White Paper

Improving VMware Disaster Recovery with EMC RecoverPoint

Applied Technology

Abstract

EMC® RecoverPoint provides full support for data replication and disaster recovery for VMware ESX Servers and their virtual machine clients. This white paper describes how RecoverPoint can be utilized to provide local and remote data protection and recovery for VMware ESX environments. It also covers the supported configurations available for VMware ESX Server and ESX virtual machine environments and the integration of RecoverPoint with VMware Site Recovery Manager.

May 2008

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.

Part Number H2352.1

Table of Contents

Executive summary

EMC® RecoverPoint is an advanced enterprise-class disaster recovery solution supporting heterogeneous storage and server environments. RecoverPoint provides bi-directional local and remote data replication across any distance, and utilizes continuous data protection technologies to provide consistent point-in-time recovery. RecoverPoint helps customers accelerate operational and disaster protection of their VMware™ Infrastructure, without impacting production environments. RecoverPoint is ideally suited for replicating and protecting virtual server environments.

Introduction

Server virtualization technology allows one physical server platform to run multiple virtual machines simultaneously. Many customers have taken advantage of server virtualization, such as that provided by the VMware ESX Server, to consolidate their server infrastructure and simplify their disaster recovery platforms. These customers have also invested in enterprise-class SAN switches, such as the EMC Connectrix® ED48000B and MDS 9000 directory family, along with a SAN-based storage infrastructure, which support their primary data center and disaster recovery sites. This leads to some challenges when it comes to managing data protection for their local and remote data centers, especially for applications running on a virtual machine in an ESX Server.

This white paper describes how customers can utilize RecoverPoint to enhance the disaster recovery and data protection capabilities of their VMware servers with local and remote replication.

Audience

This white paper is targeted to storage and server administrators, IT managers, and storage professionals, as well as integrators, consultants, and distributors.

Overview

EMC RecoverPoint is an advanced enterprise-class disaster recovery solution supporting heterogeneous storage and server environments. RecoverPoint provides bi-directional data replication across any distance, as well as local continuous data protection.

RecoverPoint provides a full-featured replication and continuous data protection solution for VMware ESX Servers. For remote replication, it utilizes small-aperture snapshots to protect the VMware ESX platform from data corruption and guarantees recoverability with minimum data loss. For local protection, it utilizes continuous data protection to preserve every write, allowing data recovery to any point in time.

EMC RecoverPoint

RecoverPoint is an out-of-band appliance-based product, designed with the performance, reliability, and supportability required for enterprise applications. Running on a cluster of tightly coupled servers, RecoverPoint's high-availability design ensures that the failure of a single appliance will not affect the data protection of the VMware ESX Server. RecoverPoint utilizes write splitters that reside on the host, in the fabric, or on the CLARiiON® CX3 array to intercept writes to protected volumes so that a copy of the write can be sent to the RecoverPoint appliance for further processing.

Local recovery is provided through the EMC RecoverPoint Continuous Data Protection (CDP) module and remote recovery is provided though the RecoverPoint Continuous Remote Replication (CRR) module. Both modules run on the same platform to provide simultaneous local and remote data protection. Additionally the same volumes (LUNs) can be protected locally and remotely. This capability is called continuous local and remote (CLR) data protection.

The innovative technology of RecoverPoint supports flexible levels of protection without distance limitations or performance degradation. Continuous data protection technology offers a fine-grain recovery of application data and reduces the recovery point to near zero. Users can recover their data to any point in time, eliminating the need to invest in physical recovery of data damaged because of server outages, data corruption, software errors, viruses, and other common user errors.

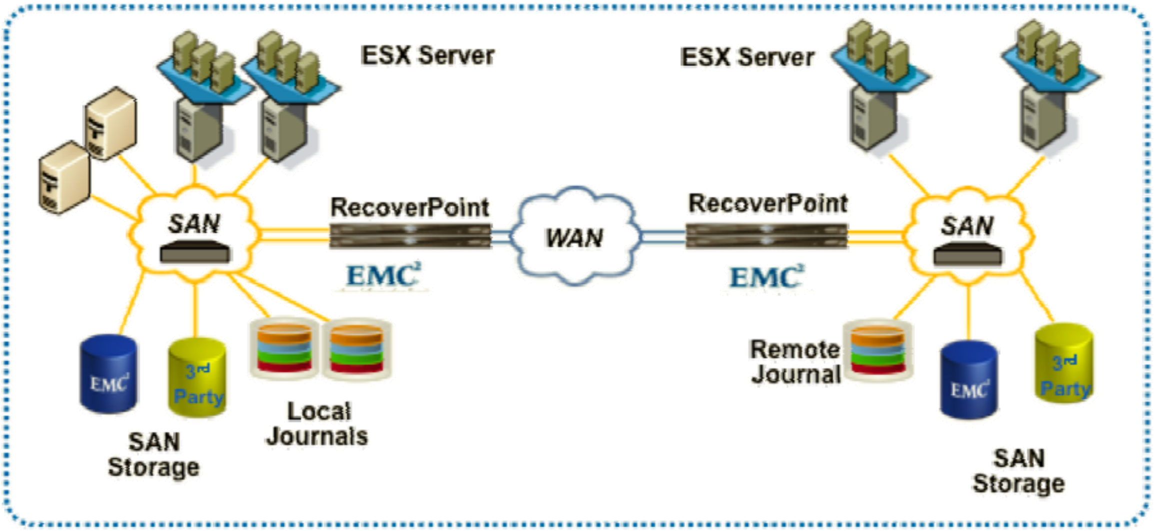

Figure 1. EMC RecoverPoint architecture overview

All of these capabilities help the customer achieve a dramatically lower total cost of ownership (TCO) compared to other host- or array-based replication solutions. Recovery testing is also made easier because of the ability to access the replicated data at the local or remote site for recovery or integrity testing purposes without interrupting the replication or the ongoing data center operations.

