VMware Site Recovery Manager 5.0

Best Practices

Dell Compellent

Document revision

Date	Revision	Comments
8/23/2011	A	Initial Draft
11/17/2011	B	Updated for 5.5.4
12/6/2011	C	Replication sections
3/22/2012	D	SRA version correction
7/2/2012	E	Added warning; spelling

THIS BEST PRACTICES GUIDE IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Contents

Document revision 2

Contents 4

- General syntax 7
- Conventions 7

Preface 8

- Audience 8
- Purpose 8
- Customer support 8

Introduction 9

- Introduction to Site Recovery Manager 9
- What’s New in SRM 5.0 9

Setup Prerequisites 10

- Enterprise Manager 10
- Storage Center 10
- VMware 10
- Storage Replication Adapter (SRA) 10

Site Recovery Manager Architecture 11

- Single Protected Site 11
- Multiple Protected Sites 12

Enterprise Manager Configuration 13

- Data Collector Configuration 13
- Enterprise Manager Logins 13
- Creating dedicated SRA access accounts 13
- Saving Restore Points 14
- Validating Restore Points 16
- Automatic Restore Point Saving Schedule 17

Configuring Replications 18

- Asynchronous Replications (Supported) 18
- Synchronous Replications (Not Supported) 18
- Live Volume Replications (Not Supported) 18
- Data Consistency while Replicating by Replay Schedule 19
- Data Consistency while Replicating the Active Replay 20
- Replication Dependencies and Replication Transfer Time 21

Custom Recovery Tasks 22
Site Recovery Manager Configuration 23
Configuring the Array Managers 23
Creating Array Pairs 25
Rescanning Array Managers 27
Creating Protection Groups 28
Creating Recovery Plans 29
Recovery Plan Execution 31
Testing a Recovery Plan 31
Running a Recovery Plan 31
Reprotect and Failback 33
Overview 33
Reprotection 33
Failback 35
Conclusion 36
Appendix A – Example Scripts 37
Appendix B – Additional Resources 39
Compellent Resources 39
VMware Resources 39

Tables

Table 1. Document syntax 7

Figures

Figure 1. Single Protected Site Configuration 11
Figure 2. Multiple Protected Site Configuration 12
Figure 3. Managed Storage Centers in Enterprise Manager 13
Figure 7. Validating Restore Points in Enterprise Manager 16
Figure 8. Review Restore Points in Enterprise Manager 16
Figure 9. Configure Automatic Restore Point Saving and Validation 17
Figure 10. Steps during a recovery when replicating via replay schedule 19
Figure 11. Steps during a recovery when replicating the active replay. 20
Figure 12. Replications completing within non-concurrent timeframes 21
Figure 13. Adding a custom pre-power on script to a recovery plan 22
Figure 14. Configure Array Managers for both sites 23

Figure 15. Add an Array Manager for each site 24
Figure 16. Specify privileged credentials for the Array Manager 24
Figure 17. Array Pairing 25
Figure 18. Array Managers at each site need to be paired........ 25
Figure 19. Pairing in a Primary and Remote Enterprise Manager configuration........ 26
Figure 20. Refreshing Array Managers for added or removed devices 27
Figure 21. Replicate recent changes option 29
Figure 22. Adding Prompts to the Recovery Plan 30
Figure 23. Test the Recovery Plan 31
Figure 24. Running a Recovery to execute a Planned Migration or Disaster Recovery or Plan 31
Figure 25. Running the Planned Migration or Disaster Recovery warning message 32
Figure 26. A successfully completed Recovery is ready for Reprotect 33
Figure 27. Reprotecting virtual machines workflow in SRM 5.0........ 34
Figure 28. SRM 5.0 reverses device/datastore/volume replication during a Reprotect 34

General syntax

Table 1. Document syntax

Item	Convention
Menu items, dialog box titles, field names, keys	**Bold**
Mouse click required	Click:
User Input	`Monospace Font`
User typing required	Type:
Website addresses	http://www.compellent.com
Email addresses	info@compellent.com

Conventions

Note

Notes are used to convey special information or instructions.

Timesaver

Timesavers are tips specifically designed to save time or reduce the number of steps.

Caution

Caution indicates the potential for risk including system or data damage.

Warning

Warning indicates that failure to follow directions could result in bodily harm.

Preface

Audience

The audience for this document is System Administrators who are responsible for the setup and maintenance of VMware Site Recovery Manager, VMware vSphere, and associated storage. Readers should have a strong working knowledge of SRM, vSphere, Dell Compellent Storage Center and Enterprise Manager.

Purpose

This document provides an overview of VMware Site Recovery Manager and introduces best practice guidelines for configuring SRM and the SRA when using the Dell Compellent Storage Center.

Customer support

Dell Compellent provides live support 1-866-EZSTORE (866.397.8673), 24 hours a day, 7 days a week, 365 days a year. For additional support, email Dell Compellent at support@compellent.com. Dell Compellent responds to emails during normal business hours.

Introduction

Introduction to Site Recovery Manager

This document will provide configuration examples, tips, recommended settings, and other storage guidelines a user can follow while integrating VMware Site Recovery Manager with the Compellent Storage Center. This document has been written to answer many frequently asked questions with regard to how VMware interacts with the Site Recovery Manager, as well as basic configuration.

Compellent advises customers to read the Site Recovery Manager documentation provided on the VMware web site before beginning their SRM implementation.

Note: The information contained within this document is intended only to be general recommendations and may not be applicable to all configurations. There are certain circumstances and environments where the configuration may vary based upon your individual or business needs.

What’s New in SRM 5.0

- **New User Interface (UI) -** Management of the primary and secondary SRM sites is consolidated from two separate interfaces down to one with both sites being visible in one vSphere Client without linked mode.
- **Planned Migration -** SRM can now be used as a tool to gracefully migrate protected virtual machines from the primary to secondary site.
- **Reprotect and Failback -** Once virtual machines are moved from one site to another via planned migration or disaster recovery, the VM reprotection process is automated and includes reverse replication which enables VMs to fail back to the oppoisite site.
- **vSphere Host-Based Replication (optional) -** A new appliance is introduced which has the ability to provide host based replication for VMs on a per-VM granular basis, abstracting the physical attributes for the storage such as array type and protocol.
- **Faster IP Customization -** Reconfiguring TCP/IP via recovery plan is more efficient and executes faster.
- **New Shadow VM Icons -** Provides better visibility at the secondary site for placeholder VMs.
- **In Guest Scripts -** Script automation can now be generated from within guest VMs themselves.
- **VM Dependency -** 5 Priority Groups and VM dependency relationships within protection groups.
- **Improved Reporting -** Provides increased awareness for historical analysis.
- **IPv6 -** Future proof network design.

Setup Prerequisites

Enterprise Manager

Compellent Enterprise Manager Version 5.5.4 or greater is required for the Storage Replication Adapter (SRA) to function. The SRA makes calls directly to the Enterprise Manager Data Collector to manipulate the storage. It is recommended to have the latest version of the Enterprise Manager Data Collector installed to ensure compatibility with SRM 5.0.x and the Compellent SRA.

Storage Center

It is required to have two Compellent Storage Center (version 5.4 or greater) systems with Remote Data Instant Replay (replication) between the sites licensed and operational. Site Recovery Manager cannot function without two Compellent systems replicating between each other.

VMware

VMware Site Recovery Manager 5.0.x with vCenter 5.0, ESXi 5.0 and/or ESXi/ESX 3.5 or newer are required. Please check the latest Site Recovery Manager Compatibility Matrix for the versions of software required for SRM to function.

Storage Replication Adapter (SRA)

The Compellent Storage Replication Adapter (SRA) is required to be running version 5.5.3 or greater.

Site Recovery Manager Architecture

Single Protected Site

This configuration is generally used when the secondary site does not have any virtual machines that need to be protected by SRM. In this example, the secondary site functions solely for disaster recovery purposes.

