Disaster Recovery of Microsoft Exchange Server 2007 on EMC Celerra iSCSI using EMC Replication Manager and VMware vCenter Site Recovery Manager

Abstract

This white paper discusses the best practices and guidelines to successfully implement disaster recovery solutions for Microsoft Exchange Server by using EMC® Replication Manager with EMC Celerra® in a VMware environment. This white paper also discusses the technical reasons for these implementation techniques.

August 2009
# Table of Contents

**Executive summary** .................................................................................................................. 5  
**Introduction** .............................................................................................................................. 5  
  Audience ........................................................................................................................................ 5  
  Terminology ................................................................................................................................... 6  
**Technology overview** ............................................................................................................... 7  
  EMC Celerra Replicator ................................................................................................................ 7  
  EMC Replication Manager ........................................................................................................... 7  
  VMware vCenter SRM ................................................................................................................... 7  
**Disaster recovery overview** ..................................................................................................... 8  
  What is a disaster? ....................................................................................................................... 8  
  What is disaster recovery? ........................................................................................................... 9  
**Disaster recovery solutions** ..................................................................................................... 9  
  Physical and virtual disaster recovery solutions ....................................................................... 9  
  Replication Manager with VMware vCenter SRM ................................................................... 9  
**Implement Replication Manager with VMware vCenter SRM** .............................................. 10  
  Celerra file system and iSCSI LUN sizing requirements ............................................................. 10  
  Hardware and software configuration requirements ................................................................. 11  
    Protected site ............................................................................................................................ 12  
    Production Replication Manager proxy client ....................................................................... 12  
    Production virtual machine hosts .......................................................................................... 12  
    Recovery site ........................................................................................................................... 12  
    Recovery Replication Manager proxy client ........................................................................... 12  
    Recovery virtual machine hosts ............................................................................................. 12  
  Configure Replication Manager server disaster recovery ......................................................... 13  
    Primary Replication Manager server .................................................................................... 13  
    Secondary Replication Manager server ................................................................................. 13  
  Configure VMFS and virtual disk replications ......................................................................... 13  
    Sample configuration .............................................................................................................. 13  
    Replication Manager application sets and jobs ...................................................................... 15  
  Configure VMware vCenter SRM .............................................................................................. 15  
    Install VMware vCenter Site Recovery Manager plug-in ....................................................... 15  
    Configure the protected and recovery sites .......................................................................... 16  
  Protect the VMware environment ............................................................................................. 16  
    Create protection groups ....................................................................................................... 17  
    Create a recovery plan ........................................................................................................... 18  
    Specify the guest OS customization ....................................................................................... 19  
**Perform disaster recovery operations** .................................................................................. 20  
  Test a failover ............................................................................................................................. 21  
    Protection Group Failover using the VMware vCenter SRM recovery plan ......................... 21  
    Test failover ........................................................................................................................... 21  
    Run recovery plan ................................................................................................................ 22  
    Post-failover actions .............................................................................................................. 24  
    Recovery-site vCenter operations ......................................................................................... 24  
    Protection-site vCenter operations ....................................................................................... 24
Executive summary
With the increasing importance of information technology for the continuity of business-critical functions, the importance of protecting an organization’s data and IT infrastructure in the event of a disruptive situation has become an increasingly visible business priority in recent years. There is no tolerance for downtime or system unavailability of information systems because downtime usually equates to a loss of revenue and a loss in productivity.

Messaging is one of the most mission-critical applications for businesses today. Microsoft Exchange Server 2007 is the leading messaging platform for customers ranging from large enterprises to branch offices to small business units. The Exchange messaging environments are growing in complexity and user requirements are becoming increasingly demanding. Additionally, the manner in which the Exchange Server environment is now used to support business operations is even more business critical than ever before. Therefore, it is important to design the Exchange Server environment for optimum performance and high availability.

Today, an increasing number of customers are exploring ways to virtualize the Exchange Server environment to reduce cost, increase availability, add flexibility, and use resources more efficiently. It is both expensive and cumbersome to implement a disaster recovery solution in physical environments, but it is much more convenient to implement a disaster recovery solution in a VMware environment. VMware vCenter Site Recovery Manager (SRM), in conjunction with array-based remote replication technologies, provides a simple, automated disaster recovery solution for VMware environments. EMC® Celerra Replicator™ and EMC Replication Manager provide an easy remote replication option to facilitate a disaster recovery solution for VMware environments. Together, they achieve the best recovery point objective (RPO) and shortest recovery time objective (RTO) of customers.

This white paper discusses the implementation guidelines for using EMC Replication Manager with VMware vCenter Site Recovery Manager to facilitate the disaster recovery of virtual machines and virtual disks hosted on a Celerra® unified storage system. EMC Replication Manager and VMware vCenter SRM with the EMC Celerra unified storage system provide customers with enhanced disaster recovery automation and management capabilities. This solution provides fast recovery and reduces the complexity and manageability challenges associated with traditional disaster recovery processes.

The best practices discussed in this white paper will help customers leverage the capabilities of EMC Replication Manager and VMware vCenter SRM to implement and test a disaster recovery solution with EMC Celerra in a VMware environment.