Write splitting technologies

Host-based write splitting

For VMware, RecoverPoint provides a host-based splitter (also called a KDriver) for Windows Server platforms. The KDriver is installed on each Windows virtual machine where it operates in the HBA stack, below the file system and volume management layers. The KDriver monitors writes and ensures that a copy of all writes to a protected volume is sent to the RecoverPoint appliance. Since the KDriver runs in the virtual machine, the only volumes that can be replicated by RecoverPoint would be SAN volumes attached to the virtual machine in physical RDM mode.

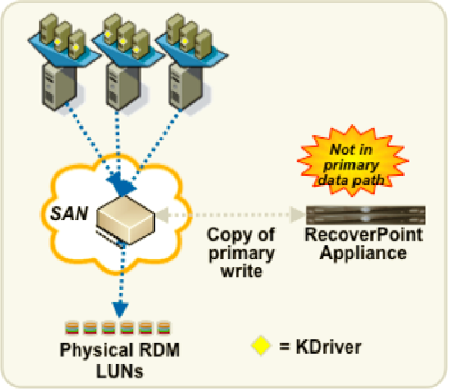

Figure 2. Host-based write splitting

In Figure 2, six virtual machines have the host-splitter (KDriver) installed, which is capturing writes to each SAN volume that is attached to each guest virtual machine in physical RDM mode.

Intelligent fabric write splitting

RecoverPoint write splitting is also provided through intelligent fabric APIs provided on EMC Connectrix switches using Brocade and Cisco technology. RecoverPoint supports the Brocade Storage Application Services APIs on the Connectrix AP-7600B department switch and on the PB-48K-AP4-18 blade installed in a Connectrix ED-48000B director. RecoverPoint also supports the Cisco SANTap APIs provided on the Connectrix Storage Services Module installed in a Connectrix MDS-9000 directory family.

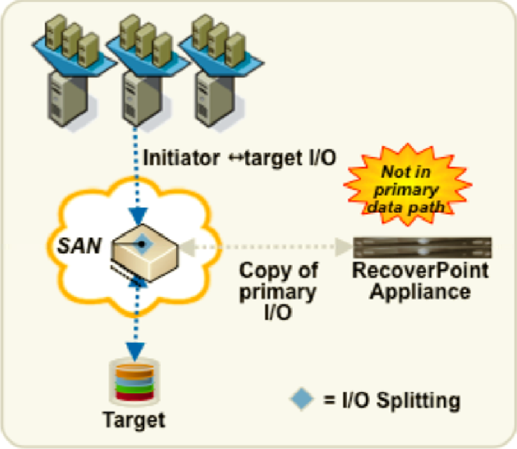

Figure 3. Intelligent fabric-based write splitting

When a write is passed down though an ESX server, either to an RDM volume in physical mode or to a VMFS volume, the intelligent fabric will mirror a copy of the write to the RecoverPoint appliance. This is an out-of-band, split-path implementation that ensures the original write is sent on to the target with no performance impact and that reads are processed directly without flowing through the RecoverPoint appliance. Intelligent fabric splitters can be used to replicate both RDM volumes in physical mode and volumes containing VMFS files.

CLARiiON array-based write splitting

Finally, RecoverPoint supports write splitting on CLARiiON CX3 arrays. The CLARiiON write splitter is a feature of CLARiiON FLARE® 26 and is supported on the CLARiiON CX3 arrays, including the CX3-10, CX3-20, CX3-40, and CX3-80. The write-splitting function operates in each storage processor where it monitors writes to protected volumes and ensures that the RecoverPoint appliance receives a copy of the write.

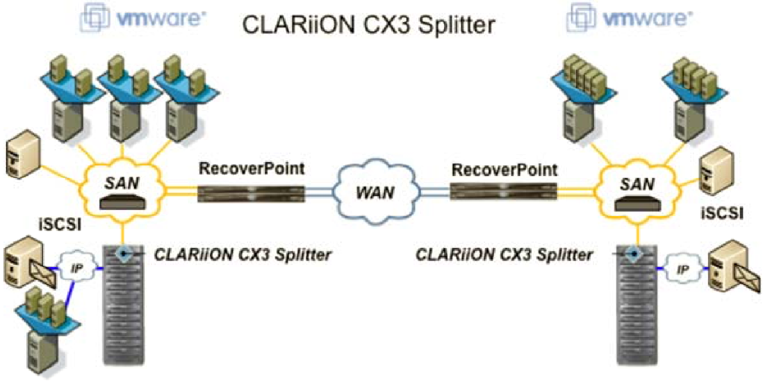

Figure 4. CLARiiON array-based write splitting

For VMware virtual machines, this enables replication of VMFS and physical RDM volumes without the cost or complexity of an intelligent fabric implementation. The splitter supports both Fibre Channel (FC) and iSCSI volumes presented by the CLARiiON array to any host, including to a VMware ESX Server.

