Abstract

IT administrators face many challenges with protecting the application and storage resources necessary for Epic, MEDITECH, and other healthcare operations. This white paper outlines how EMC® RecoverPoint provides cost-effective local and remote replication of healthcare environments.

April 2011
Copyright © 2011 EMC Corporation. All Rights Reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided “as is.” EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

VMware, ESX, and VMware vCenter are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other trademarks used herein are the property of their respective owners.

Part Number h8227
Table of Contents

Executive summary........................................................................................................4

Introduction ................................................................................................................5
  Audience...................................................................................................................5
  Overview..................................................................................................................5
  Protecting data with EMC RecoverPoint...............................................................6
  RecoverPoint remote replication.............................................................................7
  Concurrent local and remote data protection.........................................................9
  Write splitter support..............................................................................................9
  Point-in-time data recovery.....................................................................................10
  Guaranteed data consistency and write-order fidelity ............................................10
  Consistent write-order protection over long distances........................................10
  Read/write processing on replica volumes............................................................10
  Application integration capability..........................................................................11
  Integration with backup and archiving systems....................................................11

Protecting HCIS with RecoverPoint ...........................................................................11
  Application-consistent recovery from a shutdown (“cold” backup).....................12
  Crash-consistent recovery during operations (“hot” or “fuzzy” backup)..............12
  Application-consistent recovery during operation.................................................13

Using NetWorker with RecoverPoint ..........................................................................13

Using TimeFinder with RecoverPoint .........................................................................14

Using SnapView with RecoverPoint ..........................................................................15

Using array features with RecoverPoint ....................................................................15
  Performing operations on RecoverPoint production volumes...........................16
  Performing operations on RecoverPoint replica volumes....................................16

Protecting Microsoft Exchange or SQL Server with RecoverPoint............................16
  Intelligent replication and recovery options.........................................................17

Protecting VMware environments with RecoverPoint.................................................19
  VMware integration...............................................................................................20
  Using VMware vCenter Site Recovery Manager..................................................21

Conclusion ..................................................................................................................21

References ..................................................................................................................22
Executive summary

Epic makes software for midsize and large medical groups, hospitals, and integrated healthcare organizations – working with community hospitals, academic facilities, children’s organizations, safety net providers, and multihospital systems. The Epic software spans clinical, access, and revenue functions and extends into the home.

MEDITECH is a leading software vendor in the Health Care Information System (HCIS) industry. It offers a full range of software applications for today's healthcare facilities across two platforms, MAGIC OSAL and MAGIC CS.

EMC® RecoverPoint is a solution that healthcare organizations use to provide local and remote data protection for their Epic and MEDITECH solutions. RecoverPoint is also used by these same organizations to support other applications in their HCIS environment, including Microsoft Exchange and SQL Server and Oracle.

EMC RecoverPoint provides crash-consistent and application-consistent recovery points for use in a number of possible scenarios, enhancing the native availability within an Epic, MEDITECH, or other healthcare environment. EMC RecoverPoint provides full support for business continuity and disaster recovery when working with the Epic Caché database or MEDITECH Advanced Database in addition to applications such as Oracle, Microsoft Exchange or a SQL database, and others. RecoverPoint supports these solutions whether the underlying data is stored as raw disks or on a file system.

The EMC NetWorker® family of products protects data by simplifying and centralizing backup and recovery operations. NetWorker supports leading applications such as HCIS, Microsoft SQL Server, and SAP, and advanced backup/recovery technologies such as snapshot management and data deduplication. With this support, customers can realize the highest levels of flexibility, management, and cost control over their data protection operations, while protecting their overall investments in these technologies.

The EMC NetWorker Module for MEDITECH (NMMEDI) allows MEDITECH customers to utilize centralized backup and recovery management of their databases that reside on EMC storage arrays. It integrates with RecoverPoint’s point-in-time (PIT) copies for business continuity and disaster recovery. NMMEDI is integrated with MEDITECH by using MEDITECH’s Integrated Serverless Backup (ISB) API and EMC’s storage array APIs. NetWorker performs tape-based backups and uses RecoverPoint to create PIT copies that are used for disaster recovery. NMMEDI allows you to browse backups and reduces time for recovery.

Companies that use Bridgehead software can also use RecoverPoint’s PIT images. Bridgehead’s software supports MEDITECH by using MEDITECH’s ISB APIs and can be used with RecoverPoint’s PIT images to provide business continuity or disaster recovery for MEDITECH MAGIC data. Bridgehead’s software supports MAGIC OSAL and client/server platforms allowing organizations to meet their disaster recovery, business continuance, data protection, and compliance goals.
Introduction

This white paper describes and illustrates the key features, functions, and software capabilities of RecoverPoint. It also provides information about the NetWorker Module for MEDITECH, which provides effective backup and recovery of MEDITECH databases residing on EMC VNX™ series, CLARiiON®, and Symmetrix® storage arrays.

All products in the RecoverPoint family are appliance-based data protection solutions that ensure the integrity of production data at local and/or remote sites. These products enable customers to centralize and simplify their data protection management and allow for the recovery of data from nearly any point in time. The RecoverPoint features and functions are fully covered in the other EMC documents listed in References.