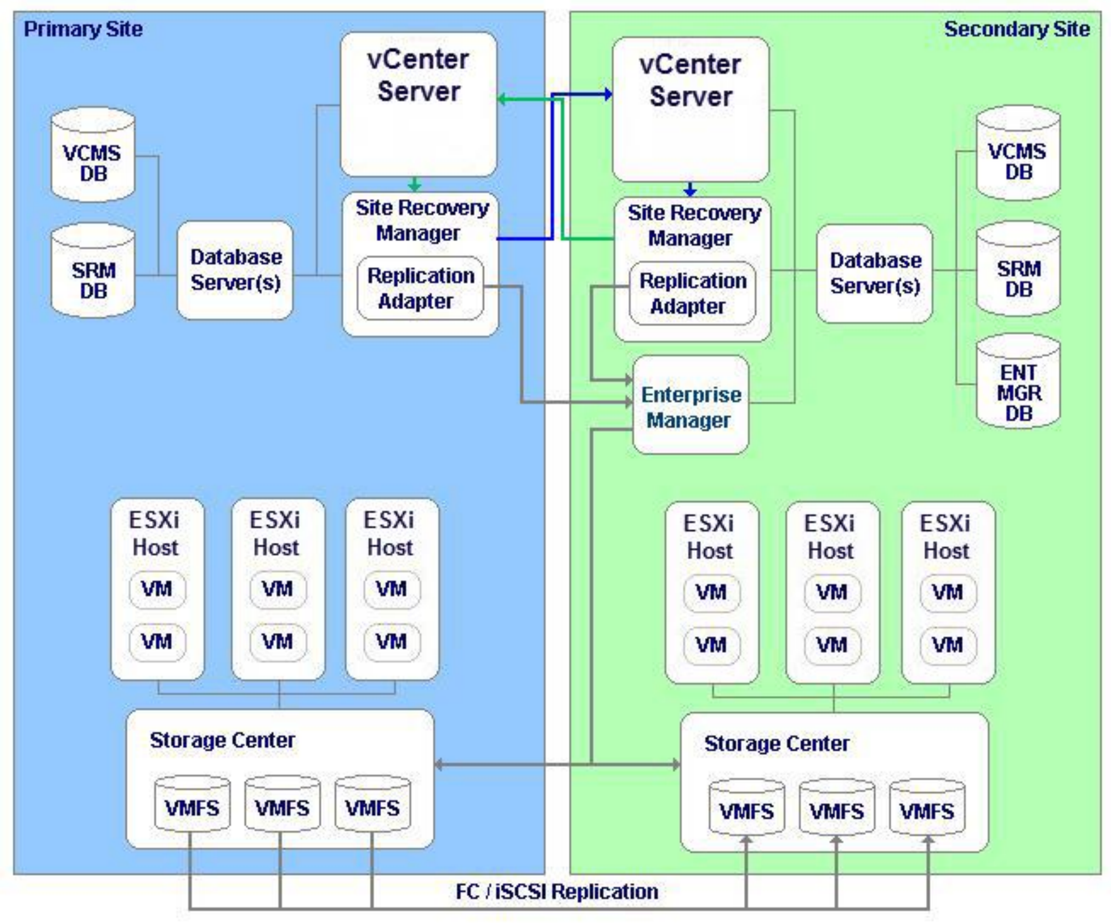


Figure 1. Single Protected Site Configuration

Note

Note: In this configuration, the Enterprise Manager Data Collector Server is placed at the disaster recovery site because it is required by SRM to perform recovery functions.

Caution

Caution: An Enterprise Manager Data Collector Server needs to be running at the site opposite of protected virtual machines in the event of a site failure for SRM to function. Keep this in mind if you are planning on using SRM 5.0’s new planned migration or failback feature.

Multiple Protected Sites

This configuration is generally used when both sites have virtual machines that need to be protected by SRM. This scenario may be commonly used in conjunction with SRM assisted migrations which is a new feature in SRM 5.0. In this example, each site replicates virtual machines to the opposing site in order to protect both sites from a failure or to orchestrate a planned migration of virtual machines. Planned migrations can be performed with just one Enterprise Manager Data Collector server. However, once there are active virtual machines running simultaneously at both the primary and secondary sites, the site with the Enterprise Manager Data Collector will not be adequately protected by SRM.

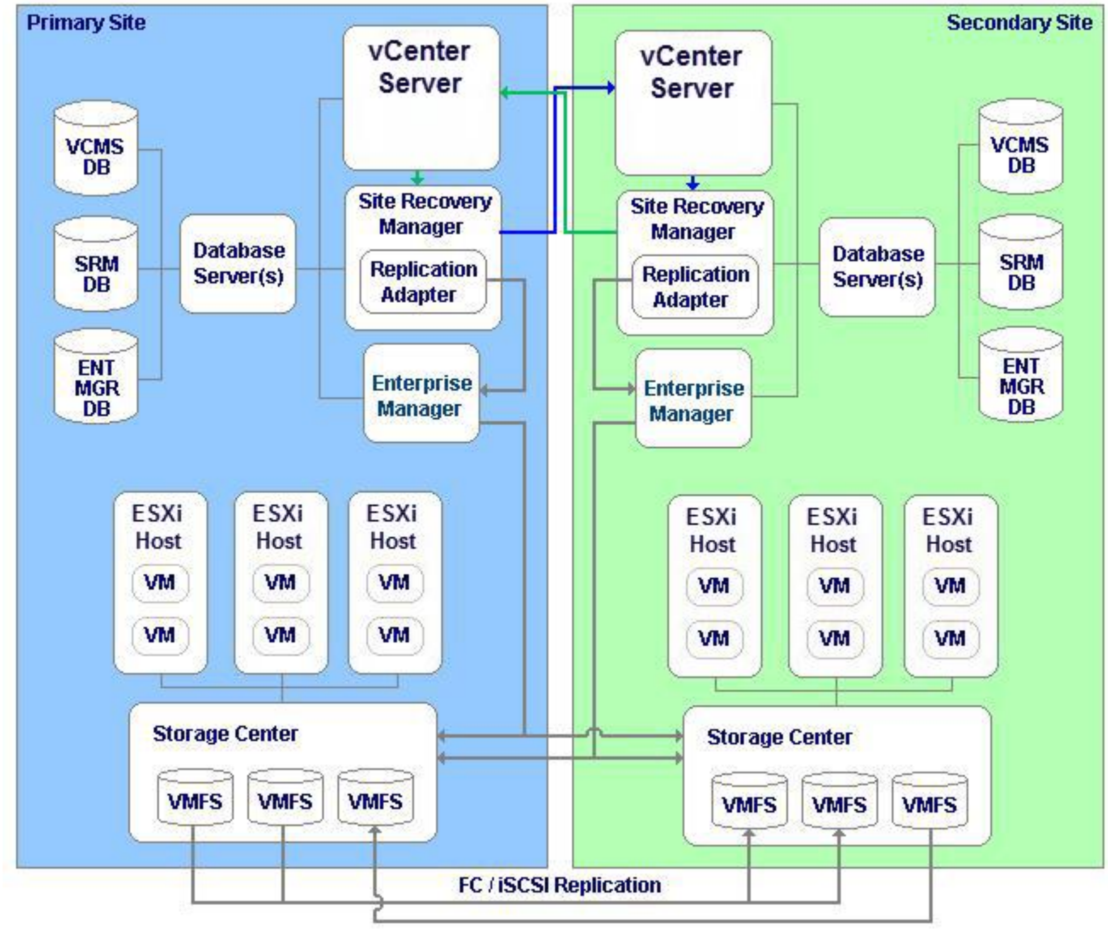


Figure 2. Multiple Protected Site Configuration

Note

Note: In this configuration, multiple Enterprise Manager Data Collector Servers are placed at each site so that either site can fail.

Caution

Caution: An Enterprise Manager Data Collector Server needs to be running at the site opposite of protected virtual machines in the event of a site failure for SRM to function. Keep this in mind if you are planning on using SRM 5.0's new planned migration or failback feature.

Enterprise Manager Configuration

Data Collector Configuration

As illustrated in the Architecture section, Enterprise Manager is a critical piece to the SRM infrastructure because the Data Collector processes all of the calls from the Storage Replication Adapter (SRA) and relays them to the Storage Centers to perform the workflow tasks.

Deciding whether or not to use one or two Enterprise Manager Servers depends on whether virtual machines need to be protected in one or multiple sites.

- If protecting virtual machines at a single site, a single Enterprise Manager Data Collector will suffice, and it is highly recommended that it be placed at the recovery site.
- If protecting virtual machines at both sites, it is highly recommended to place Enterprise Manager Data Collectors at each site.

Enterprise Manager Logins

For SRM to function, the Storage Replication Adapter (SRA) must use Enterprise Manager Login credentials that have rights to both of the Storage Center systems replicating the virtual machine volumes.

For example, if Storage Center SC12 is replicating virtual machine volumes to Storage Center SC13, the credentials that the SRA uses must have Administrator privileges to both systems.

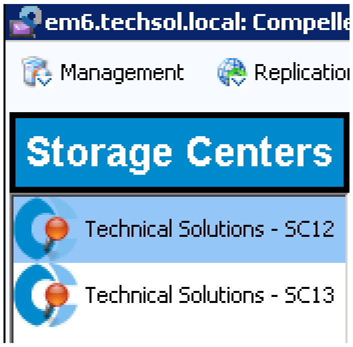

em6.techsol.local: Compelle
Management
Replicatio
Storage Centers
Technical Solutions - SC12
Technical Solutions - SC13

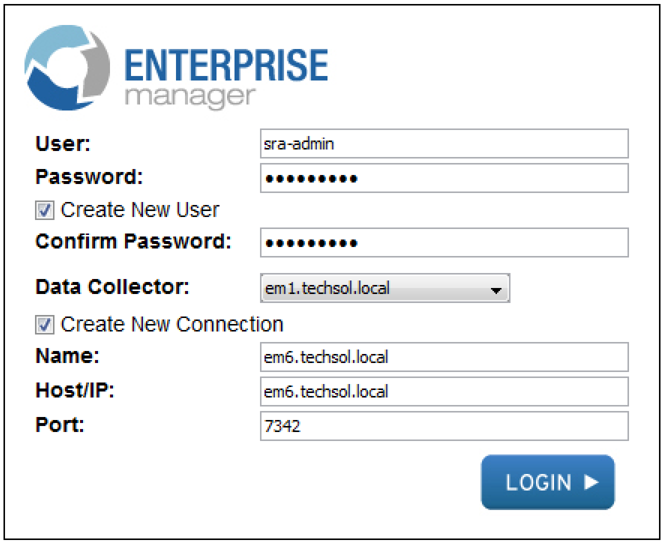
Figure 3.   Managed Storage Centers in Enterprise Manager

Creating dedicated SRA access accounts

For the SRA to have uninterrupted access to both arrays through the Enterprise Manager Data Collector, it is recommended to create dedicated accounts for SRM. Using dedicated accounts on each array will ensure that service is not disrupted due to a user changing their password.