How to choose the appropriate RecoverPoint splitter

Table 1 summarizes the VMware features and limits for each of the three write-splitting technologies supported by RecoverPoint 3.0.

The simplest configuration is the host-splitter configuration. For this configuration, the RecoverPoint host splitter (or KDriver) is installed on each virtual machine that has data that needs to be replicated. There are a few limitations on the host driver. First, it only supports the 32-bit and 64-bit Windows platforms; second, only the virtual machines data can be replicated, and it must be attached as a physical RDM volume, the boot volumes are not replicated; and third, only a maximum of 16 guest machines per VMware ESX server can be supported for replication, which is a VMware restriction.

Table 1. RecoverPoint splitter comparisons

Splitter Features	Windows Host Splitter	CLARiiON CX3 Splitter	Brocade/Cisco Fabric Splitter
Supports physical RDM	YES	YES	YES
Supports VMFS	NO	YES	YES
Supports VMotion	NO	YES	YES
Supports VMware DRS	NO	YES	YES
Supports VMware Site Recovery Manager	NO	YES	YES
Supports P2V replication	RDM	YES	YES
Supports V2V replication	RDM	YES	YES
Supports guest OS BFS	RDM	RDM & VMFS	RDM & VMFS
Supports ESX BFS	NO	YES	YES
Maximum number of guests supported per ESX Server	16 (VMware restriction)	N/A	N/A
Heterogeneous array support	EMC CX, DMX	CX3 only	EMC+3rd Party

The CLARiiON splitter is the most effective configuration for VMware replication. With a CLARiiON splitter, any of the physical RDM or volumes containing VMFS can be replicated. The only restriction on the CLARiiON splitter is that *all* of the volumes must reside on CLARiiON arrays that are supported by and attached to the RecoverPoint appliance.

The final configuration uses intelligent SAN APIs provided on some Brocade and Cisco switches. Using intelligent fabrics the volumes can reside anywhere in the SAN. Intelligent fabric splitting enables the replication of ESX boot volumes, virtual machine boot volumes (either as physical RDM volumes or as a VMFS volume), and virtual machine data volumes (either as physical RDM volumes or as VMFS volumes). Additionally, intelligent fabric splitting is the only way that replication across heterogeneous storage arrays (EMC to third party) is supported.

VMware ESX Server

The VMware ESX Server is virtual infrastructure software for consolidating and managing systems in mission-critical environments. VMware ESX Server speeds service deployments and adds management flexibility by partitioning x86 servers into a pool of secure, portable, and hardware-independent virtual machines.

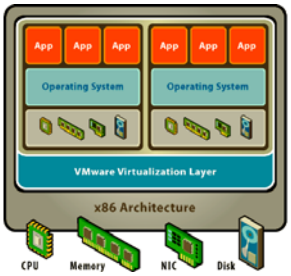

Figure 5. VMware ESX Server architecture

VMware ESX Server unifies the disaster recovery (DR) platform in a way that allows many production servers to be recovered on a single DR server without the need for costly one-to-one mapping of production and DR servers. Hardware-independent VMware ESX Server virtual machines eliminate the need to maintain identical hardware at production and DR sites.

VMware ESX Server can host multiple differing operating systems and applications that run concurrently in isolated virtual machines. System resources are dynamically allocated to each virtual machine based on need and configured service-level guarantees, providing mainframe-class control and capacity utilization of x86 servers. EMC RecoverPoint supports protection of the VMware ESX Server volumes, as well as the individual virtual machines and their data.

VMware Site Recovery Manager

VMware Site Recovery Manager uses knowledge about the virtualized infrastructure along with an external replication solution (such as EMC RecoverPoint) to provide disaster recovery management and automation for the virtual data center. What VMotion provides for movement of virtual machines within the same SAN, Site Recovery Manager can provide across two SANs separated by an arbitrary distance.

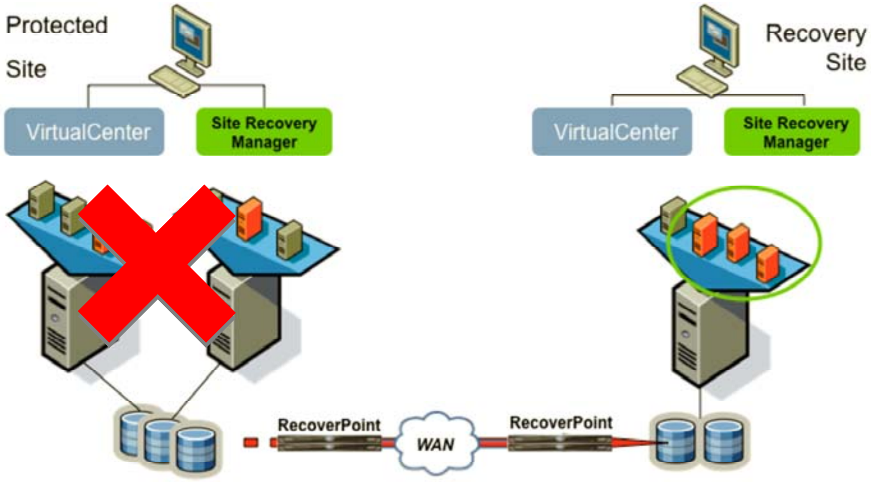

Figure 6. VMware Site Recovery Manager at a glance

VMware Site Recovery Manager makes disaster recovery rapid, reliable, manageable, and affordable. 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—yet another reason that the VMware virtualization platform is the safest platform for data center applications.

