Best Practices Guide

By Dave Brandman

October 24, 2012
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

Background ........................................................................................................ 3

Types of Operation ............................................................................................ 5
  Normal Operation .......................................................................................... 5
  Failover Operation ..................................................................................... 7

Discussion of Failover for Applications Using
Hitachi Content Platform 5 or Later ................................................................. 9

Discussion of Failover for Applications Using
Hitachi Content Platform 4 .............................................................................. 11

Summary .......................................................................................................... 13

Bibliography ..................................................................................................... 14
Hitachi Content Platform Failover Processing Using Storage Adapter for Symantec™ Enterprise Vault

Best Practices Guide

Storage Adapter for Symantec™ Enterprise Vault from Hitachi Data Systems is an implementation of an adapter using the Symantec-developed Streamer API. Storage adapter allows communication between Symantec Enterprise Vault and Hitachi Content Platform using the REST interface. It also provides support for many of the advanced storage features of Content Platform, including replication.

Replication allows one or more namespaces on one Content Platform to asynchronously replicate objects to a replica Content Platform over TCP/IP. The replica Content Platform does not need to be dedicated to this function.

In addition to hosting the replicated namespaces from other Content Platforms, a Content Platform can have its own outbound link to replicate some or all of its own namespaces to another Content Platform. This could possibly and quite commonly be in a two way replication scenario between a primary Content Platform and a replica Content Platform.

For full details on how replication works and is configured, refer to Replicating Tenants and Namespaces 1.

The discussion in this paper assumes the integration of each Content Platform into the corporate DNS system as stub zones. This paper uses following zone names, which you need to adapt for your naming policy:

- **Primary**—primary-hcp.domain.tld
- **Replica**—replica-hcp.domain.tld

---

This best practices guide is for system engineers, service and support personnel, and administrators of Symantec Enterprise Vault who use storage adapter in a replicated Content Platform environment. It documents a process that allows you to failover to a replicated Content Platform to continue normal read and write operations of Enterprise Vault. You should have knowledge of the following:

- Hitachi Content Platform 4 and 5, including replication methods
- Storage Adapter for Symantec Enterprise Vault
- Symantec Enterprise Vault
- Microsoft Windows DNS services
Background

Replication is an asynchronous process. On the primary system, new objects enter the replication queue for processing and transmission to the replica system on a first in, first out basis.

Entire objects are replicated. This includes the original file stored on the primary Content Platform and the metadata associated with that object. This includes any retention information associated with the object. Optionally, objects may be compressed or encrypted before being transmitted.

During normal conditions, the namespace on the replica Content Platform is available to applications for read only processing.

To support disaster recovery scenarios, the Content Platform administrator can failover the primary Content Platform to the replica Content Platform. When this happens, typically because the primary Content Platform is no longer available, the replica Content Platform takes on the role of primary for the replicated namespaces. These namespaces on the replica are now available for read and write operations.

When the primary Content Platform becomes available again, resynchronize the data from the replica to the primary. Upon completion of the synchronization, reverse the roles so that the primary Content Platform returns to read/write and the replica returns to read-only.

With the introduction of namespaces with Content Platform 3.0, the validation of the host name became part of the authentication process for all Content Platform namespaces, other than the default namespace. What this means is if a request for namespace.tenant.primary-hcp.domain.tld/rest/path/object was directed to namespace.tenant.replica-hcp.domain.tld/rest/path/object, the request would fail as the host name of the replica system does not match the host name specified in the URL.

The methods outlined in this paper discussing how to deal with failover and recovery for storage adapter in a replicated environment are valid for Content Platform 4 and Content Platform 5, as well DNS servers on Microsoft Windows 2003 and Microsoft Windows 2008.

Items that failed to replicate prior to the event triggering a disaster recovery scenario will not be marked as safe by Enterprise Vault until after the reestablishment of the primary Content Platform system and the ability of storage adapter to validate both the primary and the safety copy. This will also be true for copies that were successfully replicated but not yet confirmed as safe by Enterprise Vault. See *Administrator's Guide*\(^1\) for more information.

---

**Note**—Since the Content Platform replication process is asynchronous, an item written successfully to the primary Content Platform may not be written to the replica Content Platform at the time of failover. Attempts to retrieve an object not written to the replica server during failover results in an “item not found” error. Following resynchronization, this item becomes available again from the primary and replica Content Platform.
Types of Operation

These are descriptions of the types of operation.