Following the example above:

- Create an account named “sra-service-acct” on both the protected site array and the recovery site array.
    - This account needs Administrator privileges, so make sure the password assigned is secure.
    - For added security, you could create different accounts on both systems with different passwords. For example, on the protected array it could be named “sra-system1” and the secondary system it could be named “sra-system2”. The account names and passwords are arbitrary.
- Create a new account within Enterprise Manager named “sra-admin”.
    - Log into the Enterprise Manager client as the “sra-admin” account, and then add both Storage Center systems to be managed using the “sra-service-acct” usernames and passwords.



User: sra-admin
Password: ●●●●●●●●●
☑ Create New User
Confirm Password: ●●●●●●●●●
Data Collector: em1.techsol.local
☑ Create New Connection
Name: em6.techsol.local
Host/IP: em6.techsol.local
Port: 7342

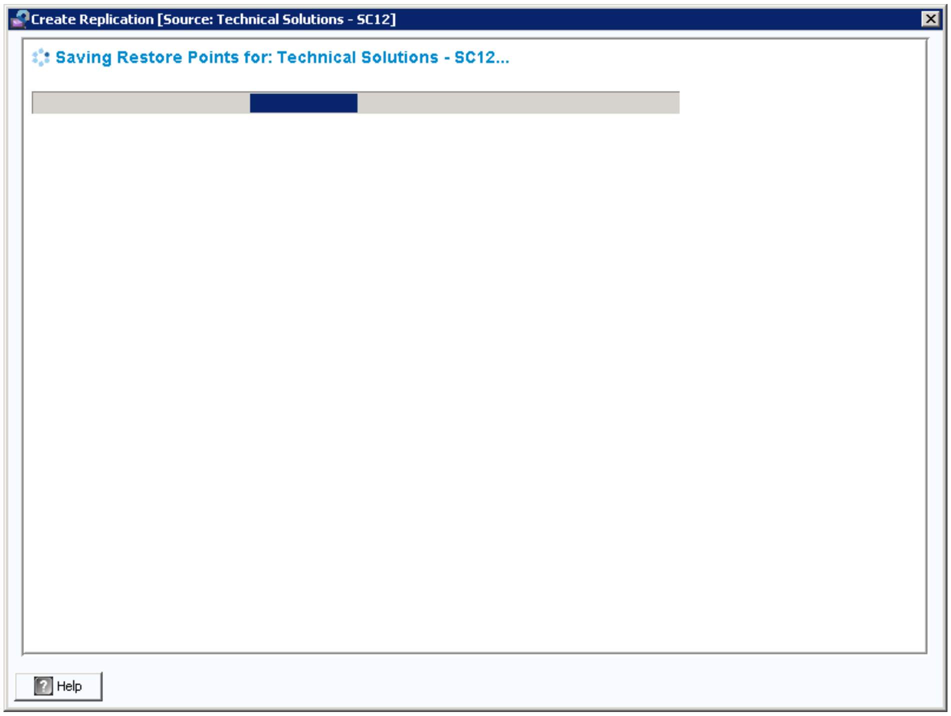
Figure 4. Creating a new Enterprise Manager account

The “sra-admin” account used to access Enterprise Manager can now be used for configuring the Storage Center credentials within SRM.

Saving Restore Points

Saving restore points must be completed for the SRA to be able to query the active replications, and can be initiated one of two ways:

1. For convenience, it is automatically initiated at the end of the **Create Replication Wizard**:



Saving Restore Points for: Technical Solutions - SC12...

Figure 5. Saving Restore Points in the Create Replication Wizard

2. From the **Enterprise Manager Replication Recovery** menu:

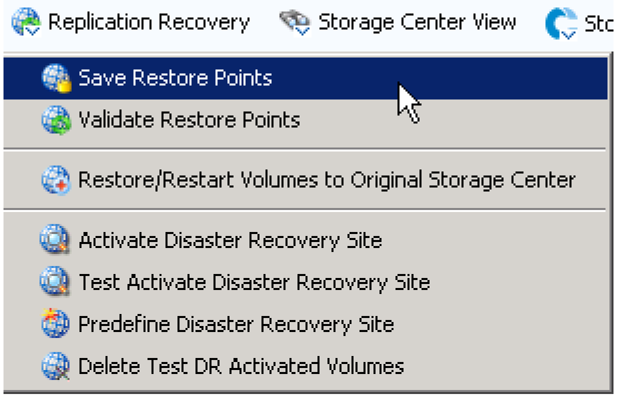

Replication Recovery
Storage Center View
Stc
Save Restore Points
Validate Restore Points
Restore/Restart Volumes to Original Storage Center
Activate Disaster Recovery Site
Test Activate Disaster Recovery Site
Predefine Disaster Recovery Site
Delete Test DR Activated Volumes

Figure 6. Saving Restore Points manually in Enterprise Manager for all managed Storage Center arrays

Note

Note: A Save Restore Points should be performed after a major SRM event such as performing a Planned Migration or Disaster Recovery.

Validating Restore Points

Restore Points can be quickly validated from the **Enterprise Manager Replication Recovery** menu:

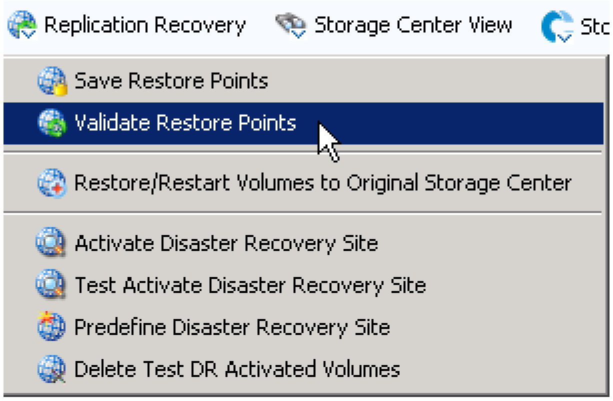
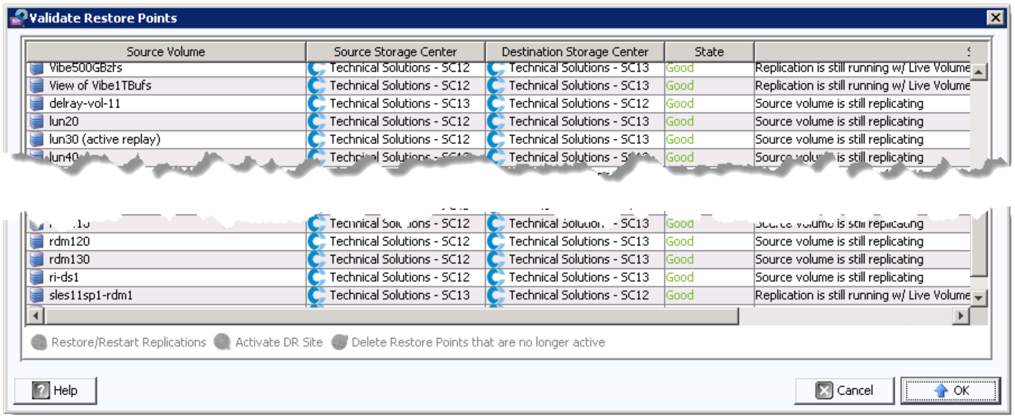

Replication Recovery
Storage Center View
Stc
Save Restore Points
Validate Restore Points
Restore/Restart Volumes to Original Storage Center
Activate Disaster Recovery Site
Test Activate Disaster Recovery Site
Predefine Disaster Recovery Site
Delete Test DR Activated Volumes

Figure 7. Validating Restore Points in Enterprise Manager

Review Restore Points and current state. Optionally delete inactive Restore Points which are no longer needed:



