

Each server blade at the local and remote site used dual-port Fibre Channel mezzanine cards. They connect internally to the internal Fibre Channel switch modules located in the Hitachi Compute Blade 500 chassis.

Two inter-switch links from the internal Fibre Channel switch module connect to two Brocade 6510 switches, one link per switch for redundancy. The multipathing policy was set to round robin in ESXi 5.5.
Figure 10 shows the storage network configured identically for each site.

**Figure 10**

**Storage to Storage SAN Design**

To facilitate the copying of data between storage systems, configure storage replication links between the Hitachi Virtual Storage Platform G1000 storage system on the local site and the Virtual Storage Platform G1000 storage system on the remote site. Each storage system used a total of two initiator ports and two RCU target ports.

A storage replication link consists of an initiator port on the primary storage system connected to a remote control unit RCU target port defined on the recovery storage system. It represents a one-way remote copy connection from the primary data volume (P-VOL) on the primary storage system to the secondary data volume (S-VOL) on the recovery storage system.

For this solution, the configuration of a second storage replication link had an initiator port on the recovery storage system connected to an RCU target port on the primary storage system. This enables reversing the direction of replication from the recovery site to the primary site for reprotect using VMware Site Recovery Manager. Two additional replication links connect through two Brocade 6510 switches. This creates a total of four paths to provide maximum hardware redundancy following best practice.
Figure 11 shows the storage system site-to-site configuration.

- **Primary-Recovery replication for Failover**
  - (2 Initiator ports – 2 RCU Target ports)
- **Recovery-Primary replication for Failback**
  - (2 Initiator ports – 2 RCU Target ports)
- **Replication Link**

---

**Figure 11**

**Storage Infrastructure**

The storage infrastructure used in this reference architecture consists of the following:

- **Storage Design**
- **Defining Volume Pair Relationship**
- **Storage Replication**

**Storage Design**

For this reference architecture, use Hitachi Dynamic Provisioning on Hitachi Virtual Storage Platform G1000 to simplify the management of the storage with the following:

- **Over provisioning**
- **Wide striping**
- **On-line expansion of dynamic provisioning pools**
This solution uses a dynamic provisioning pool comprised of a single RAID group with eight 900 GB 10k RPM SAS drives in a RAID-6 (6D+2P) configuration for each storage system. Using a RAID-6 configuration lowers the risk of data loss or pool failure, which is a primary concern for virtual machines protected in a VMware Site Recovery Manager environment.

Figure 12 shows the configuration for the dynamic provisioning pool on each storage system for our test environment.
Five VMFS LUNs were provisioned:

- Datastore for storing management virtual machines (non-replicated)
- Datastore for storing the operating system (drive C) virtual disks of synchronous replication-protected virtual machines
- Datastore for storing the data (drive D) virtual disks of synchronous replication-protected virtual machines
- Datastore for storing the operating system (drive C) virtual disks of asynchronous replication-protected virtual machines
- Datastore for storing the data (drive D) virtual disks of asynchronous replication-protected virtual machines

The Hitachi Virtual Storage Platform G1000 configuration on the recovery site is identical to the primary site configuration. The recovery LUNs on the recovery site is identical in size to their respective protected LUNs, as required for maintaining the P-VOL and S-VOL relationship.

Provision a 46 MB LUN, the smallest LUN that can be created, on both sites. Convert these LUNs to a command device. A command device is a dedicated logical volume on the storage system that functions as the interface to the storage system from a host. In this solution, command control interface sends replication commands to the command device for execution on the storage system.

Both systems had LUNs created for the storing journal data required for Hitachi Universal Replicator volume pairs. The LUNs must be assigned with journal group IDs in order to be used as a journal volume by Hitachi Universal Replicator.

**Defining Volume Pair Relationship**

A key aspect of this VMware Site Recovery Manager 5.5 reference architecture using Hitachi Virtual Storage Platform G1000 is defining the volume pair relationship for replication between storage systems. Define and manage storage replication relationships through the Hitachi Storage Navigator graphical user interface (GUI) or a host running Hitachi Open Remote Copy Manager (HORCM).

Hitachi Open Remote Copy Manager is a component of command control interface. It manages replication using a command-line interface. For this solution, the command control interface enables Hitachi Storage Replication Adapter to issue Open Remote Copy Manager commands for managing, monitoring, and controlling the replication process initiated by VMware Site Recovery Manager.