Introduction
This white paper discusses the best practices to implement a disaster recovery solution in a VMware environment by using EMC Replication Manager in conjunction with VMware vCenter SRM. This solution uses native EMC Celerra array-based remote replication technology to perform the actual replication of data. For the sake of simplicity, the business case used in this discussion involves implementing a disaster recovery solution for virtual machines running Microsoft Exchange Server 2007.

This paper does not cover the details of product configuration. Product configuration is covered in other EMC and VMware documentation that are referenced at the end of this document.

Audience
This white paper is for customers, EMC partners, and service personnel involved in planning, architecting, or administrating a VMware environment and thinking about implementing EMC Replication Manager for disaster recovery solutions. This document assumes that the audience is familiar with Celerra and VMware environments.
Terminology

datastore — A file system, either Virtual Machine File System (VMFS) or Network File System (NFS), that serves as a virtual representation of an underlying pool of physical storage resources. These physical storage resources can comprise of SCSI disks from a local server, Fibre Channel SAN disk arrays, iSCSI SAN disk arrays, or network-attached storage arrays.

disaster recovery system — The components consisting of a Windows server, Celerra Network Server, and associated software located at a secondary data center that replicate the data from the production system at the primary data center.

failback — The process by which live data on the disaster recovery system is failed over to a restored or new production system in a primary data center. Failback as used in this document does not imply a return to any pre-existing state on the production server in the primary data center. It involves failing over from the disaster recovery server to the new production server after it is online.

failover — The process of immediately routing data to an alternate data path or device to avoid interrupting services in the event of a failure. The impact to service is dependent on the application’s ability to handle the change gracefully. Initially, failover occurs from the primary data center to the secondary data center. In recovery, failover occurs from the secondary data center to the newly functional system at the primary data center.

guest operating system — An operating system that runs within a virtual machine.

live data — Data used in the live user environment, whether served by the production system at the primary data center or the disaster recovery system at the secondary data center.

logical unit number (LUN) — Identifying number of a SCSI or iSCSI object that processes SCSI commands. The LUN is the last part of the SCSI address for a SCSI object. The LUN is an ID for the logical unit, but the term is often used to refer to the logical unit itself. It refers to a single storage device on the storage array that can be mapped to one or more ESX servers.

primary Replication Manager server — Host that runs the Replication Manager server software and controls the replication.

production host — Host that runs the database/application and contains all the database production data.

production system — The components consisting of a Windows server, Celerra Network Server, and associated software at a primary data center. During a failure, the production system becomes unavailable.

protected site — The physical location of the production systems that are protected by SRM.

recovery site — The physical location of the disaster recovery system.

replica — The snapshot of live data that the disaster recovery system uses to assume the role of providing live data.

replication — The process by which Replication Manager creates snapshots of live data from the production system and copies that information to the disaster recovery system at the secondary data center.

Replication Manager proxy host — A physical or virtual Windows server that Replication Manager uses to communicate with VMware vCenter. This host runs Replication Manager agent software and facilitates Replication Manager’s interaction with VMware to perform the tasks necessary to create, mount, unmount, restore, and expire VMFS replicas.

secondary Replication Manager server — Host that runs Replication Manager server software with a read-only configuration. The Replication Manager database is automatically synchronized with the primary server host’s Replication Manager database.

virtual machine — A virtualized x86 PC environment on which a guest operating system and associated application software run. Multiple virtual machines can run concurrently on the same physical machine.

Virtual Machine File System (VMFS) — VMware VMFS is a high-performance cluster file system for ESX virtual machines and for the virtual disks for these virtual machines. Each virtual machine or virtual...
disk is encapsulated in a set of files and VMFS is the default storage system for these files on physical SCSI disks and partitions.

**VMware ESX**—A production-proven virtualization layer that runs on physical servers such that it abstracts the processor, memory, storage, and networking resources to be provisioned to multiple virtual machines.

**Technology overview**

The following section provides a brief overview of the technology and test environment discussed in this white paper.

**EMC Celerra Replicator**

EMC Celerra Replicator for iSCSI manages local snapshots of a database by using EMC Replication Manager. Celerra Replicator enables you to create and manage replication sessions, each producing a read-only, point-in-time copy of a given source object at a designated destination. Celerra Replicator sessions, which can be created by using the command line interface (CLI) or Celerra Manager, are characterized by an architecture based on snapshot/checkpoint technology, asynchronous transfer to the destination, and support for file system, Virtual Data Mover (VDM), and iSCSI LUN source object types.

By using asynchronous replication along with the snapshot functionality, only changed blocks of data are sent across the network once per update cycle and no additional server resources are required. The process also leverages Volume Shadow Copy Service (VSS) to ensure inter-database consistency and zero application downtime during the replication cycle. It also improves the replication throughput on high-latency IP networks by autosizing the TCP window.