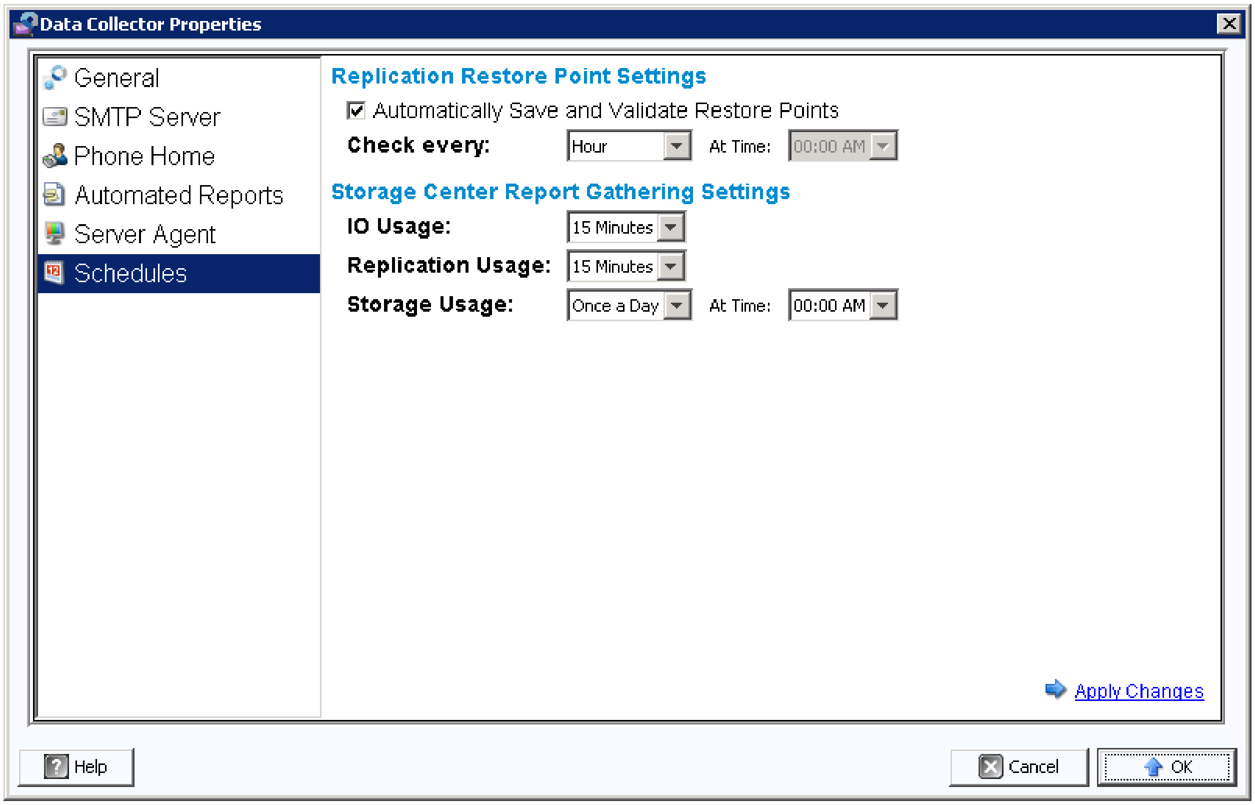
Source Volume	Source Storage Center	Destination Storage Center	State	S
Vibe500GBzfs	Technical Solutions - SC12	Technical Solutions - SC13	Good	Replication is still running w/ Live Volume
View of Vibe1TBufs	Technical Solutions - SC12	Technical Solutions - SC13	Good	Replication is still running w/ Live Volume
delray-vol-11	Technical Solutions - SC13	Technical Solutions - SC12	Good	Source volume is still replicating
lun20	Technical Solutions - SC12	Technical Solutions - SC13	Good	Source volume is still replicating
lun30 (active replay)	Technical Solutions - SC12	Technical Solutions - SC13	Good	Source volume is still replicating
lun40	Technical Solutions - [illegible]	Technical Solutions - S[illegible]	Good	Source volume is still replicating
[illegible]1o	Technical Solutions - SC12	Technical Solutions - SC13	Good	Source volume is still replicating
rdm120	Technical Solutions - SC12	Technical Solutions - SC13	Good	Source volume is still replicating
rdm130	Technical Solutions - SC12	Technical Solutions - SC13	Good	Source volume is still replicating
ri-ds1	Technical Solutions - SC12	Technical Solutions - SC13	Good	Source volume is still replicating
sles11sp1-rdm1	Technical Solutions - SC13	Technical Solutions - SC12	Good	Replication is still running w/ Live Volume

Restore/Restart Replications
Activate DR Site
Delete Restore Points that are no longer active
Help
Cancel
OK

Figure 8. Review Restore Points in Enterprise Manager

Automatic Restore Point Saving Schedule

The **Finish saving Restore Points** screen in the **Save Restore Points Wizard** has the option to save restore points automatically at a selected interval by clicking on the **Set Replication Restore Schedule** link. It is recommended to configure the data collector to save the restore points **hourly**. This helps to ensure that the most current restore points are available for the SRA to query for replication information.



Replication Restore Point Settings

☑ Automatically Save and Validate Restore Points

Check every: Hour At Time: 00:00 AM

Storage Center Report Gathering Settings

IO Usage: 15 Minutes

Replication Usage: 15 Minutes

Storage Usage: Once a Day At Time: 00:00 AM

Figure 9. Configure Automatic Restore Point Saving and Validation

Note: If using multiple Enterprise Manager Data Collectors, the first Data Collector is configured as the Primary. The second Data Collector is installed and configured as a Remote Data Collector. Restore points are saved on the Primary Data Collector and replicated to the Remote Data Collector at one minute intervals. Replications must be created and Restore Points saved before the volume can be protected by SRM. Non-replicated volumes won't be discovered as a device by SRM and thus cannot be protected.

Configuring Replications

Storage Center replication in coordination with Site Recovery Manager can provide a robust disaster recovery solution. Since each replication method affects recovery differently, choosing the correct method to meet business requirements is important. Here is a brief summary of the different options.

Asynchronous Replications (Supported)

- In an asynchronous replication, the I/O needs only be committed and acknowledged to the source system, so the data can be transferred to the destination in a nonconcurrent timeframe. There are two different methods to determine when data is transferred to the destination:
    - **By replay schedule** – The replay schedule dictates how often data is sent to the destination. When each replay is taken, the Storage Center determines which blocks have changed since the last replay (the delta changes), and then transfers them to the destination. Depending on the rate of change and the bandwidth, it is entirely possible for the replications to "fall behind", so it is important to monitor them to verify that the recovery point objective (RPO) can be met.
    - **Replicating the active replay** – With this method, the data is transferred "near real-time" to the destination, usually requiring more bandwidth than if the system were just replicating the delta changes in the replays. As each block of data is written on the source volume, it is committed, acknowledged to the host, and then transferred to the destination "as fast as it can". Keep in mind that the replications can still fall behind if the rate of change exceeds available bandwidth.
- Asynchronous replications usually have more flexible bandwidth requirements making this the most common replication method.
- One of the benefits of an asynchronous replication is that the replays are transferred to the destination volume, allowing for "check-points" at the source system as well as the destination system.

Synchronous Replications (Not Supported)

- The data is replicated real-time to the destination. In a synchronous replication, an I/O must be committed on both systems before an acknowledgment is sent back to the host. This limits the type of links that can be used, since they need to be highly available with low latencies. High latencies across the link will slow down access times on the source volume.
- The reason that this method is not supported is because replays on the source volume are not replicated to the destination, and any disruption to the link will force the entire volume to be re-replicated from scratch.

Live Volume Replications (Not Supported)

- Live Volume replications add an additional abstraction layer to the replication allowing mapping of the same volume through multiple Storage Center systems.
- Live Volume replications are not supported due to the fact that using them with SRM is mutually exclusive, and because SRM may be confused by the volume being actively mapped at two different sites.

Data Consistency while Replicating by Replay Schedule

When replicating by replay schedule here are the consistency states of replications during plan execution.

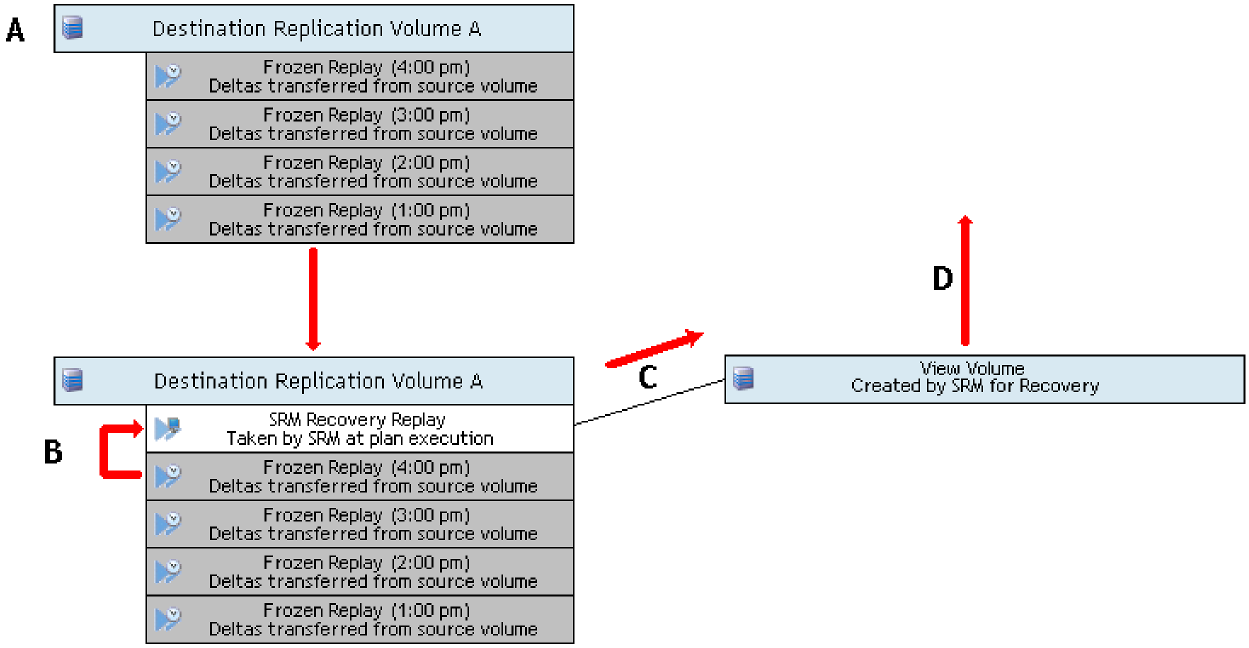

A
Destination Replication Volume A
Frozen Replay (4:00 pm)
Deltas transferred from source volume
Frozen Replay (3:00 pm)
Deltas transferred from source volume
Frozen Replay (2:00 pm)
Deltas transferred from source volume
Frozen Replay (1:00 pm)
Deltas transferred from source volume
D
C
View Volume
Created by SRM for Recovery
B
Destination Replication Volume A
SRM Recovery Replay
Taken by SRM at plan execution
Frozen Replay (4:00 pm)
Deltas transferred from source volume
Frozen Replay (3:00 pm)
Deltas transferred from source volume
Frozen Replay (2:00 pm)
Deltas transferred from source volume
Frozen Replay (1:00 pm)
Deltas transferred from source volume