RecoverPoint replication for VMware

RecoverPoint provides a full-featured replication solution for the VMware ESX. It uses unique small-aperture data capture technology that protects the VMware ESX platform from data corruption and guarantees recoverability with minimum data loss to point in time crash-consistent images. For local replication in the same SAN, every write is captured and stored in the RecoverPoint journal. For remote replication between SANs, the user specifies policies for the replication that controls the aperture-size to ensure that specific recovery point objectives (RPOs) are met for each consistency group.

RecoverPoint supports SAN-attached volumes when replicating VMware virtual machines. Both physical mode Raw Device Mapping (RDM) and VMware ESX File System (VMFS) volumes are supported for replication. Additionally, if the VMware ESX Server is configured for Boot From SAN (BFS), then these volumes can also be replicated 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 though the intelligent fabric or CLARiiON CX3-based splitters. If intelligent fabric or a CLARiiON CX3-based splitter is not used, then RecoverPoint captures the changes by using a Windows-based KDriver, however the KDriver can only capture changes written to an RDM volume in physical mode.

To ensure that the crash-consistent images are consistent for each virtual machine, it is recommended that you create frequent RecoverPoint bookmarks while the VMware ESX Server is in a quiesced state. To do so, 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, it is possible to 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 allowing 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 physical RDM volume. Once mounted it can be repurposed for backup, DR testing, or immediate recovery of files, folders, volumes or entire virtual machines. When using RecoverPoint to replicate the data, there is no awareness of the virtual infrastructure at the destination site. You will either need to script a process to scan for and register virtual machines on the replicated volumes, or you will need to manually configure each virtual machine on the destination side. The target virtual machines will be stored in a powered off, or cold state, until they are required. To provide some level of virtual machine awareness RecoverPoint implemented the VMware storage replication adapter), which enables RecoverPoint to be utilized as an external replication provider for VMware Site Recovery Manager. VMware Site Recovery Manager will automate the scanning and registration process of the replicated volumes for the virtual machines and their data as part of the disaster recovery failover process.

The following configurations for protection of the VMware ESX Server virtual machines are considered in this white paper:

[1] While it is possible to use the SYNC driver, a description of this procedure is beyond the scope of this document.

- P2V: Replication of a physical server to a local and/or remote standby virtual machine

  In this use case, the customer has implemented a VMware Infrastructure at the remote site that is utilized for disaster recovery. The production site is comprised of physical servers, or is a mix of physical servers and virtualized servers. One or more of the servers can be recovered onto a standby DR virtual machine running in a VMware ESX Server at a DR site.

- V2V: Replication of a virtual machine to a local and/or remote virtual machine

  In this configuration one or more virtual machines in one or more ESX Servers can be recovered onto a standby VMware ESX Server at a DR site.

- P2P with virtual CDP: Replication of a physical server to a remote standby physical server with local replication to a standby virtual machine

  In this configuration data from local physical servers is replicated to a remote DR site. Additionally, local replication using RecoverPoint's continuous data protection technology enables the protection and importing of the data to a VMware ESX Server residing in the local SAN.

- V2P with physical CDP: Replication of a virtual machine in one or more ESX Servers to local and remote physical machines.

  In this configuration, the local virtual machine is continuously protected and its data can be recovered onto another local physical machine or on to a physical machine at the DR site. This requires that the virtual machine's data resides in an RDM volume attached in physical compatibility mode.

- V2V with VMware Site Recovery Manager: Replication of a virtual machine to a remote virtual machine with failover automation provided by VMware Site Recovery Manager.

  In this configuration, one or more virtual machines in one or more ESX Servers can be automatically recovered onto a standby ESX Server at the DR site through the integration of RecoverPoint with VMware Site Recovery Manager.

VMware Raw Device Mapping (RDM)

All of these scenarios require that the VMware ESX Server storage reside on a SAN. When using a RecoverPoint host-splitter driver for a virtual machine the applications access their data using VMware RDM in physical compatibility mode. Additionally, when using RecoverPoint to replicate data between a physical server and a virtualized environment, the virtualized servers must access the replicated data in RDM mode or they must convert the replica copy into a VMFS image.

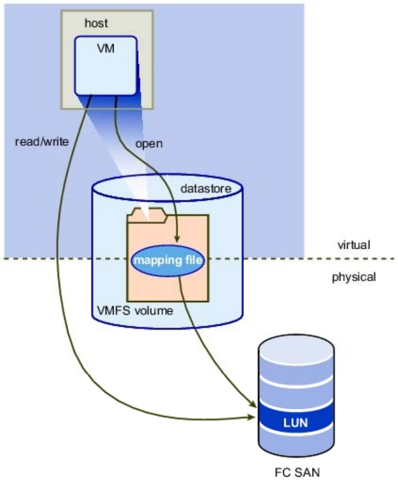

Figure 7. VMware Raw Device Mapping

Introduced with VMware ESX Server 2.5, RDM allows a special file in the VMFS volumes to act as a proxy for a raw device. An RDM can be thought of as a symbolic link from a VMFS volume to a raw LUN. The mapping makes LUNs appear as files in a VMFS volume. The mapping file, not the raw LUN, is referenced in the virtual machine configuration. When a LUN is opened for access, the mapping file is read to obtain the reference to the raw LUN. Thereafter, reads and writes go directly to the raw LUN rather than going through the mapping file.