**EMC Replication Manager**

EMC Replication Manager manages EMC point-in-time replication technologies and coordinates the entire data replication process from discovery and configuration to the management of multiple disk-based replicas. Replication Manager is designed to manage and automate snapshots and clones for EMC’s point-in-time replication products on:

- Symmetrix® arrays by using the TimeFinder® and RecoverPoint family
- CLARiiON® by using SnapView™, SAN Copy™, and the RecoverPoint family
- iSCSI Celerra by using SnapSure™ and Celerra Replicator

Replication Manager’s application-aware, host-aware, and storage-aware capabilities liberate customers from the efforts needed to perform manual backup and recovery operations along with creating and maintaining numerous scripts for them across a variety of applications, platforms, and storage systems.

With Replication Manager, customers can leverage the efficiencies of VMware infrastructure for crash-consistent replicas of VMFS containing Windows and Linux virtual machines with application servers such as Exchange Server.

**VMware vCenter SRM**

VMware vCenter SRM is a disaster recovery management and automation solution for VMware infrastructure. It is designed as a plug-in to vCenter so that you can execute disaster recovery tasks inside the same management tool that other virtual machines administration tasks are executed in. VMware vCenter SRM leverages the disaster recovery features and capabilities of the VMware infrastructure to simplify and automate the key elements of disaster recovery such as setting up disaster recovery plans, testing the plans, executing failover when a data center disaster occurs, and failing back to the primary data center.
**Figure 1** shows the key components of a VMware vCenter SRM environment.

![Image of key components](image)

**Figure 1** **Key components of a VMware vCenter SRM environment**

VMware vCenter SRM operates on a paired-site relationship (for example, one site protects another) and requires that you have access to both the protected (primary) and recovery (secondary) sites. The protected site refers to the production environment where the virtual components responsible for business continuity reside. In the event of a disaster, the protected site fails over to the recovery site.

VMware vCenter SRM provides built-in capabilities to execute realistic, nondisruptive tests without the cost and complexity of traditional disaster recovery testing. Through its failover simulations, it enables you to confirm that the recovery plan has been set up correctly for the protected configuration. It also allows you to confirm that the protected virtual machines start in the correct order, taking into account the various application dependencies for the protected virtual machines in the environment. Because the recovery process is automated, you can ensure that the recovery plan is carried out correctly in both testing and failover scenarios.

VMware vCenter SRM depends on third-party storage-based replication, such as EMC Celerra Replicator and EMC Replication Manager, to replicate the data on disk to the recovery site. SRM communicates with the third-party replication through Storage Replication Adapters (SRA) that plug in to VMware vCenter SRM such as with EMC Celerra for iSCSI SAN.

**Disaster recovery overview**

The following section briefly describes the basic concepts of disaster, disaster recovery, and disaster recovery solutions.

**What is a disaster?**

From the perspective of IT infrastructure, a disaster is an event that leads to the complete loss of a data center for an extended period of time. A disaster causes large-scale disruption, and the declaration of a disruptive event as a disaster often involves the consensus of higher management. However, do not confuse disaster with an outage such as the failure of a single host, or the disruption of any service within a data
center. A disaster involves the failure of a major portion of the critical technology infrastructure of an organization.

**What is disaster recovery?**

Disaster recovery, in general, refers to the processes, policies, and procedures that are related to the preparation for recovery or continuity of technology infrastructure critical to an organization after a disaster. In a data center, this involves setup, failover, and failback procedures that are required to actuate live data from a failed production system to a disaster recovery system, and then back to a new or restored production system.

**Disaster recovery solutions**

This section compares the disaster recovery solutions by using physical servers and virtual machines. It also discusses the capabilities of VMware vCenter SRM and the role of EMC Replication Manager and Celerra Replicator in achieving this.

**Physical and virtual disaster recovery solutions**

The conventional disaster recovery solution model involves implementing a disaster recovery solution for physical servers. For this, identical hardware is maintained at the primary data center and the secondary data center. The identical hardware at the secondary data center is kept “on-hold” and the production fails over to it during a disaster. However, using a physical server to implement such a solution has limitations. For example, to maintain an identical operating environment at the secondary location, the operating system (OS) patch levels and application service pack levels must be consistent. Also, it is difficult to test and automate the process of disaster recovery in physical environments. The process to recover the server involves many manual steps such as reinstalling the operating system, applying patches, and recovering the production data from the backup medium such as tape. Typically, these steps are performed manually in physical environments and are difficult to test.

The virtual solution for disaster recovery, that is using virtual machines instead of physical servers, overcomes these drawbacks and proves to be a better vehicle for disaster recovery. Virtual machines are portable because they can be easily transmitted over wire and programmatically powered on and off. Moreover, it is possible to programmatically reconfigure virtual networks. These features are beneficial in automating the recovery operations. By including the boot disk, virtual disaster recovery eliminates the need to apply OS patches in parallel at the primary and secondary sites. This minimizes human errors too. Based on these comparisons, you can easily see the reason for the gaining popularity of virtual disaster recovery solutions and their increasing preference over the traditional disaster recovery solution that uses physical servers.

**Replication Manager with VMware vCenter SRM**

VMware vCenter SRM builds on the capabilities of the VMware infrastructure to provide management and automation for disaster recovery. It simplifies and enables the workflows that are part of disaster recovery, for example, setup, testing, failover, and failback. In traditional disaster recovery plans, these workflows require many manual, complex steps. SRM makes it possible to eliminate or simplify the manual steps in these workflows.