RecoverPoint provides block-level local and remote synchronous replication between LUNs in Symmetrix, VNX series, CLARiiON CX3 or CX4 series, Celerra® unified, or third-party storage arrays using continuous data protection (CDP) technology that tracks every write for later recovery to any point in time. RecoverPoint also provides remote asynchronous replication between block LUNs in two different sites using near-CDP technology that tracks groups of writes for later recovery to significant points in time. RecoverPoint uses policies that enable customers to map their recovery time objectives (RTO) and recovery point objectives (RPO) into RecoverPoint consistency groups, which allows flexibility in protecting multiple applications.

Concurrent local and remote (CLR) data protection is possible when RecoverPoint local and remote replication is used for the same LUNs. CLR provides simultaneous block-level local and remote replication for the same application LUNs. Recovery of one copy can occur without affecting the other copy.

Audience

The intended audiences of this white paper are healthcare organization management and business decision-makers, including storage, server, and database administrators, IT managers, application engineers, storage integrators, consultants, and distributors.

Overview

Backup and recovery are some of the most important aspects of HCIS administration. If a database crashed and you had no way to recover it, the devastating results to a hospital and their patients could include lost data, lost revenue, and even patient death. Whether hospitals operate a single application or multiple applications, they share one common factor — the need to back up important data and protect it from disaster by developing a business continuity and disaster recovery plan. Because of the long recovery gaps, tape-based backup and recovery are no longer an option for real-time data protection. Even disk-to-disk backup and traditional snapshot techniques are not acceptable for the critical nature of these HCIS applications.

RecoverPoint systems are made up of the following modular components:
• A RecoverPoint appliance (RPA) – This is a 1U server that runs the RecoverPoint software and includes four 4 Gb/s Fibre Channel (FC) connections and two 1 Gigabit Ethernet connections. For RecoverPoint local replication, two RPAs are installed in the production site. For RecoverPoint remote or local and remote configurations four RPAs are installed, two in the production site and two in the remote site.

• RecoverPoint software – This software is installed on the RPA by EMC or an EMC Velocity Authorized Service Network partner and controls all of the local and remote replication and recovery processes.

• RecoverPoint Deployment Manager – This software is a graphical user interface wizard used to install the RecoverPoint software from a single management point. Once the Deployment Manager installation is complete, you are able to start building a replication configuration.

• RecoverPoint enabler for the VNX series, CLARiiON CX3, and CX4 array-based write splitter – The write-splitting software is free and is already installed in the VNX series and CX4 arrays. It is also available as a patch upgrade to FLARE® 03.26 or FLARE 04.28 software. An EMC customer engineer or certified partner will install the patch upgrade (if required) and the RecoverPoint enabler onto a VNX series, CLARiiON CX3, or CX4.

• RecoverPoint host agent software – This software includes agents that are integrated with Microsoft Exchange Server and Microsoft SQL Server and also includes other host utilities that are used when creating scripts to automate the RecoverPoint data protection and recovery process.

• RecoverPoint Storage Replication Adapter for VMware® Site Recovery Manager – This software is downloaded from the VMware website and enables the integration of RecoverPoint with VMware Site Recovery Manager.

• EMC licensing – Licensing controls the RecoverPoint configurations, features, and functions. RecoverPoint/SE systems can be upgraded to equivalent RecoverPoint systems without the loss of configuration or replication data.

Protecting data with EMC RecoverPoint

EMC RecoverPoint is a comprehensive replication and data protection solution designed and built from scalable and highly available hardware appliances and software modules. As shown in Figure 1, RecoverPoint provides continuous remote replication, continuous data protection, and concurrent local and remote data protection for block-based SAN volumes residing in an EMC Symmetrix, VNX series, CLARiiON CX3 or CX4, Celerra unified, or third-party storage array. When array-based write splitters are used, RecoverPoint also supports iSCSI volumes for local and remote replication. In the event of a local data corruption or a regional disaster, customers can, depending on the nature of the crisis, recover data at either the local or remote site.
RecoverPoint local replication protects volumes residing in one or more storage arrays by synchronously replicating the production volume to a local copy, as well as tracking all data changes to a local journal volume. RecoverPoint synchronously replicates FC SAN volumes and can be configured to replicate production volumes regardless of the storage model used. RecoverPoint is ideal for application or operational recovery and protects critical data from physical or logical failures such as server outages, data corruption, software errors, viruses, and common user errors. Advanced data reduction technologies for the journal volume and a DVR-like any-point-in-time recovery make this solution superior to traditional data mirroring and snapshot techniques previously used to provide this sort of protection.