Figure 10. Steps during a recovery when replicating via replay schedule

A) Once a replay is taken of the source volume, the delta changes begin transferring to the destination immediately. The consistency state of the data within this replay is dependent on whether or not the application had the awareness to quiesce the data before the replay was taken.

B) At plan execution, a new replay is taken of the destination volume. This is done per the VMware SRM specification to capture the latest data that has arrived at the DR site. Of course this means that the consistency of the data is dependent on whether or not the previous replay was completely transferred. For example using the figure above:

   a. If the 4:00 pm replay taken at the primary site was application consistent, but at the time the SRM Recovery Replay was taken, only 75% of that replay's data had been transferred and thus the data is considered incomplete.

      i. If this scenario is encountered, it may be necessary to perform manual recovery steps in order to present the next latest replay (such as the 3:00pm that was completed and is thus still consistent) back to the application.

   b. If the 4:00 pm replay taken at the primary site was application consistent, and at the time the SRM Recovery Replay was taken, all 100% of that replay had finished transferring, the resulting newly taken replay will include all of the 4:00pm replay data, and thus the application consistency of the data will be preserved.

C) Once the SRM Recovery Replay has been taken, a view volume is created from that Replay.

D) The View volume is then presented to the ESX(i) host(s) at the DR site for SRM to begin execution of the recovery plan.

Data Consistency while Replicating the Active Replay

When replicating the active replay, here are the consistency states of replications during plan execution.

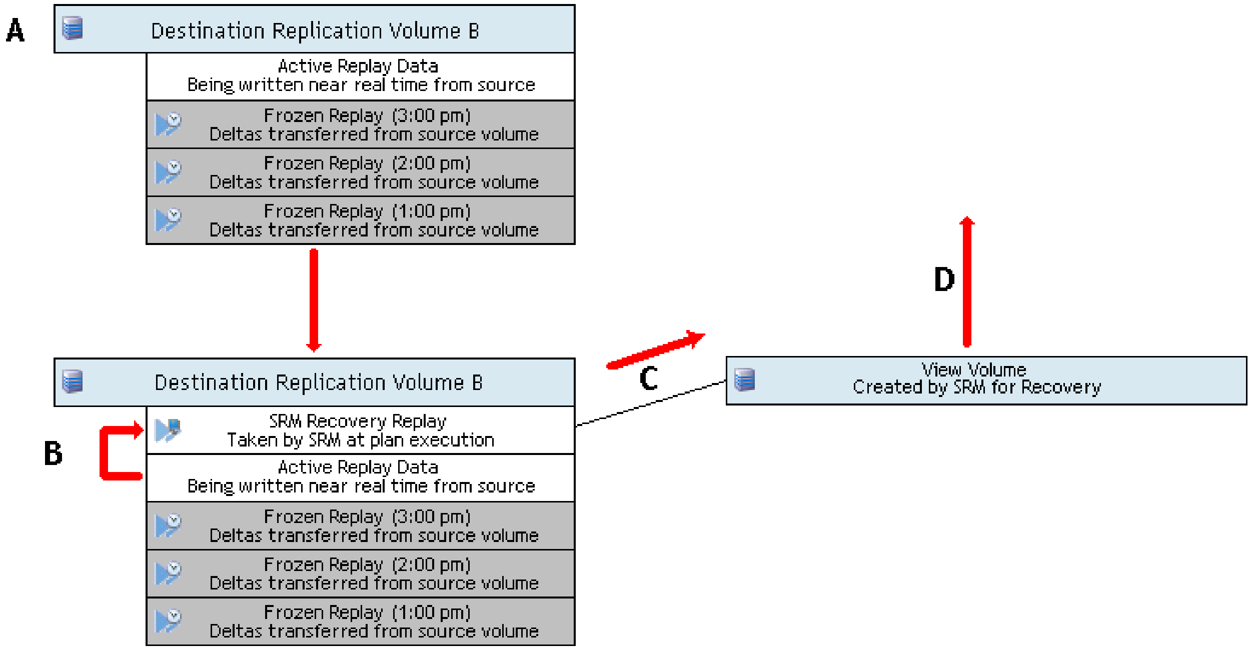

A
Destination Replication Volume B
Active Replay Data
Being written near real time from source
Frozen Replay (3:00 pm)
Deltas transferred from source volume
Frozen Replay (2:00 pm)
Deltas transferred from source volume
Frozen Replay (1:00 pm)
Deltas transferred from source volume
D
C
View Volume
Created by SRM for Recovery
B
Destination Replication Volume B
SRM Recovery Replay
Taken by SRM at plan execution
Active Replay Data
Being written near real time from source
Frozen Replay (3:00 pm)
Deltas transferred from source volume
Frozen Replay (2:00 pm)
Deltas transferred from source volume
Frozen Replay (1:00 pm)
Deltas transferred from source volume

Figure 11. Steps during a recovery when replicating the active replay.

A) As writes are committed to the source volume, they are near simultaneously transferred to the destination and stored in the Active Replay. (See figure above) Keep in mind that consistent Replays can still be taken of the source volume, and the check points will be transferred to the destination volume when replicating the active replay.

B) At plan execution, a new replay is taken of the destination volume which "locks in" all the data that has been transferred up to that point in time. Data stored within the Active Replay will most likely be crash consistent. For example, using the figure above:

   a. Although the 3:00 pm replay taken at the primary site was application consistent, at the time the SRM Recovery Replay was taken, the data must still be deemed crash consistent because it is highly probable that writes into the Active Replay occurred after the 3:00 pm replay was taken.

   b. If the application is unable to recover the crash consistent data captured in this replay, then manual steps would be required to present the last known consistent replay (such as the 3:00pm frozen replay) back to the host.

   c. The only time that application data can be considered consistent while replicating the active replay, is if ALL I/O has ceased to the source volume, followed by a complete synchronization of the data from the source to the destination.

C) Once the SRM Recovery Replay has been taken, a view volume is created from that Replay.

D) The View volume is then presented to the ESX(i) host(s) at the DR site for SRM to begin execution of the recovery plan.

Replication Dependencies and Replication Transfer Time

If the application has multiple volumes as part of its data set, it is important to remember that not all volumes may finish replicating within the same timeframe.