However, VMware vCenter SRM does not actually perform the replication for disaster recovery. It works on the setup, test, and recovery workflows only. SRM depends on third-party storage-based replication to replicate the data on disk to the recovery site. It communicates with the third-party replication through storage replication adapters that plug in to SRM. EMC Celerra Replicator provides the required third-party storage-based remote replication option that you can use to implement the disaster recovery solution across geographical locations. This is where Replication Manager adds value by providing easy management of Celerra replication in VMware environments. Replication Manager provides a single, easy-to-use interface...
to manage and schedule replicas across the environment through integration with application agents. Replication Manager not only supports the replication of VMFS volumes, but it also supports the replication of a single virtual disk configured on the entire VMFS volume that resides on a single Celerra LUN. SRM is designed to provide crash consistency at the level of datastore, but when it is used with Replication Manager, application consistency is achieved. At this time, Replication Manager does not support an application-consistent replica of an Exchange Server database hosted in a VMFS datastore. This solution creates a crash-consistent copy of the Exchange database.

Figure 2 illustrates the Celerra and VMware vCenter SRM disaster recovery environment.

**Implement Replication Manager with VMware vCenter SRM**

By using Replication Manager for Celerra iSCSI in a VMware environment, an administrator can quickly configure Celerra Replicator sessions of iSCSI LUN-based VMFS datastores to simplify protection with VMware vCenter SRM. This section discusses the steps involved in the protection process.

**Celerra file system and iSCSI LUN sizing requirements**

Celerra can create point-in-time replicas of databases or file systems residing on supported storage arrays. Customers implementing solutions that use Celerra iSCSI replication technology are uncertain of the space required for the iSCSI replicas. It is important to determine the space requirements of the file systems accurately for local and remote replication so that you can use the available storage space optimally.

In most customer environments, Celerra iSCSI replicas are managed by using EMC Replication Manager. The sizing guidelines presented here are applicable to replications that are managed by using built-in Celerra iSCSI management tools or EMC Replication Manager.
EMC recommends virtually provisioned iSCSI LUNs for customer environments in a protect scenario. If you are using virtually provisioned iSCSI LUNs, it is recommended that you closely monitor the file system space to ensure that enough space is available. Enable the automatic file system extension option and set a conservative high water mark. Use the following formula when sizing the Celerra file system:

\[
FS_{\text{min}} \cong L + [(A + ((N-1)*C)) + [M*L]]
\]

<table>
<thead>
<tr>
<th>Variable</th>
<th>Long Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>FS_{\text{min}}</td>
<td>Minimum file system size</td>
</tr>
<tr>
<td>L</td>
<td>Published LUN size</td>
</tr>
<tr>
<td>A</td>
<td>Actual data size</td>
</tr>
<tr>
<td>N</td>
<td>Number of snapshots</td>
</tr>
<tr>
<td>C</td>
<td>Snapshot data change</td>
</tr>
<tr>
<td>M</td>
<td>Number of TWS</td>
</tr>
</tbody>
</table>

Sizing Considerations for iSCSI Replication on EMC Celerra on Powerlink® provides more information about sizing the Celerra system.

**Note:** File systems that contain virtually provisioned iSCSI LUNs support automatic file system extension. However, file systems that contain fully provisioned LUNs do not support automatic extension.

**Hardware and software configuration requirements**

Before implementing VMware vCenter SRM protection, address the hardware and software configuration requirements. This paper does not address the steps required to install the required hardware and software. Figure 3 shows the Exchange Server disaster recovery environment with VMware vCenter SRM and EMC Celerra NX4. VMware vCenter SRM is implemented by using Celerra NX4.

![Exchange environment with VMware vCenter SRM and Celerra](image)

**Figure 3** Exchange environment with VMware vCenter SRM and Celerra
Protected site
The protected site has the production vCenter that manages one or more VMware ESX servers. The ESX servers manage the VMFS datastores used for virtual machine Virtual Machine Disk Format (VMDKs) and virtual disk VMDKs.

Production Replication Manager proxy client
To replicate VMFS datastores, configure a Replication Manager “proxy” client into the Replication Manager environment. A Replication Manager proxy client is a Microsoft Windows 2003 host that has been added as a Replication Manager client and configured with access credentials for the production vCenter.

Production virtual machine hosts
The virtual machines at the production data center are the hosts that you must protect by using Replication Manager and VMware vCenter SRM. These include the Exchange 2007 mailbox server, Exchange HUB transport and Client Access server (CAS), Active Directory, Replication Manager server, and the Replication Manager proxy at the production site.

Recovery site
The recovery site includes the secondary vCenter that manages one or more ESX servers at the secondary data center.

Recovery Replication Manager proxy client
The secondary Replication Manager proxy client is configured for the secondary vCenter. When there is a VMware vCenter SRM failover, the secondary proxy client assumes the role of VMFS replications.

Recovery virtual machine hosts
Create an additional Exchange HUB/CAS server and Active Directory on the secondary side for high availability. This is a Microsoft best practice to create multiple HUB/CAS servers instead of replicating them for high availability.

Along with the Replication Manager client, install the Replication Manager console on a Windows host to connect to the Replication Manager server and perform Replication Manager operations.