RecoverPoint remote replication
RecoverPoint provides remote replication between volumes in two CLARiiON arrays in two sites as shown in Figure 2. RecoverPoint enables protection from site disasters and provides volume recovery to significant or application-consistent points in time with no data loss. RecoverPoint provides bidirectional replication with no distance limitation, guaranteed data consistency, and advanced bandwidth reduction technology, which reduces the IP network bandwidth used for replication. Application integration, intelligent bookmarks, and data change journaling enable customers to support RTO service-level agreements measured in seconds or minutes instead of hours or days.
WAN telecom costs continue to present significant financial challenges to customers looking to replicate data remotely. EMC RecoverPoint is a leading replication solution due to its integrated WAN bandwidth reduction and compression that provide solid cost savings through reduced bandwidth requirements. To further enhance this capability, EMC recently added support for deduplication of data sent over a WAN to RecoverPoint. Working with its other intelligent data compression and bandwidth reduction technologies, RecoverPoint customers can now see up to a 90 percent reduction in total WAN bandwidth.

RecoverPoint uses unique intelligent bandwidth reduction technologies that minimize bandwidth requirements. This enables the system to provide the best possible level of protection for the available bandwidth, while dramatically reducing WAN costs, particularly over long distances. Transmission size is reduced by using data deduplication, data compression, and network-aware algorithmic techniques to conserve bandwidth, which was not possible with traditional technologies.

The WAN deduplication process requires that the local and remote RecoverPoint clusters all use Generation 4 (GEN4) RecoverPoint appliances. If the clusters are not homogeneous GEN4 appliances, then the deduplication option is not provided. You can enable deduplication on a consistency group basis using the RecoverPoint Administrative GUI or the RecoverPoint command line interface. Deduplication operates on the data replicated between sites across the WAN. If data deduplication is enabled, then during replication, RecoverPoint creates a fingerprint for each 512-byte block of data. If the fingerprint does not exist at the remote site, then RecoverPoint transfers the data and stores the fingerprint. If the fingerprint does exist, then it does not send the data to the remote site.
**RecoverPoint/Cluster Enabler**

EMC RecoverPoint/Cluster Enabler (RecoverPoint/CE) is software that enables geographically dispersed Microsoft Failover Clusters to replicate their data using RecoverPoint. Geographically dispersed clusters offer increased levels of high availability, disaster recovery, and automation over those solutions that are not clustered. RecoverPoint/CE works seamlessly with applications designed to take advantage of Failover Clusters, such as SharePoint, Exchange, and SQL Server, in Microsoft Windows 2003 and 2008 environments.

The topology in Figure 3 shows RecoverPoint/CE configured with a file share witness. A file share witness provides a tiebreaker in an even-node Microsoft cluster configuration. Microsoft Failover Clusters ensure that a single point of failure does not impact the application by moving it to a different node. RecoverPoint/CE ensures that the data that RecoverPoint remotely replicates is available to all nodes in the cluster.

![RecoverPoint/CE topology](image)

**Figure 3. RecoverPoint/CE topology**

**Concurrent local and remote data protection**

Some customers need to protect their application data locally from data corruption, as well as remotely from a local or regional disaster. These customers can implement both local and remote replication for the same data volume. RecoverPoint protects the volume locally by replicating all changes to a copy in a local storage array; it also protects the volume remotely by replicating significant changes to a copy in a remote storage array. Recovery and use of the local and remote copies can be performed independent of each other and without affecting the ongoing local and remote replication of the production data.

**Write splitter support**

RecoverPoint replicates data by using intelligent write-splitting modules to intercept the application writes. The RecoverPoint write-splitting module resides in a VNX
The VNX array-based splitter is part of the VNX Operating Environment and the CLARiiON array-based splitter is part of the FLARE Operating Environment. The VNX and CLARiiON array-based write splitter runs in each storage processor and can access volumes from either storage processor.

All array-based write splitters split (that is, mirror) all writes to a SAN or iSCSI volume, sending one copy to the original target and the other copy to the RecoverPoint appliance. The array-based write splitter supports all FC SAN and iSCSI SAN LUNs on the VNX series, CLARiiON CX3 and CX4 series, and Celerra unified arrays. The array-based RecoverPoint splitter also supports all operating systems that are qualified for attachment to the VNX series, CLARiiON CX3 and CX4, and Celerra unified arrays.

**Point-in-time data recovery**

RecoverPoint stores changed data and time together in a journal volume, enabling immediate recovery to any point in time for local copy volumes, and to significant points in time for remote copy volumes. RecoverPoint can recover applications quickly to a selected time or event with guaranteed write-order consistency, even when data spans multiple heterogeneous storage and servers. For local copy volumes, RecoverPoint retains every change in a local history journal for later recovery. For remote asynchronous replication, RecoverPoint supports multiple transactional-consistent snapshots at the remote site, allowing reliable recovery in database environments. It uses frequent snapshots taken seconds apart to minimize the risk of data loss due to data corruption.

**Guaranteed data consistency and write-order fidelity**

RecoverPoint guarantees a consistent replica of business-critical data in the event of most potential failures or disaster scenarios. Many products available today cannot ensure consistency through rolling disasters or during resynchronization. With RecoverPoint, consistency is maintained at all times, even for data spanning multiple heterogeneous storage systems and servers.