Each Open Remote Copy Manager instance installed at the primary and recovery site contains a configuration definition file (`horcmx.conf`). This file defines the devices in copy pairs. Define the configuration file before starting the Open Remote Copy Manager daemon.
Figure 13 shows the `horcm0.conf` file contents used when testing the environment:

```
#FileName: horcm0.conf
#
/*---------------------------------- For HORCM_MON ----------------------------------*/
HORCM_MON
#ip_address service poll(10ms) timeout(10ms)
172.17.171.233 horcm0 1000 3000
#
/*---------------------------------- For HORCM_CMD ----------------------------------*/
HORCM_CMD
#dev_name dev_name dev_name
\\CMD-300002
#
/*---------------------------------- For HORCM_LDEV ----------------------------------*/
HORCM_LDEV
#dev_group dev_name Serial# CU:LDEV(LDEV#) MU#
VM01_TC VM01_C 300002 00:08
VM01_TC VM01_D 300002 00:09
VM02_UR VM02_C 300002 00:0C
VM02_UR VM02_D 300002 00:0D
#
/*---------------------------------- For HORCM_INST ----------------------------------*/
HORCM_INST
#dev_group ip_address service
VM01_TC 172.17.171.234 horcm1
VM02_UR 172.17.171.234 horcm1
```

Figure 13

Figure 14 shows the `horcm1.conf` file contents used when testing the environment:

```
#FileName: horcm1.conf
#
/*---------------------------------- For HORCM_MON ----------------------------------*/
HORCM_MON
#ip_address service poll(10ms) timeout(10ms)
172.17.171.234 horcm1 1000 3000
#
/*---------------------------------- For HORCM_CMD ----------------------------------*/
HORCM_CMD
#dev_name dev_name dev_name
\\CMD-354321
#
/*---------------------------------- For HORCM_LDEV ----------------------------------*/
HORCM_LDEV
#dev_group dev_name Serial# CU:LDEV(LDEV#) MU#
VM01_TC VM01_C 354321 00:23
VM01_TC VM01_D 354321 00:24
VM02_UR VM02_C 354321 00:2F
VM02_UR VM02_D 354321 00:30
#
/*---------------------------------- For HORCM_INST ----------------------------------*/
HORCM_INST
#dev_group ip_address service
VM01_TC 172.17.171.233 horcm0
VM02_UR 172.17.171.233 horcm0
```

Figure 14
Figure 13 and Figure 14 show logical devices or LUNs associated to device group TC-SRM and device group HUR-SRM.

In the VM01_TC pair, the following is true:

- **horcm0** instance manages P-VOLs defined as LUN 00:08 and LUN 00:09 on a Virtual Storage Platform G1000 registered with serial number 300002.
- **horcm1** instance manages S-VOLs defined as LUN 00:23 and LUN 00:24 on a Virtual Storage Platform G1000 registered with serial number 354321.

For the VM02_UR pair, the following is true:

- **horcm0** instance manages P-VOLs defined as LUN 00:0C and LUN 00:0D on a Virtual Storage Platform G1000 registered with serial number 300002.
- **horcm1** instance manages S-VOLs defined as LUN 00:2F and LUN 00:30 on a Virtual Storage Platform G1000 registered with serial number 354321.

Following recommended practice when testing, the following was done:

- The HORCM configuration file on the primary site managing the P-VOL was labeled with an even number (**horcm0.conf**).
- The HORCM configuration file on the recovery site managing the S-VOL was labeled with an odd number (**horcm1.conf**).

Table 3 shows the pair configuration defined by the configuration files in Figure 13 and Figure 14.

<table>
<thead>
<tr>
<th>Device Group</th>
<th>VSP G1000 Serial Number</th>
<th>LUN</th>
<th>Volume Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM01_TC</td>
<td>300002</td>
<td>00:08</td>
<td>P-VOL</td>
</tr>
<tr>
<td></td>
<td>354321</td>
<td>00:23</td>
<td>S-VOL</td>
</tr>
<tr>
<td>VM01_TC</td>
<td>300002</td>
<td>00:09</td>
<td>P-VOL</td>
</tr>
<tr>
<td></td>
<td>354321</td>
<td>00:24</td>
<td>S-VOL</td>
</tr>
<tr>
<td>VM02_UR</td>
<td>300002</td>
<td>00:0C</td>
<td>P-VOL</td>
</tr>
<tr>
<td></td>
<td>354321</td>
<td>00:2F</td>
<td>S-VOL</td>
</tr>
<tr>
<td>VM02_UR</td>
<td>300002</td>
<td>00:0D</td>
<td>P-VOL</td>
</tr>
<tr>
<td></td>
<td>354321</td>
<td>00:30</td>
<td>S-VOL</td>
</tr>
</tbody>
</table>
Figure 15 verifies the pair relationship by running the `pairdisplay` command from the `horcm0` instance. Initially, the volumes are in simplex (SMPL) mode. The volumes are not paired and synchronized until running the `paircreate` command.