Two important considerations are the availability of the Replication Manager console during the entire disaster recovery to perform the necessary Replication Manager operations, and the connectivity of the Replication Manager proxy client with the Celerra Data Mover.

Best practice: Install the Replication Manager console on both the primary and secondary proxy client or on a separate Windows server that does not form part of the disaster recovery configuration.

There are a few storage-specific configuration requirements. Each ESX server (protection and recovery side) must have LUNs masked to it from IQNs on both Celerra systems. For example, suppose the source LUNs on the production Celerra for VMFS are on Celerra A with IQN X, and the target LUNs on the destination Celerra are on Celerra B with IQN Y. In such a configuration, the ESX server hosting the production VMFS and the ESX server that will host the failover VMFS must each have at least one LUN masked to each ESX from Celerra A with IQN X and from Celerra B with IQN Y. It is also necessary to use Replication Manager to set up all Celerra Replicator links between the protection and recovery sites. Replication Manager cannot manage Celerra Replicator environments that were not created as a result of running a Replication Manager job.
Configure Replication Manager server disaster recovery

There is a possibility that Replication Manager server software is installed on a host that might get affected by a disaster. To avoid such a single point of failure, it is recommended that you implement a Replication Manager server disaster recovery solution in the environment. This section discusses this solution. *EMC Replication Manager Administrator’s Guide* on Powerlink provides a detailed description of the configuration.

**Best practice:** Implement Replication Manager server disaster recovery solution instead of a stand-alone Replication Manager server implementation in the environment. This prevents a single point of failure if the server hosting Replication Manager software gets affected by a disaster.

Primary Replication Manager server

The primary (or production) Replication Manager server is the host that coordinates the replication activity for the production environment. The primary server may be physically located in the same data center as the production vCenter environment and Celerra storage or it may be located in a separate environment. The primary Replication Manager server requires IP connectivity to the production vCenter and Celerra Data Movers.

When Replication Manager server software is installed on this host, ensure that you indicate this host as the “Primary” Replication Manager server during the installation process.

Secondary Replication Manager server

The secondary Replication Manager server is a standby server that can assume control of the replication environment in the event of a failure of the primary Replication Manager server. For disaster recovery purposes, the secondary Replication Manager server can be used if the primary Replication Manager server is involved in the disaster.

When Replication Manager server software is installed on this host, ensure that you indicate this host as the “Secondary” Replication Manager server during the installation process.

Interestingly, you can use the same hosts to install both the Replication Manager proxy client and Replication Manager server.

After you install Replication Manager software in the primary and secondary servers, configure the systems as indicated in the disaster recovery section of the *EMC Replication Manager Administrator’s Guide*. After the configuration is completed, test the Replication Manager server failover process by failing over to the secondary Replication Manager server, and then back to the primary Replication Manager server.

Configure VMFS and virtual disk replications

This section describes how to configure the Replication Manager application sets (appsets) and jobs to prepare for VMware vCenter SRM protection of the Exchange environment.

**Sample configuration**

No two environments are the same. Adjust the configuration based on the environment.
Table 1

<table>
<thead>
<tr>
<th>Production Replication Manager Server: ex3vrm01</th>
<th>Production Proxy Host: ex3vrm01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production VMware ESX Server 1: ex3esx01</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VMFS1: Store_MX VMFS</th>
<th>VMFS2-5: Store_db1, Store_db2, Store_db3 and Store_db4 VMFS</th>
<th>VMFS6-9: Store_log1, Store_log2, Store_log3 and Store_log4 VMFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1: ex3vmx01</td>
<td>VMDK1-4: D:, E:, F:, and G:\ for VM1 (Exchange DB)</td>
<td>VMDK5-8: L:, M:, N:, and O:\ for VM1 (Exchange DB Logs)</td>
</tr>
</tbody>
</table>

In this configuration as shown in Table 1, the production vCenter host is ex3pvc01. This vCenter manages one VMware ESX server ex3vmx01. The server ex3vmx01 manages nine Celerra iSCSI-based VMFS datastores VMFS1 to VMFS9 as shown in Figure 3 on page 11.

One VMFS is used to host the virtual Exchange Server and from the rest, eight VMDKs have been created. The eight VMDKs for the virtual machine are for Exchange Server databases and logs.

The production Replication Manager server is hosted on the virtual machine ex1vrm01. A Replication Manager proxy host is also created on the same machine.

Figure 4 provides a pictorial representation of this sample configuration.
Replication Manager application sets and jobs

To use SRM, protect all source LUNs on the source Celerra by using Celerra Replicator and Replication Manager. To protect virtual machines and Exchange databases and logs, the protection method you need to consider is “crash-consistent” replication of VMFS datastores.

With the above configuration, the administrator must set up application sets as follows:

**Virtual machine replication**

By using the Replication Manager console, connect to the production Replication Manager server and create a VMFS application set for the VMFS1 datastore by using ex1vrm01 as the proxy host for the replication. After the application set is defined, configure the jobs.

Based on the size of the VMFS and the link bandwidth between the source and target Celerra systems, it may require some time to complete the Celerra Replicator job. Copy the entire contents of the LUNs for the source VMFS to the target Celerra.