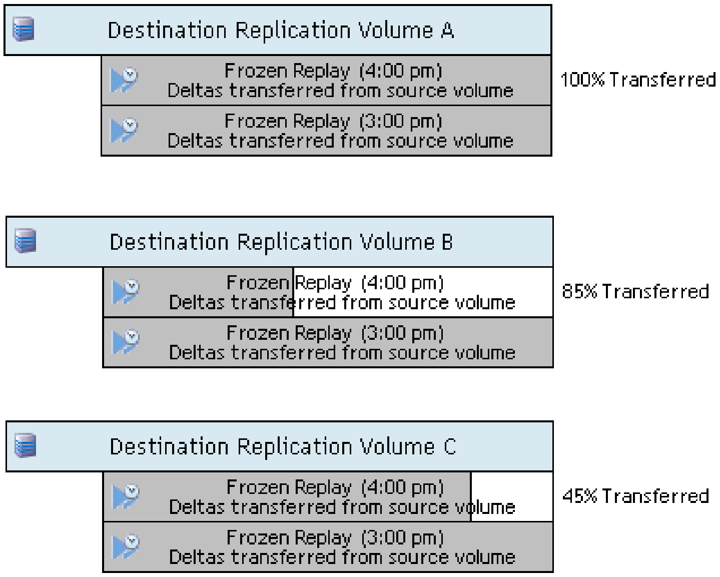
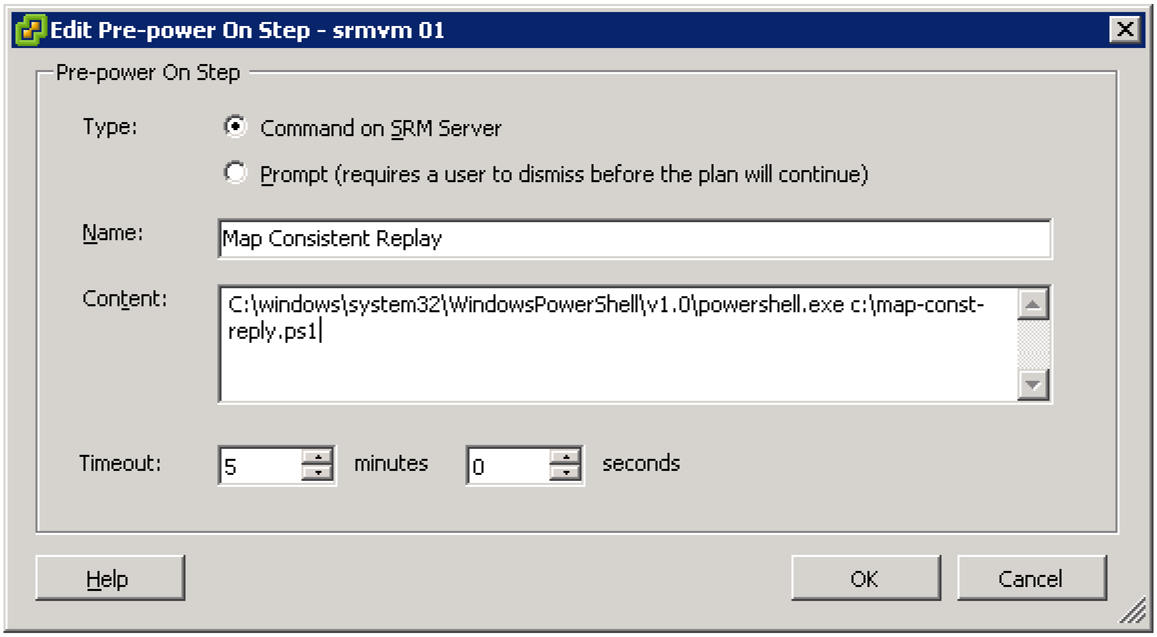

Destination Replication Volume A
Frozen Replay (4:00 pm)
Deltas transferred from source volume
100% Transferred
Frozen Replay (3:00 pm)
Deltas transferred from source volume
Destination Replication Volume B
Frozen Replay (4:00 pm)
Deltas transferred from source volume
85% Transferred
Frozen Replay (3:00 pm)
Deltas transferred from source volume
Destination Replication Volume C
Frozen Replay (4:00 pm)
Deltas transferred from source volume
45% Transferred
Frozen Replay (3:00 pm)
Deltas transferred from source volume

Figure 12. Replications completing within non-concurrent timeframes

Due to various factors such as rate of change, link bandwidth, volume size, and replication QOS, it is possible for multiple volumes in a backup set to finish replicating at different times. This means that if the plan is executed before the replications have completely transferred all of the data (as seen in figure 12), Volume A may have application consistent data, while Volumes B and C will have partially transferred data and be considered crash consistent. Depending on the application, partially transferred volumes will most likely cause problems with the application. If this happens, manual intervention may be required to present the previous set of replays back to the host (for example, the 3:00 pm replay from each volume may need to be used instead of the 4:00 pm).

Custom Recovery Tasks

If the environment has applications that require custom recovery strategies to avoid any of the situations mentioned above, both Dell Compellent and VMware have a robust set of PowerShell cmdlets in which to customize the recovery steps where needed. The Storage Center cmdlets can control which replay are selected, view volume creation, volume mappings, and even modifying replications. Within the same script, the VMware cmdlets can rescan HBA's, manipulate vDisks, add virtual machines to inventory, and most every other conceivable task required for recovery.



Type: ● Command on SRM Server
○ Prompt (requires a user to dismiss before the plan will continue)

Name: Map Consistent Replay

Content: C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe c:\map-const-reply.ps1

Timeout: 5 minutes 0 seconds

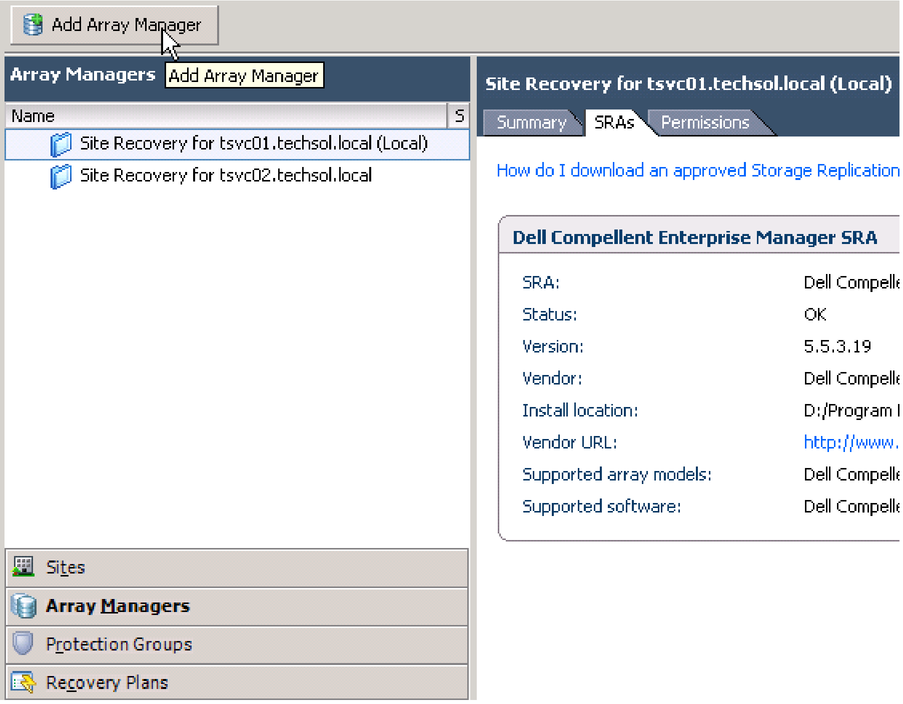
Figure 13. Adding a custom pre-power on script to a recovery plan

See Appendix A for examples of CompCU and PowerShell scripts that can be used within Site Recovery Manager.

Site Recovery Manager Configuration

Configuring the Array Managers

Configuring the array managers so the Storage Replication Adapter can communicate with the Enterprise Manager Data Collector is performed from the **Array Managers** module. An Array Manager must be added for each site in the unified interface.



Site Recovery for tsvc01.techsol.local (Local)
Site Recovery for tsvc02.techsol.local

Site Recovery for tsvc01.techsol.local (Local)

Dell Compellent Enterprise Manager SRA

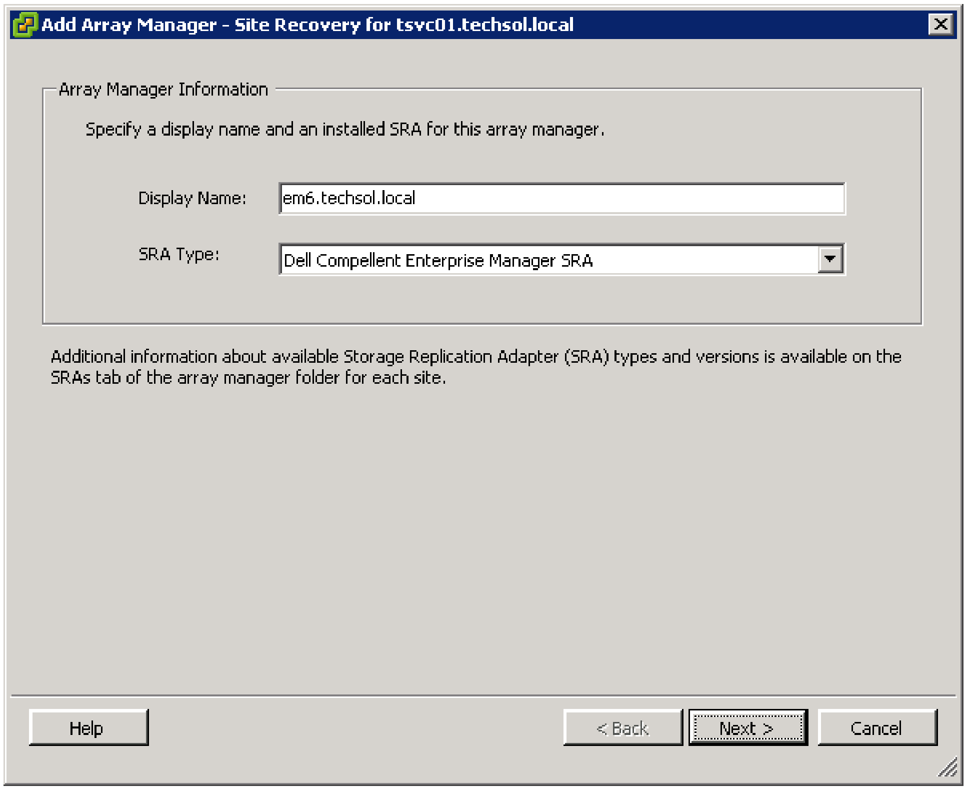
SRA:	Dell Compell
Status:	OK
Version:	5.5.3.19
Vendor:	Dell Compell
Install location:	D:/Program
Vendor URL:	http://www.
Supported array models:	Dell Compell
Supported software:	Dell Compell

Figure 14. Configure Array Managers for both sites

The **Protected Site Array Managers** and the **Recovery Site Array Managers** must both be configured so that they can be paired. Depending on the architecture, a single Enterprise Manager Data Collector can be added for both sites, or an Enterprise Manager Data Collector and Remote Data Collector model can be deployed.