Using RDM allows SAN-aware layered applications, such as a RecoverPoint host splitter, to run inside the virtual machine. If RDM is not feasible, then a SAN-agnostic solution, such as the CLARiiON array-based splitter or intelligent-fabric splitters from Brocade or Cisco, must be used.

Physical-to-virtual replication

This is a common configuration for customers that have deployed VMware infrastructure to provide disaster recovery resources in a remote data center, but have not migrated their production data center onto a VMware infrastructure. This is commonly referred to as physical-to-virtual replication. Additionally, customers that are evaluating the use of a virtualized infrastructure for their production environment can use this replication to clone their production environments and test them in a virtualized configuration.

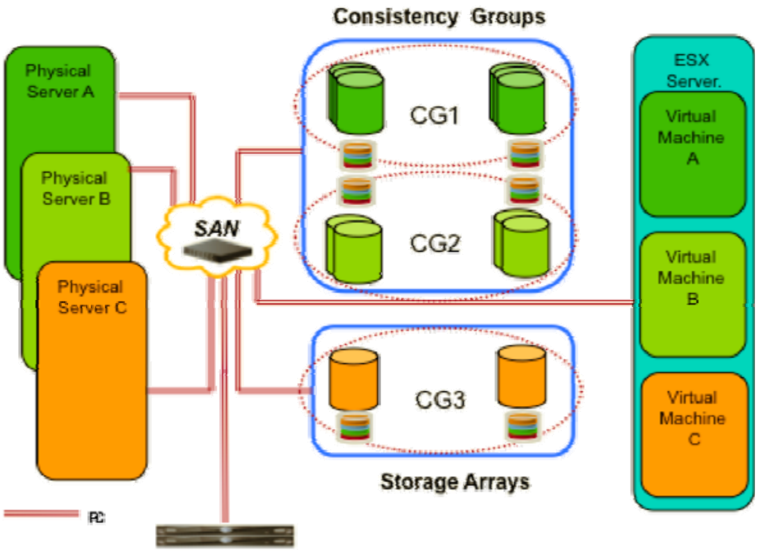

Figure 8. Physical-to-virtual replication

This configuration requires that the VMware virtual machines utilize RDM volumes in physical mode, or that VMware Converter is used to migrate the RDM volumes to VMFS.

In physical-to-virtual replication, each physical machine is mapped to a RecoverPoint consistency group. Each of the LUNs accessed by the production machine become a replication set in the consistency group. Separating the physical server replication by consistency group allows for either a planned failover or for the use of the replicated image in the ESX machine for purposes such as testing, data mining, and object recovery. The target virtual machine can be either local, as shown in the figure above, and/or remote. With RecoverPoint there is no need to have the replicas reside in the same array, array family, or volume type as RecoverPoint will manage the physical replication between dissimilar arrays.

The ESX server is built and configured with virtual machines that match the application configuration of the physical machines. The virtual machines are not running during normal operations, and are only powered on to access new data. The basic flow is as follows:

1. Select the appropriate image using either a point-in-time selection or a bookmark selection requesting physical image access. This will cause RecoverPoint to roll back the replica image to the selected point-in-time image.
2. Once the rollback is completed, the selected image LUNs will be unmasked and will become visible to the ESX Server
3. From the ESX Server console, scan for the new LUNs and then register them with the appropriate virtual machine.
4. Power up the virtual machine, which will see the point-in-time image data. At this point any reads and writes to the image are tracked by RecoverPoint so that they can be backed out when image access is completed.

After step 2 completes, a TimeFinder® BCV or SnapView™ clone can be created from the replica LUNs, and then RecoverPoint would be informed that image access is completed. Once RecoverPoint resumes processing the user would present the BCV or clone copies to the ESX server for use by the virtual machines. Alternatively, these copies can be used by VMware Converter to import the data to existing VMFS volumes.

Virtual-to-virtual replication

In this usage case the customer has fully migrated to a VMware infrastructure for their production and disaster recovery sites. At the disaster recovery site, they are taking advantage of the server and storage consolidation capabilities of VMware and RecoverPoint. The customer has fully deployed a VMware ESX Server environment using VMFS deployed with either a CLARiiON CX3 splitter or an intelligent fabric write splitter. This configuration can also be supported using a Windows-based KDriver when SAN LUNs are attached as physical RDM volumes.