Normal Operation

Storage Adapter for Symantec™ Enterprise Vault is one of several replica-aware applications dealing with Hitachi Content Platform. This means that storage platform knows that a replica exists and can perform certain functions automatically with respect to that replica.

Figure 1
Storage adapter must be installed on all Enterprise Vault servers that access Content Platform. When configuring storage adapter to define a vault store partition on an Enterprise Vault server, specify the following in the property sheet of the vault store partition:

- Namespace
- Tenant
- FQDN of the Content Platform primary host system
- FQDN of the Content Platform replica host system
- Number of safety copies on each system

Make the value for the number of safety copies equal to the value of the data protection level (DPL) of the namespace. The DPL level of the primary system does not necessarily equal that of the replication system.

Following the practices in this document, this is true for storage adapter:

- Two stub zones defined, each with its own set of IP values.
- The FQDN of the hostname of the primary system is primary-hcp.domain.tld.
- The FQDN of the hostname of the replica system is replica-hcp.domain.tld.

When properly configured and in normal operation, Enterprise Vault either reads or writes files to Content Platform. Storage adapter directs reads or writes to the primary Content Platform system (namespace.tenant.primary-hcp.domain.tld/rest/path/object). When Enterprise Vault asks if the previously written object is "safe," storage adapter makes a "head" call to the replica Content Platform asking if the object is present or not. If the object is present, a status of safe is returned, otherwise a status of unsafe is returned. Enterprise Vault repeats this process periodically for all unsafe objects until they are safe.

If there is a disruption in the operation of the primary Content Platform, then the read or write operation to the primary Content Platform will fail.

- If this was a write operation, no more processing by storage adapter occurs and returns a write failure status to Enterprise Vault.
- If this was a read operation, then storage adapter will retry the operation, attempting to read the object from the replica Content Platform. If the object was previously replicated by Content Platform, then the read operation to the replica will succeed and the object will be returned to Enterprise Vault.
Failover Operation

While this process of automated reads from the replica works fine for limited outages of the primary Hitachi Content Platform, more robust actions are often required for prolonged outages for the following:

- Allow for read and write actions to the replica Content Platform
- Restoration of all data to the primary Content Platform at a later time

Perform this process on all instances of storage adapter where read and write operations are desired.

**Note**—Initiation of failover processing typically takes place on the replica system. If you have implemented a Symantec Enterprise Vault environment using the building block approach, see the steps in the *Administrator’s Guide* section “Failover in a building blocks configuration.” This has the specific steps required for an Enterprise Vault environment prior or after to the following steps.

Upon detection of a primary Content Platform system failure, do the following.

   - This stops all I/O operations to storage partitions on the Enterprise Vault server.
2. Perform a failover operation for the failed link from the primary Content Platform to the replica Content Platform
   - This is usually performed from the replica Content Platform.
3. Modify the primary Content Platform entry on the property page of the vault store partition to point to the replica Content Platform by changing the following:
   - primary-hcp.domain.tld to replica-hcp.domain.tld
   - DPL value for the namespace
   - When finished, the primary Content Platform and the replica Content Platform entries are identical.
4. If necessary, make the number of safety copies for the primary Content Platform identical to the value currently specified for the replica Content Platform.
5. Save this configuration.

---

Failover Operation
All I/O operations from Enterprise Vault are directed exclusively to the replica Content Platform. Performing the failover operation to the replication link means write operations will succeed, also.

When Enterprise Vault asks if a written object is safe during failover, it always returns true. This is because storage adapter makes an enquiry against the replica Content Platform, which during failover is the same as the primary Content Platform.

Resume Normal Operations
This process must be repeated for each Symantec Enterprise Vault server running storage adapter.

When the primary Hitachi Content Platform becomes available again, do the following.

1. Initiate Begin Recovery on the link.
   At this point, Content Platform begins to resynchronize data written to the replica Content Platform to the primary Content Platform. During resynchronization, Enterprise Vault and storage vault continues to read and write from the replica Content Platform.
   - When the primary Content Platform and the replica Content Platform determine they are mostly caught up, the Complete Recovery button becomes available. Do not click this button yet.

2. Stop Enterprise Vault Storage Services.

3. Restore the values for the primary Content Platform to the original values (pre-failover values) on the property page of the vault store partition by changing the following:
   - replica-hcp.domain.tld to primary-hcp.domain.tld
   - DPL value for the namespace
   When finished, the primary Content Platform and the replica Content Platform entries are different.

4. Click Complete Recovery.


At this point, all the items written to the replica Content Platform during the interrupted service have been replicated to the primary Content Platform. These items remain on the replica.