- Single Enterprise Manager Data Collector
  - The **Protected Site Array Manager** and the **Recovery Site Array Manager** should both specify the Data Collector at the recovery site.
- Multiple Enterprise Manager Data Collectors
  - The **Primary Site Array Manager** should specify the Data Collector at the primary site, while the **Secondary Site Array Manager** should specify the Remote Data Collector at the secondary site.

For example, in a single data collector configuration, the **Protection Site Array Manager** should specify the recovery site data collector. Likewise, the **Recovery Site Array Manager** should specify the same data collector residing within at the same physical site.



Add Array Manager - Site Recovery for tsvc01.techsol.local

Array Manager Information

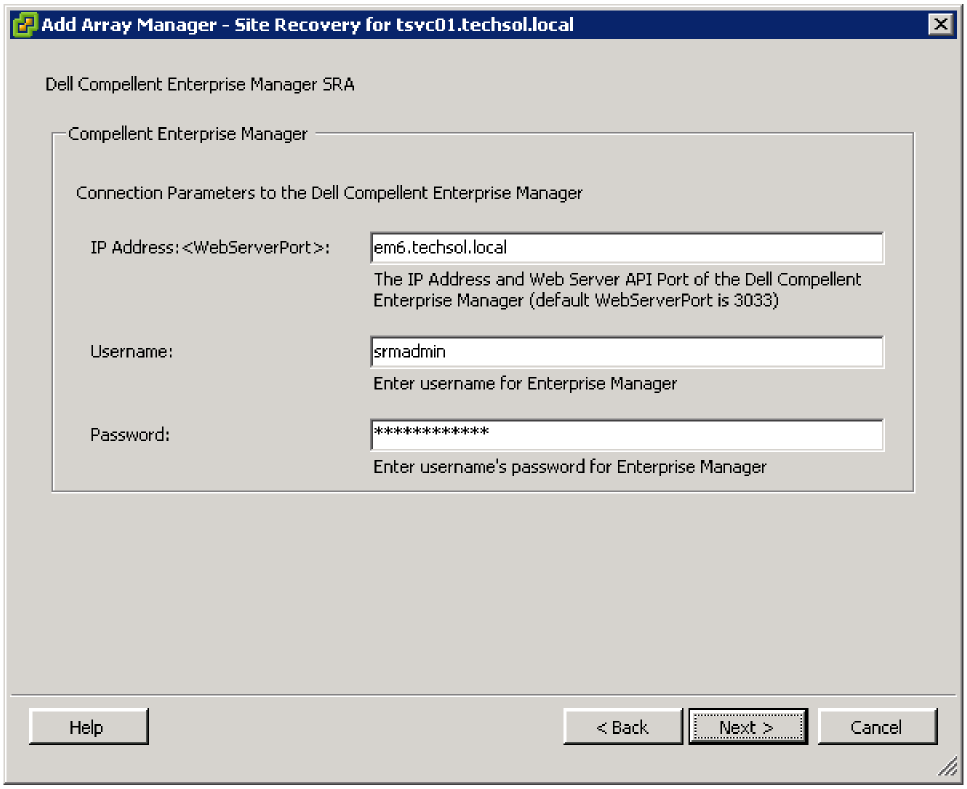
Specify a display name and an installed SRA for this array manager.

Display Name: em6.techsol.local

SRA Type: Dell Compellent Enterprise Manager SRA

Additional information about available Storage Replication Adapter (SRA) types and versions is available on the SRAs tab of the array manager folder for each site.

Figure 15. Add an Array Manager for each site



Add Array Manager - Site Recovery for tsvc01.techsol.local

Dell Compellent Enterprise Manager SRA

Compellent Enterprise Manager

Connection Parameters to the Dell Compellent Enterprise Manager

IP Address:<WebServerPort>: em6.techsol.local

The IP Address and Web Server API Port of the Dell Compellent Enterprise Manager (default WebServerPort is 3033)

Username: srmadmin

Enter username for Enterprise Manager

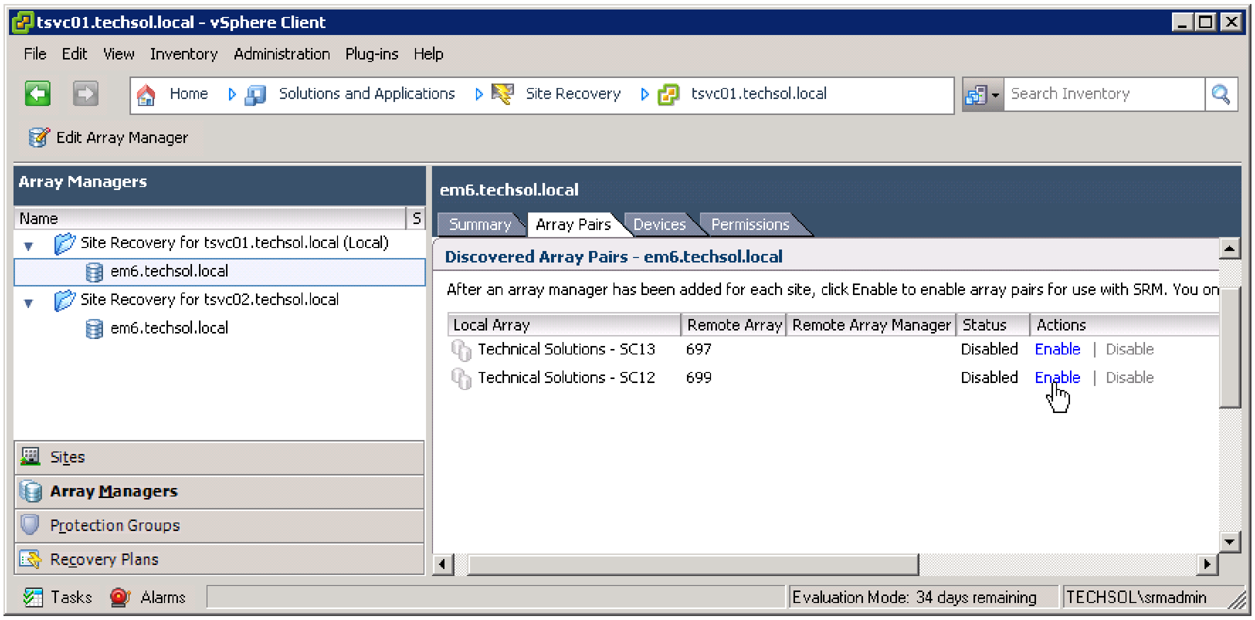
Password: ************

Enter username's password for Enterprise Manager

Figure 16. Specify privileged credentials for the Array Manager

Creating Array Pairs

Once an Array Manager has been added to each of the two sites in SRM, the arrays need to be paired so that replicated volumes can be discovered by SRM as devices. Pairing is an action that is typically only performed after the initial installation of SRM. Once the arrays are paired, they cannot be unpaired while downstream dependencies such as Protection Groups exist.

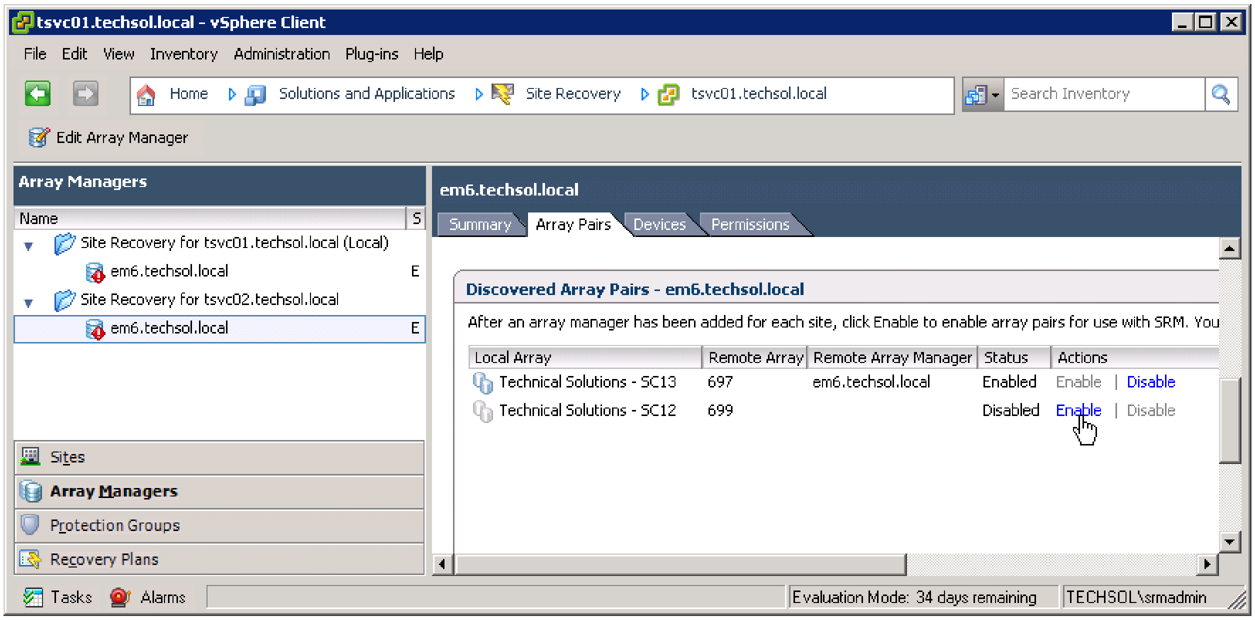


Discovered Array Pairs - em6.techsol.local

After an array manager has been added for each site, click Enable to enable array pairs for use with SRM. You on