C:\HORCM\etc\pairdisplay.exe -g VM01_TC -Ih00 -fc
Group    PairVol(L/R) (Port#, TID, LU), Seq#, LDEV#. P/S, Status,Fence, %,P-LDEV# M
VM01_TC  VM01_C(L) (CL3-C-3,30), 2) 300002 8. SMPL ---- ----- ----- ----- -
VM01_TC  VM01_C(R) (CL2-D-2,19, 2) 354321 23. SMPL ---- ----- ----- ----- -
VM01_TC  VM01_D(L) (CL3-C-3,30, 4) 300002 9. SMPL ---- ----- ----- ----- -
VM01_TC  VM01_D(R) (CL2-D-2,19, 4) 354321 24. SMPL ---- ----- ----- ----- -

C:\HORCM\etc\pairdisplay.exe -g VM02_UR -Ih00 -fc
Group    PairVol(L/R) (Port#, TID, LU), Seq#, LDEV#. P/S, Status,Fence, %,P-LDEV# M
VM02_UR  VM02_C(L) (CL3-C-3,30, 3) 300002  c. SMPL ---- ----- ----- ----- -
VM02_UR  VM02_C(R) (CL2-D-2,19, 3) 354321 2f. SMPL ---- ----- ----- ----- -
VM02_UR  VM02_D(L) (CL3-C-3,30, 5) 300002  d. SMPL ---- ----- ----- ----- -
VM02_UR  VM02_D(R) (CL2-D-2,19, 5) 354321 30. SMPL ---- ----- ----- ----- -

**Figure 15**

**Storage Replication**

After defining volume pair relationships and starting the Hitachi Open Remote Copy Manager (HORCM) daemon, initiate storage replication using HORCM commands.

The reference architecture tested the VMware Site Recovery Manager environment using two types of storage replication technologies available with Hitachi Virtual Storage Platform G1000. This addressed different recovery point objective (RPO) requirements, as shown in Table 4.

**Table 4. RPO Requirements**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Replication Type</th>
<th>Storage Replication Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low RPO</td>
<td>Synchronous remote replication</td>
<td>Hitachi TrueCopy Remote Replication bundle</td>
</tr>
<tr>
<td>Flexible RPO</td>
<td>Asynchronous remote replication</td>
<td>Hitachi Universal Replicator</td>
</tr>
</tbody>
</table>

VMware Site Recovery Manager 5.0 introduced a hypervisor-based replication called vSphere Replication. This complements storage-based replication by enabling disaster recovery protection for another tier of virtual machines that may not fall under the higher priority RPO requirements provided by a storage system. This replication method is outside of the scope of this reference architecture.
Low RPO — Synchronous remote replication

Synchronous (real-time) replication provides a high level of data consistency protection. It ensures that the remote data is identical to the local data.

The drawback to synchronous replication is its distance limitation. In synchronous replication, an input-output update operation from a virtual machine is not complete until confirming the completion at the primary and recovery site. With increased distances, this can cause problems for latency-sensitive applications or virtual machines.

The practical distance for synchronous replication ranges from 20 miles (32 km) to 100 miles (161 km), depending on application or virtual machine tolerance. Synchronous replication up to 190 miles (300 km) requires using WAN-optimized controllers.

Initiate Hitachi TrueCopy Synchronous replication from the horcm0 instance by typing the following at a command prompt in the C:\HORCM\etc directory:

```
paircreate.exe -g <grp> -vl -fg <fence> <CTGID> -IH0
```

Figure 16 shows the command and the output of a TrueCopy pair creation based on the HORCM configuration files in Figure 13 and Figure 14 on page 24.

```
C:\HORCM\etc>paircreate.exe -g VM01_TC -vl -fg never -IH0
```