**Consistent write-order protection over long distances**

RecoverPoint achieves write-order consistency for remotely replicated data by tagging each replicated write, and then reassembling the writes into the correct order at the remote site. This enables RecoverPoint to provide synchronous levels of protection with little to no application degradation and no distance limitations. This unique capability shatters today’s distance/latency limitations, and enables complete up-to-date protection from regional disasters with no impact on application performance.

**Read/write processing on replica volumes**

RecoverPoint enables direct read/write access to data on the replica volumes without the need to first make an additional copy or without halting data protection. The system supports robust failover and failback capabilities, reducing management and operational costs. Data volumes at the selected point in time are instantly available
upon request, with full read/write capability. Using these data volumes, the customer can offload their backups or perform live application testing, on-demand recovery, data migration, and many other valuable data processing applications.

**Application integration capability**

The RecoverPoint scripting interface enables business applications to integrate RecoverPoint into existing application protection and recovery processes, dramatically reducing recovery time and eliminating potential data loss. You can create RecoverPoint scripts which create application-specific bookmarks to represent transaction and event boundaries. Without these bookmarks, the application must perform “crash-recovery” on the image, which increases the RTO, and may result in some data loss. When you use these bookmarks to select the recovery image you ensure that the application can be restarted from an application-consistent point-in-time image, minimizing RTO and data loss.

RecoverPoint also ships with application agents for Microsoft Exchange Server and Microsoft SQL Server. These agents use the Microsoft Volume Shadow Copy Services (VSS) and Virtual Device Interface (VDI) APIs to ensure the applications are in a consistent state before creating an application bookmark. Selecting a recovery image that uses one of these bookmarks facilitates easy recovery with minimal RTO and no data loss. Additionally, many customers use EMC Replication Manager software. This software is integrated with RecoverPoint and delivers point-and-click replica management for instant restoration to production by creating a “gold copy” of production data for an instant restoration should a corruption occur.

**Integration with backup and archiving systems**

RecoverPoint is qualified with MEDITECH and is integrated with EMC NetWorker through the NetWorker Module for MEDITECH (NMMEDI), which uses RecoverPoint to provide enhanced backup and recovery for various MEDITECH solutions.

Additionally, RecoverPoint has been qualified to support Epic Caché configurations and for general protection of Epic solutions. Finally, many customers use RecoverPoint to protect their third-party HCIS solutions locally for business continuity and/or remotely for disaster recovery.

**Protecting HCIS with RecoverPoint**

RecoverPoint includes continuous protection. This means that it eliminates HCIS protection gaps, facilitates compliance to guidelines and the regulatory requirement, and considerably simplifies the HCIS data protection lifecycle. Furthermore, with RecoverPoint, you no longer need windows for your backup, since RecoverPoint can protect the data locally and remotely without impact to production HCIS servers. For example, you can use a RecoverPoint point-in-time image, either at the local site or at the remote site, as the source for a backup operation. This backup can be performed without having to freeze or shut down the HCIS solution, which provides concurrent backup and processing.
Many HCIS customers run relational database configurations such as Oracle. Many relational databases provide several options for protecting their databases and many of these options can be integrated with RecoverPoint replication. If a database is shut down normally, using RecoverPoint to protect the database provides an application-consistent image of the database. If the database terminates abnormally, using RecoverPoint to protect the database provides a crash-consistent image of the database. Restarting from an application-consistent image is fairly quick, however, restarting from a crash-consistent image will take longer, depending on the number and size of transactions that were in process at the time of termination. A RecoverPoint disaster recovery image that is not application-consistent is similar to an abnormally terminated database.

The database restart procedure transforms image into a transactional consistent image by completing committed transactions and rolling back uncommitted transactions during database initialization. Using RecoverPoint, the user creates a consistency group whose replication sets contain all volumes associated with their HCIS application and then processes the consistency group based on the type of recovery required.

**Application-consistent recovery from a shutdown (“cold” backup)**

A consistency group that represents the HCIS application running on a relational database instance contains all volumes for the application, including data files, online redo log files, and configuration files. Optionally, it can include control files as well. Since the application is shut down, this method produces a copy from which you can restore the database, if necessary, with 100 percent reliability. With this method you must halt normal operations while this “cold” backup is created, so this method is not appropriate for systems that must operate on a 24×7 basis, including HCIS applications. In addition, any changes to the database made before or after the “cold” backup will not be available as an application-consistent recovery point, but will be a crash-consistent recovery point.

When the relational database is shut down, the user then creates a RecoverPoint bookmark for the specific consistency group to identify the image as a “cold” backup image. This bookmark identifies a point-in-time recovery image that represents a fully restorable and restartable HCIS image.

**Crash-consistent recovery during operations (“hot” or “fuzzy” backup)**

A crash-consistent process enables the creation of crash-consistent images without requiring a shutdown of the HCIS system or relational database. RecoverPoint performs this process by default for all applications as part of the RecoverPoint write-splitting operations. As HCIS writes are sent to the production volumes, RecoverPoint splitters also intercept them and send copies to the RecoverPoint appliance for further processing. These writes represent the on-disk consistent data, which is the same data that remains on external storage even when an application crashes. When the HCIS applications are restarted from a server crash, the HCIS application needs to error check its data and log volumes before completing the restart process. When the
HCIS applications are restarted from a RecoverPoint crash-consistent image, the HCIS applications will perform the same error-checking process.