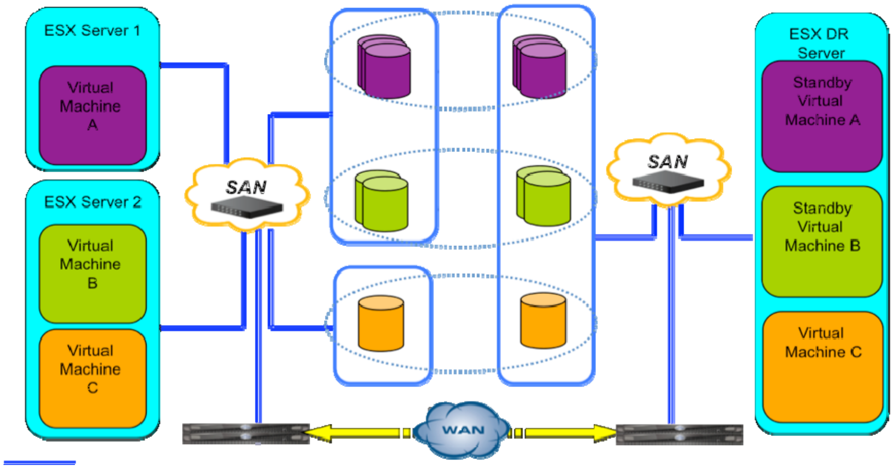

Figure 9. Virtual-to-virtual replication

If a VMFS is used, then the virtual machines are either configured to use a separate VMFS volume for each machine or all of the virtual machines use the same VMFS volumes. In the figure above, each virtual machine is assumed to have its own VMFS; this allows for an individual virtual machine to be tested and/or failed over to the disaster recovery site without impacting the remaining virtual machines. When multiple guest operating systems (OSs) are distributed over a limited set of LUNs, such as combined into one or more VMFS volumes, a special configuration is recommended that allows single guest OS replication granularity, thereby expediting failover and test activities.

In the combined VMFS configuration, two RecoverPoint consistency groups will be defined. The first RecoverPoint consistency group contains all of the existing LUNs (or VMFS volumes) with the entire set of guest OSs and their data. The second RecoverPoint consistency group, or *standby*, contains storage volumes at each site that are at least as large as the largest combined guest OS image and related virtual data disks. Although this group is configured for RecoverPoint replication, it does not replicate any data as long as there are no writes taking place at the source site. When needed, any guest OS with its data can be moved to this storage space, and individually replicated to the target site. As a result, it is also possible to test and, if desired, fail over this guest OS independently from the other guest OSs.

Physical-to-physical replication with local virtualization

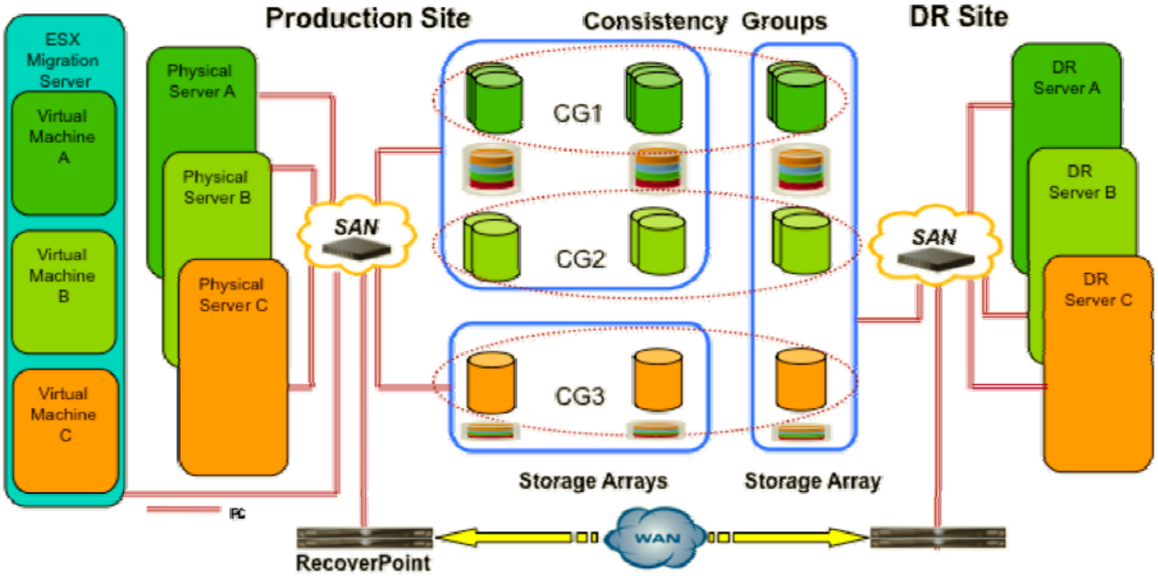

Figure 10. Physical-to-physical replication with local virtualization

This is a typical configuration where the customer is looking to migrate from a physical to virtual environment either for their production data center or for their disaster recovery data center. This is similar to local physical-to-virtual replication with the addition that physical machines still exist in the disaster recovery site. Each physical machine is mapped to a RecoverPoint consistency group and the virtual machines access the local replicas as physical mode RDM volumes. The benefit of using RecoverPoint concurrent local and remote data protection is that the local replica copies can be accessed without impacting the protection and disaster recovery of the physical servers. As this configuration requires the use of SAN volumes accessed as physical mode RDM volumes, any of the RecoverPoint write splitting technologies can be implemented, including host, CLARiiON CX3, and intelligent-fabric splitters.

Using VMware Site Recovery Manager with RecoverPoint

Traditional disaster recovery solutions leave many organizations unable to meet recovery time and recovery point objectives. The slow and often manual recovery processes common in traditional disaster recovery solutions are prone to errors and result in frequent failures. VMware Site Recovery Manager automates the recovery process so it becomes as simple as pressing a single button. There is no need for the user to interact with the RecoverPoint console and the VMware console; instead VMware automates the process. All the user has to do is ensure that the production virtual machines are mapped to LUNs that are replicated by RecoverPoint to the remote site.

As you can see by the following figure, RecoverPoint sits below the VMware Infrastructure and is responsible for replicating all changes from the production LUNs to the remote replicate LUNs at the disaster recovery site. The RecoverPoint storage replication adapter is installed on the same servers that are running Virtual Center and the Site Recovery Manager service in the production and disaster recovery site.