After clicking Complete Recovery, I/O operations by Enterprise Vault (reads and writes) are directed to the primary Content Platform. Now objects are declared safe only when a copy exists on the primary Content Platform and the replica Content Platform.
Discussion of Failover for Applications Using Hitachi Content Platform 5 or Later

The vast majority of applications written for Hitachi Content Platform are not aware of the existence of a replica, or whether one is present.

While Content Platform 5.0 has methods to make this process automatically, you may prefer to control the disaster recovery process rather than it happening automatically without your knowledge.

For Content Platform 5 and later, one option is to modify the IP values in the DNS entry of the primary Content Platform stub zone to be identical to the IP values of the replica Content Platform.

When modifying the IP values in the DNS entry of the primary Content Platform while using Storage Adapter for Symantec™ Enterprise Vault, do the following:

- Stop Enterprise Vault Storage Services before doing this operation.
- After the operation, do the following:
  - Restart Enterprise Vault Storage Services.
  - Flushing the server DNS cache.
    - From a command prompt, type the following: `ipconfig /flushdns`

To modify the values in the DNS from your DNS server, do the following:

1. Right-click the stub zone entry from the primary Content Platform under Forward Looking Zone.
2. Click **Properties**.
3. From the properties dialog box, edit the server values (Figure 2 on page 10).
Figure 2

This process is specific to Content Platform 5.0 and later.

After this modification, you may need to do the following:

- Reload the stub zone on the DNS server
- Flush the DNS cache on the application servers
Discussion of Failover for Applications Using Hitachi Content Platform 4

For Hitachi Content Platform 4, this process is application specific. It involves a combination of the following:

- Perform the Content Platform failover operation
- Modify the mount points of the application to point to the replica Content Platform rather than the primary Content Platform.

For applications using the default namespace use the following approach, if the following is true:

- Implement the references to the primary Content Platform and replica Content Platform as stub zones and not as secondary.
  - DNAME records are not supported by the DNS on Windows 2003 nor Windows 2003 R2. Servers using Windows 2003 or Windows 2003 R2 will not properly resolve DNAME references.

**Note**—This process only works for mount references pointing to protocols using the default namespace, such as {nfs|cifs|www}.primary-hcp.domain.tld. This includes Content Platform 4 and Content Platform 5 systems. It will not work for DNS references using the REST notation, such as default.default.primary-hcp.domain.tld. It will not work with Enterprise Vault using storage adapter.

To prepare the environment for failover, do the following.

1. Create the following stub zones:
   - Primary-Content Platform stub zone
   - Replica-Content Platform stub zone
2. Create a DNAME record for the primary Content Platform server:
   - Tor hcp.domain.tld, created this DNAME record: primary-hcp.domain.tld
3. Change all mounts to reference the following:
   - **NFS**—nfs.hcp.customer.com
   - **CIFS**—cifs.hcp.customer.com"
When failover is required, do the following.

1. Quiesce or stop the application or applications.
2. Edit the DNAME reference to point to the replica Content Platform.
   - For hcp.domain.tld, change to this DNAME record: replica-hcp.domain.tld
3. Reload the zone in DNS.
4. Failover to the replica Content Platform.
5. Flush the DNS cache on the relevant application servers
   - Type this at a command prompt: ipconfig /flushdns
6. Restart the application or applications.
Summary

Replication using Hitachi Content Platform provides a valuable tool to provide data availability during a failover operation to provide read/write access for short term outages and longer outages.

Symantec Enterprise Vault and Storage Adapter for Symantec™ Enterprise Vault provide a robust environment to take full advantage of the replication capabilities of Content Platform.

- During short term outages, Enterprise Vault can continue to retrieve data automatically and transparently from the replica Content Platform.
- During longer term outages requiring the failover of the primary Content Platform to the replica Content Platform, Enterprise Vault operations can continue with minimal operational intervention and allow resumption of normal operations in a very straight forward manner.
Bibliography


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.
Corporate Headquarters
2845 Lafayette Street, Santa Clara, California 95050-2627 USA
www.HDS.com

Regional Contact Information
Americas: +1 408 970 1000 or info@HDS.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@HDS.com
Asia-Pacific: +852 3189 7900 or hds.marketing.apac@HDS.com

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

Notice: This document is for informational purposes only, and does not set forth any warranty, expressed or implied, concerning any equipment or service offered or to be offered by Hitachi Data Systems Corporation.
© Hitachi Data Systems Corporation 2012. All Rights Reserved. AS-178-00, October 2012