**Application-consistent recovery during operation**

The application-consistent recovery process enables the creation of application-consistent images without requiring system shutdown. All data files must belong to the relevant tablespaces, and the relevant archive log files and control files must be flushed from the server’s in-memory buffers to disk. To ensure your HCIS application can recover from these images, the HCIS application must write additional state information. This writing may have an adverse impact on system performance, and may limit how frequently application-consistent images are created.

Using this feature with RecoverPoint requires that the user script several commands to both the HCIS application environment, such as Oracle, and to the RecoverPoint appliance. By using scripting, the user first freezes the HCIS application; for example, if the HCIS uses Oracle, use the script ALTER TABLESPACE BEGIN BACKUP or ALTER DATABASE BEGIN BACKUP. The HCIS application must update its LOG files to indicate that the HCIS application is frozen and it must also ensure that the appropriate in-memory buffers are flushed to disk. Once the HCIS application is frozen, the script creates a RecoverPoint bookmark for the specific consistency group to identify the image as an HCIS application-consistent image. You can use this bookmark to recover the HCIS applications to a specific point in time and restart the HCIS applications for operations. Finally, the HCIS applications thaw, which then allows other processing to occur. For HCIS applications using Oracle, this process is documented in the Reference section below.

**Using NetWorker with RecoverPoint**

The EMC NetWorker Module for MEDITECH (NMMEDI) allows MEDITECH customers to use RecoverPoint to protect and recover their MEDITECH databases with point-in-time (PIT) copies for disaster recovery. NMMEDI uses the MEDITECH Integrated Serverless Backup (ISB) API and EMC RecoverPoint APIs to replicate and create PIT copies for disaster recovery. NMMEDI allows you to browse backups and reduces time for recovery.

EMC NetWorker Module for MEDITECH provides SAN-based backup and recovery of MEDITECH databases that are located on EMC Symmetrix and EMC CLARiiON storage arrays. When used with RecoverPoint, NMMEDI works with all EMC and third-party storage arrays that RecoverPoint supports to protect all of the MEDITECH data, as well as all of the customer’s data.
Figure 4. NM MEDI and RecoverPoint topology

Figure 4 shows a combined RecoverPoint and NM MEDI configuration. NM MEDI uses MEDITECH-provided ISB APIs to:

- Communicate with MEDITECH OSAL and MEDITECH CS environments
- Freeze the MEDITECH databases in preparation for a RecoverPoint bookmark
- Thaw the MEDITECH databases and return them to standard operation

NM MEDI uses RecoverPoint APIs to:

- Communicate with RecoverPoint to ensure that MEDITECH databases reside on volumes that EMC RecoverPoint protects
- Create RecoverPoint bookmarks that identify points in time when RecoverPoint replicated MEDITECH databases

NM MEDI uses NetWorker to schedule and manage the protection of MEDITECH databases. NM MEDI writes backup metadata to the NetWorker server, which restores and browses the replicas that RecoverPoint created.

Using TimeFinder with RecoverPoint

The EMC TimeFinder® family of software provides a local copy of EMC Symmetrix VMAX™ data, independent of the host and operating system, application, and database. VMAX can also provide an array-based full or space-saving differential volume copy by using TimeFinder/Clone or TimeFinder/Snap. RecoverPoint production or local or remote replica volumes can be the source for a TimeFinder operation. The next section contains more information about TimeFinder products. Typical applications for using TimeFinder with RecoverPoint would be data warehousing or other applications that require a full-volume, independent host-addressable, local point-in-time copy of a VMAX production device. For example, you
can use RecoverPoint to replicate SharePoint remotely and then use TimeFinder at the remote site to create a fully writeable replica for use in an SQL Server database. RecoverPoint’s continuous local and remote data protection with DVR-like rollback capabilities are very complementary to TimeFinder.

**EMC TimeFinder products**

- **TimeFinder/Clone**: Creates a functional, full-volume, independent host-addressable, local point-in-time copy of a VMAX production device and allows up to 16 active clones of a single production device, all of which are immediately available for both read and write access and can use RAID 5 and/or RAID 6 protection schemes.

- **TimeFinder/Snap**: Creates a space-saving replica as compared to the TimeFinder/Clone operation. This operation creates a replica by generating pointers back to the source. No synchronization, copy, or additional storage utilization occurs unless a write occurs on the target copy.

- **TimeFinder/Consistency Groups**: Ensures dependent-write consistency of the application data when it creates a point-in-time image across multiple devices associated with an application within a single VMAX array or with applications that also span multiple VMAX storage arrays.

- **TimeFinder/Exchange Integration Module and TimeFinder SQL Integration Module**: Integrates the TimeFinder family with Microsoft Exchange and SQL applications for automated backup and restore.