The benefits of RecoverPoint are that the replication can be between differing arrays, such as between a Symmetrix DMX™ and a CLARiiON CX3. Additionally, there is no requirement that the production volumes be attached to the VMware servers in physical RDM mode; instead the data can reside on VMFS file systems that are contained on the production LUNs. Finally, with RecoverPoint the distance between the sites is not a limit, since RecoverPoint replicates the data asynchronously, but maintains the write-order consistency at the remote site, ensuring that all replicas remain fully consistent.

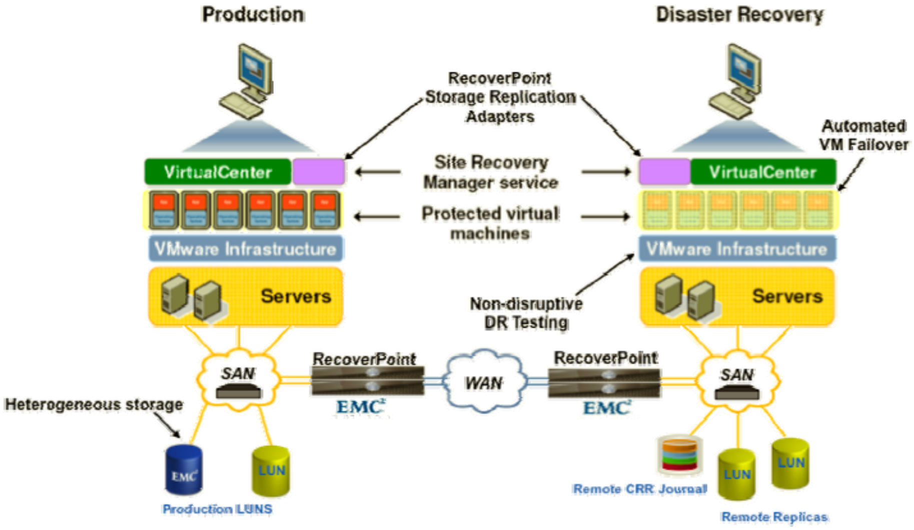

Figure 11. RecoverPoint integration with VMware SRM

Integration with RecoverPoint

VMware Site Recovery Manager is designed as a plug-in to VirtualCenter 2.5 so that DR tasks can be executed inside the same management tool as other VM administration tasks such as creation, migration, and deletion. VMware Site Recovery Manager is highly automated and is responsible for the setup, test, and recovery workflows for DR recovery automation. VMware Site Recovery Manager reduces the RTO for DR and relies on block-based replication, such as is provided by RecoverPoint, to reduce the RPO for DR. To implement replication, a VMware storage replication adapter for RecoverPoint is used to map the VMware Site Recovery Manager requests into the appropriate RecoverPoint actions. The RecoverPoint replication adapter was developed and qualified, and is supported by EMC. The RecoverPoint adapter can be downloaded from the VMware site and it is also available from EMC.

All of the benefits of RecoverPoint discussed in this paper also apply when VMware Site Recovery Manager uses RecoverPoint for replication. This includes the use of CLARiiON CX3 array-based write splitters, heterogeneous storage, and policy-based replication. VMware Site Recovery Manager is designed for site-to-site replication, as such it only works with remote replication as provided by RecoverPoint CRR, or if continuous local and remote data protection is being used, Site Recovery Manager will only operate with the remote replica copy.

Ensuring reliable recovery through automation and testing

Testing disaster recovery plans and ensuring that they are executed correctly are critical to making recovery reliable. However, testing is difficult with traditional solutions due to the high cost, complexity, and disruption associated with tests. Another challenge is ensuring that staff are trained and prepared to successfully execute the complex process of recovery.

Site Recovery Manager helps you overcome these obstacles by enabling realistic, frequent tests of recovery plans and eliminating common causes of failures during recovery. It provides built-in capabilities for executing realistic, non-disruptive tests without the cost and complexity of traditional disaster recovery testing. Because the recovery process is automated, you can also ensure that the recovery plan will be carried out correctly in both testing and failover scenarios. Site Recovery Manager also leverages VMware Infrastructure to provide hardware-independent recovery to ensure successful recovery even when recovery hardware is not identical to production hardware.

Taking control of disaster recovery plans

Until now, keeping recovery plans and their associated processes accurate and up to date have been practically impossible due to the complexity of plans and the dynamic environment in today's data centers. Adding to that challenge, traditional solutions do not offer a central point of management for recovery plans and make it difficult to integrate the different tools and components of disaster recovery solutions.

VMware Site Recovery Manager simplifies and centralizes the creation and ongoing management of disaster recovery plans. Site Recovery Manager turns traditional oversized disaster recovery processes into automated plans that are easily to manage, store, and document. Additionally, Site Recovery Manager is tightly integrated with VMware Infrastructure 3, so you can create, manage, and update recovery plans from the same place that you manage your virtual infrastructure.