**Best practice:** Perform replications for production databases at planned, regular intervals to achieve the required RPO.

**Configure VMware vCenter SRM**

After you configure the Replication Manager jobs, you are ready to configure VMware vCenter SRM to protect your virtual machines and the virtual disk VMDK data that the virtual machines use. The following section discusses the tasks that are involved in configuring SRM. The Site Recovery Manager 1.0 Update 1 Administration Guide on the VMware website provides additional information to perform these operations.

Install VMware vCenter Site Recovery Manager plug-in

VMware vCenter Site Recovery Manager is a plug-in module that you can download from the VMware website. The plug-in creates a Site Recovery button on the vCenter console as shown in Figure 5. You must install the VMware vCenter Site Recovery Manager plug-in at the production and disaster recovery vCenter systems. Configure each vCenter such that it is aware of the other site. The vCenter at the production side is called the “protected” site, and the vCenter at the disaster recovery virtual center is called the “recovery” site.

**Figure 5 Protection site vCenter**

After you install the VMware vCenter Site Recovery Manager plug-in, download and install the Celerra Storage Replication Adapter (SRA) for SRM. The SRA enables VMware vCenter SRM to be aware of Celerra Replicator sessions and to communicate with Celerra.
Configure the protected and recovery sites

After you install the Celerra SRM adapter, you can configure the protected and recovery sites through vCenter. On both copies of vCenter, select VMware Site Recovery, and then define the connection between each copy. You must provide the name and credentials of the vCenter system at the other site. After the credentials are configured, VMware vCenter SRM establishes “reciprocity” between the two vCenter systems.

After the relationship is defined between the two vCenter systems, configure the array managers. Select Configure Array Manager to begin the process. On the protection-site vCenter, configure a protection-site array manager. This is the name, IP address, and credentials of the Celerra Control Station that contains the production file systems and LUNs. On the recovery site, configure the recovery-site array manager.

When you configure the array managers, each array is interrogated to determine which LUNs are configured in Celerra Replicator sessions with the other site Celerra. The current version of VMware SRM plug-in and Celerra SRA requires that each Celerra have Celerra Replicator sessions with only one other Celerra. Figure 6 shows the LUNs that were configured with Array Manager.

Protect the VMware environment

To protect the Exchange environment, perform the following steps:

- Create protection groups
- Create recovery plans
- Guest OS customization for virtual machines (optional)
Create protection groups
A protection group is configured on the protection-site vCenter. In the Site Recovery main window, right-click Protection Groups, and then select Create Protection Group. If the Create Protection Group option is not enabled, there are two possibilities:

- There is a configuration problem between the protection-site and recovery-site vCenter systems.
- The Celerra Replicator relationship between the two Celerra systems is incomplete.

You can run the Configure Array Manager option again to reconfigure the protection-site and recovery-site arrays.

If you suspect that the Celerra Replicator session relationships are incomplete, return to Replication Manager to verify the application sets and jobs. Verify if the target storage in all Celerra Replicator jobs refer to the same target Celerra system.

If the Create Protection Group action is enabled, select this option to create the protection group. In the subsequent windows, you are asked to supply the protection group name and also select from a list of VMFS volumes that are eligible for VMware SRM protection. During the creation of the protection groups, VMware vCenter SRM requires a placeholder location to store some temporary vCenter inventory files for the protected virtual machines. VMware vCenter SRM presents the available datastores that you can select at the recovery site for storing these temporary files as shown in Figure 7.

Figure 7 Protection group – Select datastore for temporary files
Enter the remaining details and complete the definition of the protection group. You need to configure the protection group (Figure 8 on page 18) by providing all recovery-site resource information that the virtual machine can use in a failover situation.
Best practice:
- Ensure that no Replication Manager replicas of the protection site are mounted when you create a protection group.
- It is preferable and suggested that you select a non-replicated datastore for the temporary files at the recovery site.

Create a recovery plan
After you define the protection group, you can create the recovery plan on the recovery-site vCenter. Subsequently, you are asked to select the name of the protection groups to be connected to the recovery plan. You can include one or more protection groups in the plan. If the protection group you defined in the previous step is not listed in the recovery plan, there is a configuration issue. Verify if the protection group is defined. After selecting the protection groups, proceed to set the response times for the virtual machines in the plan and select the network during the recovery tests. This response time, as shown in Figure 9, is very important. By default, it is 5 minutes. Modify it depending on the virtual machine resources and the network configuration.
You can also select “Auto” from the Test Network list box to create an isolated network for recovery tests. On the last dialog box of the Recovery Plan wizard, select the local virtual machines that need to be suspended when the plan is tested or run and complete the recovery plan configuration.

For the sample configuration, a recovery plan named Exchange Server has been created, which includes the protection group defined earlier.

**Specify the guest OS customization**

SRM can customize the guest OS network settings after a failover at the recovery site. You can bring the virtual machines online with different network settings based on the network configuration of the recovery site. In the recovery-site vCenter, select **Customization Specifications** (Figure 10) from the Edit menu option and work through the wizard.