**Using SnapView with RecoverPoint**

The VNX series and CLARiiON CX3 and CX4 series also provide array-based full or differential volume copies using SnapView™ software. RecoverPoint production or replica volumes can be the source for VNX series or CLARiiON array snapshot operations, as long as you follow the caveats in the section [Performing operations on RecoverPoint production volumes](#). In addition, the RecoverPoint local and/or remote replica copies can be the source for array-based clones or snapshots that SnapView creates. Typical applications for using SnapView clones with RecoverPoint would be data warehousing or other applications that require a full, fractured replica. For example, use RecoverPoint to replicate an Oracle database remotely and then use SnapView at the remote site to create a fully writeable replica for use in an SQL Server database. RecoverPoint’s continuous local and remote data protection with DVR-like recovery capabilities are complementary to array-based snapshot and replication facilities.

**Using array features with RecoverPoint**

TimeFinder and SnapView coexist with RecoverPoint and can use the same production volumes as long as only one product is active at a single time. The following two examples show how to use these products on the RecoverPoint production and replica volumes.
Performing operations on RecoverPoint production volumes

There are many ways that RecoverPoint can be combined with native array capabilities. A common request from customers is to combine array-based snapshots with remote replication using RecoverPoint. For example, the production volumes for an Oracle application can be protected locally using TimeFinder and replicated using RecoverPoint. The RecoverPoint splitter will intercept all writes by the Oracle application to the protected volumes and sends a copy to the RecoverPoint appliance. Additionally, TimeFinder intercepts the write and uses it to maintain the replica as required.

If the production volume needs to be resynchronized, the user must disable the specific RecoverPoint consistency group that contains the affected volumes before recreating those volumes. For example, if TimeFinder needs to resynchronize the Oracle production volume, the user must disable the specific RecoverPoint consistency group that contains the affected volumes before recreating those volumes. When this is completed and TimeFinder resumes normal operations the user enables the RecoverPoint consistency group. At this point RecoverPoint will perform a full sweep of its production and replica copies to synchronize the RecoverPoint replica with the production volume.

Performing operations on RecoverPoint replica volumes

RecoverPoint supports the use of TimeFinder and SnapView on local and remote replica copies. To use one of these layered array operations, access the point-in-time image as a physical volume hosted by the appropriate array. You accomplish this by selecting enable image access for the specific consistency group copy that contains the selected volumes. Then perform a DVR-like recovery by selecting an appropriate point-in-time image or consistent bookmark from the RecoverPoint journal and requesting logged access as the image access mode. This causes RecoverPoint to recreate the physical volumes as they existed at the requested point in time.

Once the RecoverPoint volume is rolled back to the point in time and is visible in the SAN, TimeFinder or SnapView can create a copy of this volume. Once the volume copy is created, the RecoverPoint image is no longer needed. At this point the user selects disable image access for the consistency group copy, which causes RecoverPoint to resynchronize its replica copies. These volume copies can now be used for any purpose without any impact to RecoverPoint. If these volume copies need to be resynchronized, repeat the image access steps, selecting a different point-in-time copy. Once the RecoverPoint image is available, resynchronize the copy from the RecoverPoint image and continue with the processing.

Protecting Microsoft Exchange or SQL Server with RecoverPoint

Because many healthcare systems use industry-standard products for database and collaboration capabilities, it is important to consider these applications when developing your overall HCIS disaster recovery strategy. EMC RecoverPoint provides full-featured local operational recovery and remote disaster recovery solutions for all applications, including Microsoft Exchange Server and SQL Server. RecoverPoint's
innovative technology supports flexible levels of protection, without distance limitations or performance degradation. Local protection synchronously mirrors the data between groups of local volumes while remote protection replicates the data between groups of volumes in two different sites.

RecoverPoint provides continuous, crash-consistent protection for multiple physical and virtualized applications such as Exchange and SQL Server. RecoverPoint supports applications that run on multiple hosts as well as applications that have data residing different arrays. RecoverPoint has the ability to roll back the target volumes for all applications to the same point in time.

Additionally, RecoverPoint offers advanced integration capabilities for data protection, including support of the Microsoft VSS framework for Exchange and support of the VDI API for SQL Server. These APIs provide maximum reliability and performance, and support the full range of Exchange Server and SQL Server backup and restore functionality, including the full range of hot and snapshot backup capabilities.

To support a highly scalable, highly available server configuration, administrators must implement a highly available storage infrastructure. By using RecoverPoint, server administrators can improve the data recovery and availability of their application servers (either physical or virtual) while improving their recovery point objective (RPO) and recovery time objective (RTO). With its unique architecture, powerful data recovery features, and business-driven approach, RecoverPoint offers advanced levels of data protection and enables business continuity to organizations running Microsoft Exchange and/or Microsoft SQL applications.

**Intelligent replication and recovery options**

RecoverPoint recovers the target volumes to recover a specific point in time. RecoverPoint can undo individual write operations, and can recover images that may be fractions of a second apart. RecoverPoint remote replication supports a feature called dynamic synchronous replication where RecoverPoint will automatically toggle between synchronous replication and asynchronous replication according to user-defined thresholds. Asynchronous replication is performed over the customer’s existing IP infrastructure or Fibre Channel network and benefits from intelligent data compression and IP-bandwidth optimization. Synchronous replication is performed over the customer’s existing Fibre Channel network. Additionally the source and target arrays do not need to be identical, or even on the same storage array. This allows you to use different storage arrays or storage tiers between locations. It also simplifies the resource requirements necessary when performing DR fire drills.