<table>
<thead>
<tr>
<th>Group</th>
<th>PairVol(L/R)</th>
<th>Port#, TID, LU</th>
<th>Seq#</th>
<th>LDEV#</th>
<th>P/S</th>
<th>Status</th>
<th>Fence</th>
<th>%</th>
<th>P-LDEV#</th>
<th>M CTG</th>
<th>JID</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM01_TC</td>
<td>VM01_C(L)</td>
<td>CL3-M-3,30</td>
<td>2000002</td>
<td>8</td>
<td>P-VOL COPY NEVER</td>
<td>36</td>
<td>23</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VM01_TC</td>
<td>VM01_C(R)</td>
<td>CL2-D-2,19</td>
<td>354321</td>
<td>23</td>
<td>S-VOL COPY NEVER</td>
<td>8</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VM01_TC</td>
<td>VM01_D(L)</td>
<td>CL3-M-3,30</td>
<td>300002</td>
<td>9</td>
<td>P-VOL COPY NEVER</td>
<td>24</td>
<td>0</td>
<td>-</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VM01_TC</td>
<td>VM01_D(R)</td>
<td>CL2-D-2,19</td>
<td>354321</td>
<td>24</td>
<td>S-VOL COPY NEVER</td>
<td>9</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 16

The fence level setting specified during the `paircreate` operation is critical in defining the P-VOL behavior when interrupting a TrueCopy pair. For example, setting the fence level to `Data` prevents the host from writing updates to the P-VOL during a replication failure. This keeps the S-VOL identical to the P-VOL, which can lower recovery time by assuring the currency of the data.

However, when storage replication has failed but the primary site still functions, TrueCopy disables write access to the VMFS volume from the primary site ESXi hosts. This disrupts the production virtual machines. Use this setting for critical volumes where data consistency outweighs virtual machine uptime.

The example in Figure 16 uses a fence level setting of `Never`. This supports input-output performance and virtual machine uptime over data recovery. The host has access and continues to update the P-VOL. However, the S-VOL may not be synchronized.
During a replication link failure, the primary site could still function. However, a data consistency vulnerability exists on the recovery site until fixing replication.

Carefully consider various disaster recovery scenarios when setting fence levels.

The CTGID, or consistency group ID, ensures data consistency among multiple datastores assigned to Hitachi device groups. The datastores are maintained in a state of replication consistent with each other. For example in Figure 16 on page 27, a CTGID of 0 is assigned. If replication is stopped on the pair VM01_C, replication will also be stopped on VM01_D. Use consistency groups in virtual machine configurations where multiple virtual disks reside on different datastores.

Find further details on fence level and consistency group ID settings in Hitachi TrueCopy User Guide.

**Flexible RPO — Asynchronous Remote Replication**

Asynchronous replication provides a less favorable RPO than synchronous replication. However, it overcomes the distance limitations of synchronous replication.

Hitachi Universal Replicator uses disk journal volumes on the primary site and the storage system at the recovery site as a buffer mechanism. This eliminates the wait for the input-output response from the remote site. Providing data integrity with minimal host performance impact, this reduces the complexity and cost of replicating data.

Initiate Hitachi Universal Replicator asynchronous replication from the horc0 instance by typing the following at a command prompt in the C:\HORCM\etc directory:

```cmd
paircreate.exe -g <grp> -vl -f async -jp < jornal id> -js <journal id> -l H0
```

Figure 17 shows the command and the output of a Universal Replicator pair creation based on the configuration files in Figure 13 and Figure 14 on page 24.

C:\HORCM\etc>paircreate.exe -g VM02_UR -vl -f async -jp 00 -js 00 -lH0

```cmd
C:\HORCM\etc>pairdisplay.exe -g HUR-SRM -lH0 -fexe
Group PairVol(L/R) (Port#,TID, LU), Seq#, LDEV#: P/S, Status, Fence, %,P-LDEV# M CTG JID AP
VM02_UR VM02_C(L) (CL3-C-3,30, 3) 300002 c. P-VOL COPY ASYNC, 0 2f  1 0 1
VM02_UR VM02_C(R) (CL2-D-2,19, 3) 354321 2f. S-VOL COPY ASYNC,----- c - 1 0 1
VM02_UR VM02_D(L) (CL3-C-3,30, 3) 300002 d. P-VOL COPY ASYNC, 0 30 - 1 0 1
VM02_UR VM02_D(R) (CL2-D-2,19, 5) 354321 30. S-VOL COPY ASYNC,----- d - 1 0 1
```

**Figure 17**
Engineering Validation

This describes the tests performed in the Hitachi Data Systems lab using VMware vCenter Site Recovery Manager 5.5.

Test Methodology

These were the steps followed to test the reference architecture:

1. Build the environment and have VMware vCenter Site Recovery Manager discover the replicated devices on both sites.

2. Create Site Recovery Manager Protection Groups for the protected virtual machines based on the replicated VMFS datastore where they resided.


4. Perform the following functions:
   - Recovery
   - Reprotect
   - Recovery (failback) and reprotect
   - Test Recovery
   - Cleanup

5. Use the `pairdisplay` command in command control interface to verify each function worked.

A test passes if each function works as intended in the reference architecture.