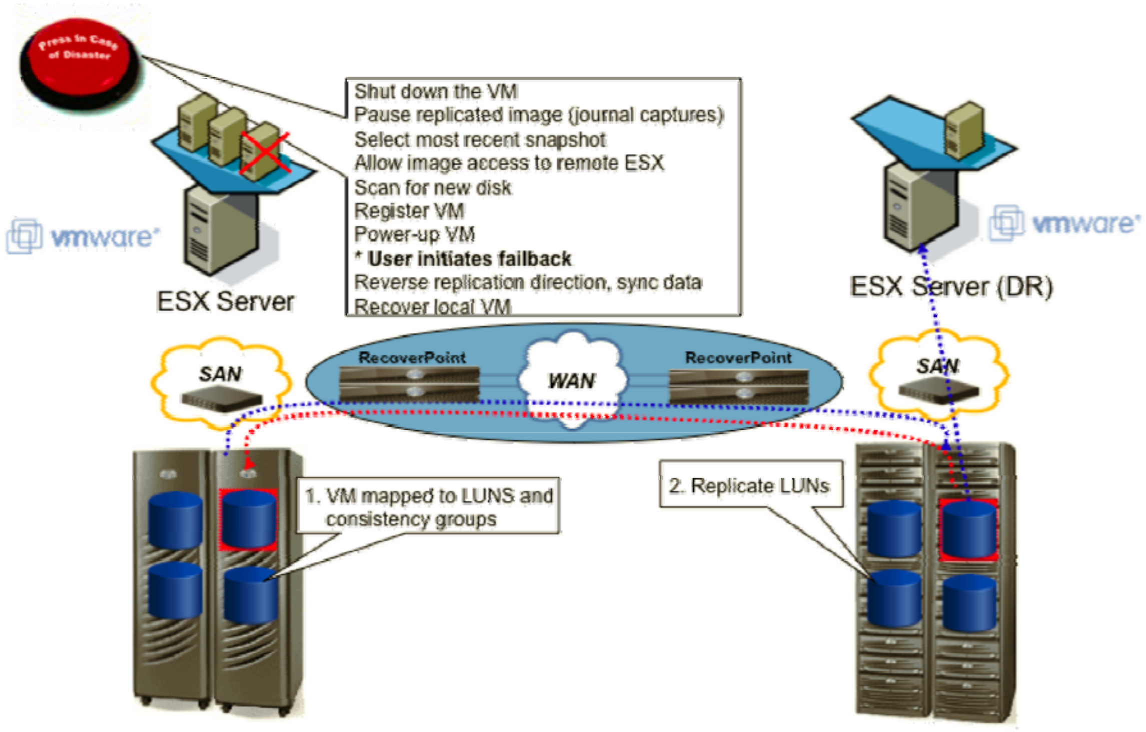
Press in Case of Disaster
Shut down the VM
Pause replicated image (journal captures)
Select most recent snapshot
Allow image access to remote ESX
Scan for new disk
Register VM
Power-up VM
* User initiates failback
Reverse replication direction, sync data
Recover local VM
vmware
ESX Server
vmware
ESX Server (DR)
SAN
RecoverPoint
WAN
RecoverPoint
SAN
1. VM mapped to LUNS and consistency groups
2. Replicate LUNs

Figure 12. Automated recovery using VMware Site Recovery Manager and RecoverPoint

The figure above shows what happens when a disaster occurs and the VMware administrator utilizes VMware Site Recovery Manager to perform the disaster recovery. Following the DR plans, VMware will shut down the appropriate virtual machine(s) and select the most recent image replicated by RecoverPoint. At the remote site this image becomes visible to the DR VMware ESX Server. At this point the DR ESX discovers the new LUNs, registers the virtual machines that reside on the LUNs, and then powers up the virtual machines. When the administrator needs to fail back the virtual machine it is very simple to use the RecoverPoint GUI to reverse the replication direction and resynchronize the data. Once data is fully synchronized the virtual machine at the DR site can be shut down and the local virtual machine can be restarted.

Conclusion

The innovative technology of EMC RecoverPoint supports flexible levels of protection, without distance limitations and performance degradation. With its unique architecture, powerful data recovery features, and business-driven approach, RecoverPoint offers superior levels of local and remote data protection and business continuity to organizations running VMware ESX. Organizations implementing RecoverPoint with the VMware ESX Server are expected to see the following benefits:

- Full support for RecoverPoint integrated with VMware Site Recovery Manager
- Ability to leverage RecoverPoint concurrent local and remote data replication to accelerate the transitioning or migration to a VMware Infrastructure
- Full support for VMware physical-to-virtual and virtual-to-virtual replication models.
- Support for heterogeneous storage reduces the need to perform data migration between storage architectures
- Coexists with VMware technologies, including DRS, HA, Storage VMotion, and VMotion
- Supports replication between VMFS volumes as well as between RDM volumes in physical mode
- Simple and quick planned or unplanned failover for virtual machines and their data without distance limitation
- Out-of-band processing for replication that ensures that the performance of the ESX Server and its virtual machines are not impacted by RecoverPoint
- Innovative compression algorithms and intelligent bandwidth policy management that eliminate the need for dedicated IP or FC links between sites
- Rapid and simple replication for virtual machines and their data to an alternate location and instantly accessible for disaster recovery or for recovery from logical corruption
- Ability to leverage local replication for operational or application recovery of a virtual machine while still maintaining remote replication to provide protection in case of a site-wide disaster

References

- *Replicating VMware ESX 2.5/3.0x with EMC RecoverPoint Technical Notes*
- Customer Presentation: *EMC RecoverPoint VMware Support – Complete Data Protection for VMware Virtual Infrastructure*

View EMC’s proven solutions for data replication, data lifecycle management, disaster recovery, and continuous data protection at http://www.EMC.com.