**Application-aware bookmarks improve recovery options**

EMC RecoverPoint offers seamless integration with business applications that facilitate intelligent protection and recovery. Application, environmental, and user bookmarks are created by RecoverPoint during the replication process. These bookmarks are used during recovery to dramatically reduce the application recovery time and to eliminate data loss.
Using VSS, RecoverPoint puts Exchange Server briefly into a quiescent state, committing in-memory transactions and then halting all I/O to the storage groups and log files, so that it can create a bookmark to this consistent state. A recovery using this bookmark ensures that Exchange Server can restart without going through any Exchange Server crash-recovery processing. This dramatically improves the recovery time and enables a quick return to production.

Using the VDI APIs, RecoverPoint puts SQL Server briefly into a quiescent state, which commits in-memory transactions and then halts all writes to the database and log files. This allows RecoverPoint to create a bookmark that records this image as an application-consistent VDI image. RecoverPoint also protects the metadata information that the VDI API provides, which can be used later when restoring the SQL Server database.

The built-in crash recovery mechanism of these two applications allows them to recover from a power outage, hardware crash, or software crash. During crash recovery, Exchange and SQL Server recover all completed transactions while removing all incomplete transactions, thereby maintaining transactional consistency. As a result, crash recovery allows Exchange and SQL Server to recover from a point-in-time image.

Most relational applications manage one or more user databases. Additionally, special system volumes contain additional systems configuration information. A database is composed of multiple files such as data files and log files. These files usually reside on several different volumes, all of which must be protected and restored as a single group. When a database or special volume is added to an application, the user must update the freeze/thaw scripts. To eliminate the need for freeze/thaw scripts, EMC Replication Manager integrates with RecoverPoint and supports Microsoft Exchange, SQL, SharePoint, and Oracle for backup and recovery from local and remote replicas created by RecoverPoint.

**Instant recovery**

Continuous data protection gives administrators significant flexibility for application recovery. An application image that RecoverPoint protects can be instantly recovered from any point in time and mounted in read/write mode on a recovery server. The recovered image can be used for any purpose, such as single object recovery or full application recovery. Application-aware bookmarks, such as the VSS bookmarks mentioned previously, give the administrator the flexibility to select the most appropriate image for recovery processing.

In the event of a server failure, a standby server can quickly mount the most current image for operational recovery from server failure. Alternatively, a standby server, for such uses as individual object recovery, can recover the entire application from the RecoverPoint CDP image.

**Recovery from array and complete site failure**

With RecoverPoint, every write that an HCIS application makes to the local storage subsystem is intercepted and copied in parallel to the local RecoverPoint appliance.
In the event of an array or site failure, the appliance flushes its buffer to the secondary site, preserving the write order. The RecoverPoint Management Application GUI allows you to bring up a consistent replica image for Exchange recovery processing, which enables quick recovery from the array and/or complete recovery from a site failure.

**Protection from data corruption**

RecoverPoint efficiently maintains a transactional-consistent snapshot history at the remote site, allowing convenient rollback to any point in time and enabling quick recovery. This continuous protection eliminates the backup window and the data-loss vulnerability inherent in traditional backup and snapshot systems. RecoverPoint supports multiple volumes in any application configuration. Each single write to the application is replicated, preserving the write order. Using the time-stamped and application-aware bookmarks, the administrator can recover the appropriate image just prior to the data corruption. This gives the administrator a powerful tool that minimizes the data loss and data recreation necessary to recover from data corruption.

**Protecting VMware environments with RecoverPoint**

RecoverPoint provides a full-featured local and remote replication solution for VMware ESX®. For local and remote synchronous replication every write is captured and stored in the RecoverPoint journal. For remote asynchronous replication, the user specifies RPO policies for the replication that controls the time between replicated images to ensure that specific RPOs are met for each consistency group. Additionally, the user can specify synchronous remote replication or dynamic synchronous replication. Using dynamic synchronous replication, RecoverPoint will automatically switch between synchronous and asynchronous replication based on latency and throughput policies. For both local and remote replication, RecoverPoint guarantees recovery of VMware guest operating systems with minimal to no data loss by using point-in-time crash-consistent images.

RecoverPoint supports SAN-attached volumes when replicating VMware virtual machines. It supports both Raw Device Mapping (RDM) and VMware ESX File System (VMFS) volumes for replication. Additionally, if VMware ESX Server is configured for Boot from SAN (BFS), then RecoverPoint can also replicate the BFS volumes to the remote site. RecoverPoint captures changes to data by intercepting every write (either to an RDM volume or to a VMFS volume) that reaches the SAN through the array-based write splitters.