![Customization Specifications](image)

**Figure 10 Customization Specifications**

Ensure that you select the correct target virtual machine OS and provide a name for the virtual machine customization profile in the Customization Specifications information. When the protected virtual machine is restarted on the recovery site after an actual failover, the only information retained by SRM is the information entered against network properties. Different IP addresses from the production site are used, as shown in **Figure 11** on page 20, and all other information remains the same.
Perform disaster recovery operations

After you create the recovery plan, the production VirtualCenter environment is protected from disaster. As with all disaster recovery plans, test the failover to the recovery-site VirtualCenter. With SRM, you can test the disaster recovery setup without affecting the production environment.
Test a failover

To test the disaster recovery plan that is implemented, test the following failover scenario: Protection Group Failover using the VMware vCenter SRM recovery plan

Protection Group Failover using the VMware vCenter SRM recovery plan

VMware vCenter SRM does not automatically trigger the failover of a recovery plan, rather human intervention is required to evaluate and declare a disaster, and then the recovery plan is initiated within VMware vCenter SRM from the recovery-side data center. Therefore, end-user tasks to test VMware vCenter SRM failover are similar to those for actual failover.

Test failover

Test failover is a great feature to prepare for an actual failover. To test if the recovery plan has been set up correctly for the protected virtual machines, you can execute “Test” from the Site Recovery tab of the recovery-site vCenter. With the test recovery, you can test a recovery plan by simulating a failover of virtual machines from the protected site to the recovery site. The benefit of using VMware vCenter SRM to run a failover simulation against a recovery plan is that it allows you to confirm that the protected virtual machines start in the correct order, taking into account the various application-service dependencies for the protected virtual machines in the environment.

Interestingly, when you select the option to test a recovery plan through VMware vCenter SRM, the simulated failover is executed in an isolated environment that includes network and storage infrastructure at the recovery site. This infrastructure is isolated from the protected site (production environment), which ensures that the protected virtual machines at the protected site are not subject to any kind of service interruption during the testing of the recovery plan.

While the simulated failover test is running as shown in Figure 13 on page 22, you can monitor the status of each step that forms part of the recovery plan by using the Recovery Steps tab in the VI Client. It provides information about the steps that are currently running in addition to the steps that were completed with a “Success” status. There are a few steps (for example, shutting down the protected virtual machines if they are accessible) that run only during an actual recovery, and a few steps (for example, cleanup of virtual machines, reset storage, and so on) that run only during a test recovery. This is mentioned in the “Mode” column. Also, during failover testing, the disaster recovery file system space grows because of the mounted snaps. Hence, it is very important that you size it accordingly.

The simulated failover ends by resetting the environment, preparing it for the next event that might be another simulated failover or an actual failover for a scheduled business continuity/disaster recovery test or in response to an event that resulted in the business declaring a disaster. After the simulated failover test completes a report of the test run, you can view it from the History tab.
Run recovery plan

You can execute a recovery plan for the actual VMware vCenter SRM failover through the Run option on the Site Recovery tab of the recovery-site vCenter.

At this time, the Run Recovery Plan dialog box warns you that you are about to run a recovery plan that results in changes to the protected virtual machines and the infrastructure of both the protected and recovery site data centers. Select the provided option to confirm that you understand the implications of running the recovery plan, and then click Run Recovery Plan to start the failover of the protected virtual machines from the protected site to the recovery site. The Run Recovery Plan dialog box also provides a summary of the recovery plan information, which includes the recovery plan that is going to be run along with the names of the protected and recovery sites, the number of protected virtual machines that will be failed over in addition to a connectivity status from the recovery site back to the protected site.

When the failover is executed as shown in Figure 14 on page 23, you can monitor the status of each step that makes up the recovery plan by using the Recovery Steps tab of the recovery site’s VI Client, which provides information regarding steps that are currently running in addition to the steps that were completed with a “Success” status.
During the actual failover, VMware vCenter SRM performs the following tasks:

1. Powers down the protected virtual machines if there is connectivity between sites and if they are available.
2. Suspends data replication and enables read/write operations to the replicated datastores.
3. Rescans the ESX servers at the recovery site.
4. Registers the replicated protected virtual machines.
5. Shuts down non-essential virtual machines at the recovery site to free resources for the protected virtual machines being failed over.
6. Completes power-up of the replicated protected virtual machines in accordance with the recovery plan.

After a successful failover, Exchange Server comes back online in the recovery site with the new network configurations as shown in Figure 15 on page 24.
Best practice: Do not perform any Replication Manager operation for the production appsets such as replication, mount, unmount, or restore during the failover operation. It is recommended that you disable Replication Manager job schedules planned to execute during this time.

**Post-failover actions**

After the execution of all steps in the recovery plan, you need to perform a few additional tasks to complete the failover and bring the configurations to a proper consistent state. These tasks and their purposes are discussed below.

**Recovery-site vCenter operations**

During a VMware vCenter SRM failover, datastores that fail over to the recovery-site vCenter are renamed with a prefix such as “snap-xxxxx” as shown in Figure 15. These prefixes are not needed and may interfere with the failback or Replication Manager operations. As such, these VMFSs should be renamed to the original datastore names because they were on the production vCenter.

VMware vCenter SRM does not support automatic failback. This restriction limits the reusability of the recovery plan on this vCenter. Hence, delete the recovery plan.