Separate testing used Hitachi TrueCopy Remote Replication bundle and Hitachi Universal Replicator to validate this reference architecture.

Test Results

All functions described in worked as intended. Using the `pairdisplay` command in command control interface confirmed the replicated pair had the correct status for each function tested.

Each function performed with Site Recovery Manager yielded the same results from a storage replication perspective whether using Hitachi TrueCopy Remote Replication bundle or Hitachi Universal Replicator for the procedure.
Conclusion

This reference architecture guide documents validating a disaster recovery solution using VMware Site Recovery Manager 5.5 with VMware vSphere 5.5 on Hitachi Virtual Storage Platform G1000.

Hitachi Virtual Storage Platform G1000 provides multiple storage replication capabilities for different business needs. Hitachi Storage Replication Adapter allows VMware vCenter Site Recovery Manager to leverage these storage replication capabilities to protect virtualized vSphere data centers effectively.

This integrated and coordinated effort provides IT administrators with multiple options to match the desired recovery point objective (RPO) and recovery time objective (RTO).
Configuring the Hitachi ShadowImage Pair

The Hitachi ShadowImage pair definition used these HORCM configuration files during testing.

Only specify mirror unit numbers (MU#) when defining ShadowImage pairs. Initiate ShadowImage local replication using the following command run from the `horcm1` instance in `C:\HORCM\etc>`:

```
paircreate.exe -g <grp> -vl -lm
```

Only initiate Hitachi ShadowImage replication after establishing Hitachi TrueCopy replication.

**horcm1.conf**

Figure 18 shows the contents of an updated `horcm1.conf` file.

```bash
#FileName: horcm1.conf
/#**************************************** For HORCM_MON ********************************************/
HORCM_MON
#ip_address service poll(10ms) timeout(10ms)
172.17.171.234 horcm1 1000 3000
/#**************************************** For HORCM_CMD ********************************************/
HORCM_CMD
#dev_name dev_name dev_name
\\.CMD-354321
/#**************************************** For HORCM_LDEV ********************************************/
HORCM_LDEV
#dev_group dev_name Serial# CU:LDEV(LDEV#) MU#
VM01_TC VM01_C 354321 00:23
VM01_TC VM01_D 354321 00:24
VM02 UR VM02_C 354321 00:2F
VM02 UR VM02_D 354321 00:30
VM01 SI VM01_C SI 354321 00:23 0
VM01 SI VM01_D SI 354321 00:24 0
/#**************************************** For HORCM_INST ********************************************/
HORCM_INST
#dev_group ip_address service
VM01 TC 172.17.171.233 horcm0
VM02 UR 172.17.171.233 horcm0
VM01 SI 172.17.171.234 horcm2
```

**Figure 18**
Figure 19 shows the contents of `horcm2.conf` file.

```
#FileName: horcm2.conf
#************************************************************************ For HORCM_MON **************************************************************************
HORCM_MON
#ip_address service poll(10ms) timeout(10ms)
172.17.171.234 horcm2 1000 3000
#************************************************************************ For HORCM_CMD **************************************************************************
HORCM_CMD
#dev_name dev_name dev_name \\CMD-354321
#************************************************************************ For HORCM_LDEV **************************************************************************
HORCM_LDEV
#dev_group dev_name Serial# CU:LDEV(LDEV#) MU#
VM01_SI VM01_C_SI 354321 00:14
VM01_SI VM01_D_SI 354321 00:15
#************************************************************************ For HORCM_INST **************************************************************************
HORCM_INST
#dev_group ip_address service
VM01_SI 172.17.171.234 horcm1
```
For More Information

Hitachi Data Systems Global Services offers experienced storage consultants, proven methodologies and a comprehensive services portfolio to assist you in implementing Hitachi products and solutions in your environment. For more information, see the Hitachi Data Systems Global Services website.

Live and recorded product demonstrations are available for many Hitachi products. To schedule a live demonstration, contact a sales representative. To view a recorded demonstration, see the Hitachi Data Systems Corporate Resources website. Click the Product Demos tab for a list of available recorded demonstrations.

Hitachi Data Systems Academy provides best-in-class training on Hitachi products, technology, solutions and certifications. Hitachi Data Systems Academy delivers on-demand web-based training (WBT), classroom-based instructor-led training (ILT) and virtual instructor-led training (vILT) courses. For more information, see the Hitachi Data Systems Services Education website.

For more information about Hitachi products and services, contact your sales representative or channel partner or visit the Hitachi Data Systems website.