To ensure that the crash-consistent images are recorded for each virtual machine, EMC recommends that you create a RecoverPoint bookmark while VMware ESX Server is in a quiesced state. To ensure crash-consistent data capture, you must first power off all guest virtual machines that reside on replication LUNs or VMFS volumes. Once the virtual machines are powered off, create a RecoverPoint bookmark for the appropriate consistency groups using either the RecoverPoint GUI or CLI. Alternatively, you can use the VMware Tools SYNC driver (LGTO_SYNC) to flush...
pending writes to a VMFS before creating the bookmark.¹ Most of today’s applications and databases have a built-in resiliency that allows them to deal with crash-consistent images without the need to flush pending writes or shut down virtual machines.

RecoverPoint’s image access technology allows administrators to access any image in seconds and to mount it directly as either a VMFS volume or as a RDM volume. Once you have mounted the image, you can repurpose it for backup, DR testing, or immediate recovery of files, folders, volumes, or entire virtual machines. When using RecoverPoint to replicate a virtual machine’s data, there is no awareness of the virtual infrastructure at the destination site.

You must script a process to scan for and register virtual machines on the replicated volumes, or you must manually configure each virtual machine on the destination side. The target virtual machines are in a powered-off or cold state, until they are used. EMC implemented a VMware Storage Replication Adapter for RecoverPoint, which enables VMware vCenter™ to use RecoverPoint as an external replication provider for VMware vCenter Site Recovery Manager. VMware vCenter Site Recovery Manager automates the scanning and registration process of the replicated volumes for the virtual machines and their data as part of the disaster recovery failover process.

**VMware integration**

In the RecoverPoint Management Application GUI, you can view ESX servers and all their virtual machines, data stores, and RDM drives. This view also displays the replication status of each volume.

You can see each vCenter that RecoverPoint monitors. Under each vCenter object you can see data extracted from VMware vCenter, including its site name and username, its IP address, and the RecoverPoint replication state for each virtual machine that vCenter manages. The following information is displayed for an individual vCenter:

- Each ESX server in the vCenter and its IP address
- Each virtual machine configured and powered by ESX Server
- The replication status of each virtual machine, that is, if the VM is fully configured for replication, partially configured for replication, or not configured for replication
- The primary IP address of each virtual machine
- The replication status of each LUN and raw device attached to each virtual machine, that is, if the volume is configured for replication or not configured for replication
- If RecoverPoint has configured the volume for replication, then the RecoverPoint Management Application GUI displays the RecoverPoint consistency group, copy

¹ While it is possible to use the SYNC driver, a description of this procedure is beyond the scope of this paper.
type (production, local, or remote), replication set that contains the LUN, and the ESX datastore contains the LUN

Using VMware vCenter Site Recovery Manager

VMware vCenter Site Recovery Manager accelerates and ensures successful VM and VM data recovery by automating the recovery process and eliminating the complexity of managing and testing recovery plans. Site Recovery Manager eliminates complex manual recovery steps and removes the risk and worry from disaster recovery. It uses its knowledge about the virtualized infrastructure and uses an external replication solution (such as EMC RecoverPoint) to provide disaster recovery management and automation for the virtual data center.

![Diagram of VMware vCenter Site Recovery Manager](image)

Figure 5. VMware vCenter Site Recovery Manager at a glance

VMware vCenter Site Recovery Manager makes disaster recovery rapid, reliable, manageable, and affordable. As is shown in Figure 5, Site Recovery Manager leverages VMware infrastructure and external storage replication software to deliver centralized management of recovery plans, automate the recovery process, and enable dramatically improved testing of recovery plans. It turns the complex processes associated with traditional disaster recovery into an integrated element of virtual infrastructure management. Site Recovery Manager enables organizations to take risk and worry out of disaster recovery, another reason that the VMware virtualization platform is the safest platform for data center applications.

Conclusion

EMC RecoverPoint offers continuous data protection, continuous remote replication, and concurrent local and remote data protection. With its customer-defined RPOs and RTOs, RecoverPoint allows critical business processes to be available locally for operational recovery, or remotely at a disaster recovery site hundreds or thousands of miles away from the primary site. With support for consistency groups, RecoverPoint is a no-data-loss model with full write-order consistency for replicated volumes that can span multiple heterogeneous storage systems and servers.
References

More information on EMC RecoverPoint can be found at the RecoverPoint page on EMC.com and in the following documents on the EMC Powerlink® website:

- Introduction to EMC RecoverPoint 3.4: New Features and Functions — Applied Technology white paper
- Improving Microsoft Exchange Server Recovery with EMC RecoverPoint — Applied Technology
- EMC RecoverPoint Family Overview — A Detailed Review white paper
- Improving VMware Disaster Recovery with EMC RecoverPoint — Applied Technology
- Solving Data Protection Challenges with EMC RecoverPoint — Best Practices Planning
- Using EMC RecoverPoint Concurrent Local and Remote for Operational and Disaster Recovery — Applied Technology white paper
- Enhancing Oracle Database Protection with EMC RecoverPoint — Applied Technology
- Replicating Oracle with EMC RecoverPoint Technical Notes (Powerlink only)
- The EMC NetWorker Module for MEDITECH Backup Solution for MEDITECH Databases on EMC Symmetrix and EMC CLARiiON — Applied Technology