When a Celerra Replicator job is run, it creates a VMware snapshot of the virtual machine before the remote LUN is updated. After the replication is complete, the snapshot is removed on the production side, but not on the replicas, and the Celerra clone on the recovery-site Celerra is a replica. As a result, after a VMware vCenter SRM failover, the failed-over virtual machine has a VMware snapshot. You can remove or rename this snapshot.

**Best practice:** After a VMware vCenter SRM failover, you can rename or remove the VMware snapshots of the failed-over virtual machines on the recovery vCenter to reclaim the corresponding used space.

**Protection-site vCenter operations**

If the protection-site vCenter is still available and accessible, you must remove the protection group from it. During a VMware vCenter SRM failover, Celerra sessions are failed over making the source LUNs as destination and vice versa. As a result, the LUNs previously accessible to the protection vCenter for protection group resources become read-only and hence, inaccessible for the protection vCenter. Therefore, you must rescan the iSCSI software host bus adapter (HBA) of the affected VMware ESX to remove the failed-over datastores. Subsequently, remove the failed-over virtual machines from the vCenter inventory. These steps are necessary if you want to perform a failback at a later stage.
Failover Replication Manager replicas
Replication Manager cannot automatically detect a VMware vCenter SRM failover and requires certain actions to be performed by the user before it can be used for replications in the failed-over environment.

As it is created before the VMware vCenter SRM failover, there must be one clone replica in the Replication Manager database for the VMFS-hosting virtual machine and the Microsoft Exchange Server database and logs. For this Replication Manager clone replica, which is involved in the VMware vCenter SRM failover, right-click the clone replica and select Perform Post SRM Failover Steps. Subsequently, a dialog box appears with a message to confirm if a VMware vCenter SRM failover has occurred and whether Replication Manager should continue with post VMware vCenter SRM failover steps. Respond affirmatively to proceed.

For clone replica, the VMware vCenter SRM post-failover steps involve assigning a new proxy host that is configured for the recovery-site vCenter. Replication Manager configures the existing VMFS appsets and jobs to use the new proxy host so that they can be used to create new replicas in the failed-over environment. It also allows you to use the existing replicas for Replication Manager operations such as mount and restore.

You can configure Replicator Manager jobs in the recovery-site Replication Manager server to replicate the failed-over VMFS volumes. No previous existing replications are lost if the original Celerra is still available and jobs have been reconfigured properly. Celerra Replicator (remote) replicas that existed before the VMware vCenter SRM failover are now considered local replicas and may be restored to the failed-over VMFS or mounted.

At this point, if it is assumed that the production side is still unavailable, the configuration looks similar to the representation shown in Figure 16.

Prepare for failback
If the original production Celerra is operational, you must fail back to the protected site to complete the testing of the disaster recovery plan. However, VMware vCenter SRM does not support automated
failback. Hence, you can consider failback operation as another failover operation from the recovery site to the protected site.

Before proceeding with failback, as mentioned in the previous sections, you must reconfigure the required Celerra Replicator jobs to point to the original Celerra. You must also run these jobs at least once so that it incrementally establishes the sessions to the original Celerra. At the completion of replication, you must perform a rescan of the iSCSI software HBA on the VMware ESX servers hosting the protected datastores. After this, you can proceed to rebuild VMware vCenter SRM protection groups and recovery plans from the recovery site back to the protected site and conduct the failover process in the same manner as the full failover test discussed in the previous sections of this document.

Conclusion
VMware vCenter SRM integrates very closely with Celerra arrays, VMware infrastructure, and the Microsoft Exchange Server application for an easy implementation of a disaster recovery solution by using EMC Replication Manager. This white paper highlighted the ways in which SRM can be leveraged in a better way for additional benefits such as:

- Removing the burden of manually configuring and managing Celerra replications
- Achieving a crash-consistent replica of the production Exchange server by using Replication Manager (Replication Manager does not support application consistency with the Exchange database residing on VMware VMFS)
- Reusing existing replicas post-failover with little configuration for restore and mount operations
- Facilitating quick reconfiguration of jobs and creation of Celerra sessions for a faster failback
- Improving the RPO and RTO through a completely automated failover process with minimal manual intervention
- Nondisruptively testing the recovery plan, making it easier for the administrator to manage the disaster recovery process

The configuration suggestions and best practices discussed in this paper facilitate the implementation of a rapid, reliable, and easily manageable disaster recovery solution in similar environments.

References
The following documents on Powerlink provide additional relevant information:

- EMC Business Continuity for Microsoft Exchange 2007 enabled by EMC Celerra and VMware SRM — Build Document
- Optimizing Disaster Recovery with VMware Site Recovery Manager and EMC Celerra Replicator V2 — Applied Technology
- VMware ESX using EMC Celerra Storage Systems TechBook
- EMC Replication Manager Version 5.2 Administrator’s Guide
- Using Celerra Replicator (V2) — Technical Module

The following documents about VMware Virtual Infrastructure 3 and SRM are available on the VMware website:

- VMware Infrastructure 3 Documentation
- Site Recovery Manager 1.0 Update 1 Administration Guide