Local Array	Remote Array	Remote Array Manager	Status	Actions
Technical Solutions - SC13	697		Disabled	Enable | Disable
Technical Solutions - SC12	699		Disabled	Enable | Disable

Figure 17. Array Pairing

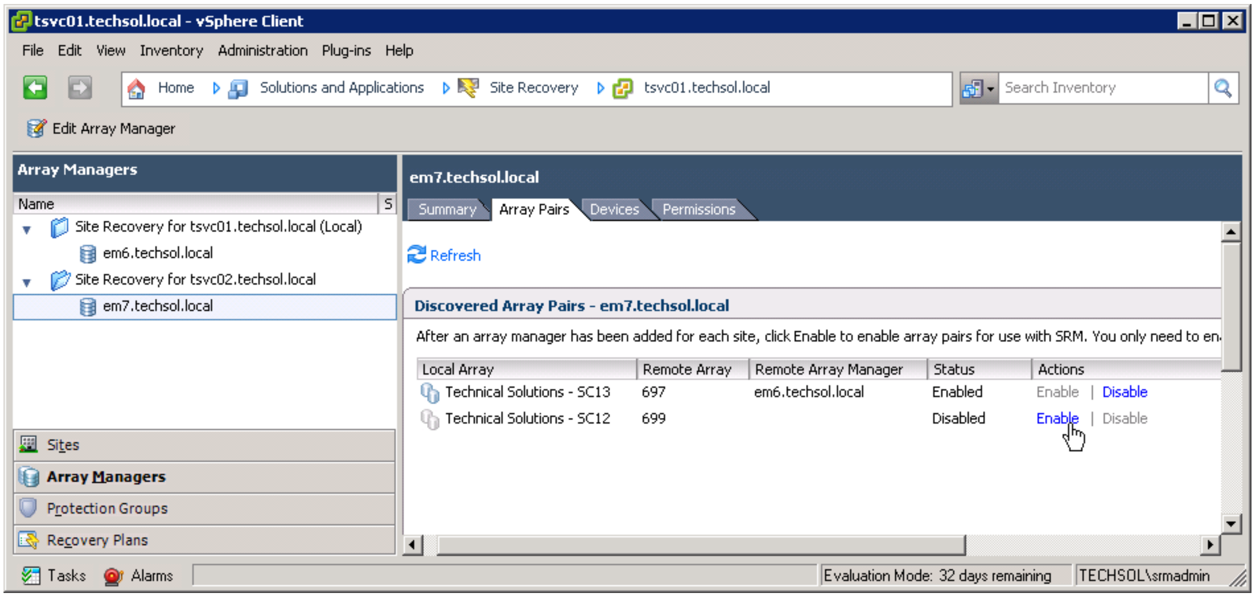


Discovered Array Pairs - em6.techsol.local

After an array manager has been added for each site, click Enable to enable array pairs for use with SRM. You

Local Array	Remote Array	Remote Array Manager	Status	Actions
Technical Solutions - SC13	697	em6.techsol.local	Enabled	Enable | Disable
Technical Solutions - SC12	699		Disabled	Enable | Disable

Figure 18. Array Managers at each site need to be paired



Discovered Array Pairs - em7.techsol.local

After an array manager has been added for each site, click Enable to enable array pairs for use with SRM. You only need to en

Local Array	Remote Array	Remote Array Manager	Status	Actions
Technical Solutions - SC13	697	em6.techsol.local	Enabled	Enable | Disable
Technical Solutions - SC12	699		Disabled	Enable | Disable

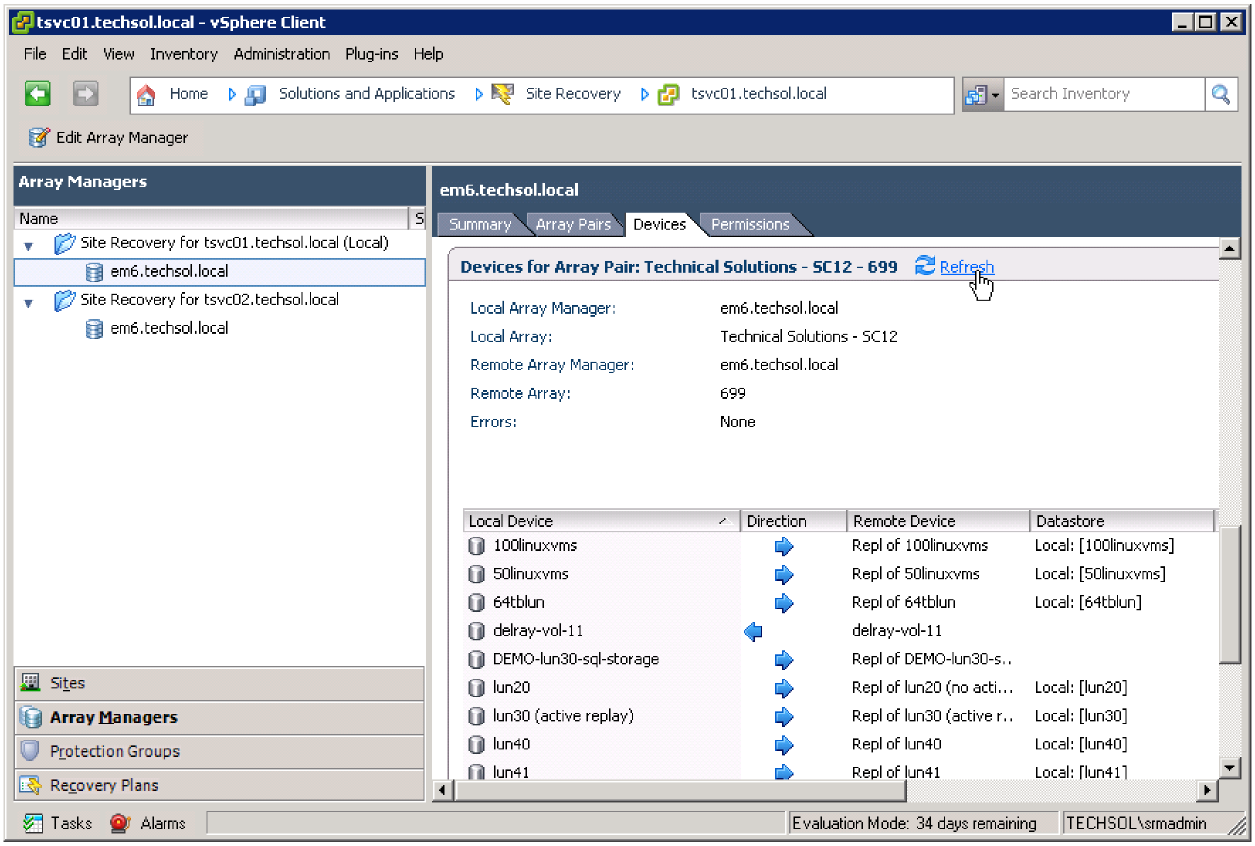
Evaluation Mode: 32 days remaining

TECHSOL\srmadmin

Figure 19. Pairing in a Primary and Remote Enterprise Manager configuration

Rescanning Array Managers

Whenever a new virtual machine datastore or replicated Storage Center volume is added to the environment, the arrays should be rescanned within SRM in addition to rescanning for new LUNs within the ESXi hosts. The Refresh link can be found on the Devices tab in the Array Managers module. Both Array Manager pairs should be refreshed to provide a consistent list of devices.



Devices for Array Pair: Technical Solutions - SC12 - 699

Local Array Manager:	em6.techsol.local
Local Array:	Technical Solutions - SC12
Remote Array Manager:	em6.techsol.local
Remote Array:	699
Errors:	None

Local Device	Direction	Remote Device	Datastore
100linuxvms	→	Repl of 100linuxvms	Local: [100linuxvms]
50linuxvms	→	Repl of 50linuxvms	Local: [50linuxvms]
64tblun	→	Repl of 64tblun	Local: [64tblun]
delray-vol-11	←	delray-vol-11	
DEMO-lun30-sql-storage	→	Repl of DEMO-lun30-s..	
lun20	→	Repl of lun20 (no acti...	Local: [lun20]
lun30 (active replay)	→	Repl of lun30 (active r..	Local: [lun30]
lun40	→	Repl of lun40	Local: [lun40]
lun41	→	Repl of lun41	Local: [lun41]

Figure 20. Refreshing Array Managers for added or removed devices

By clicking on the **Refresh** link on this screen, the SRA will re-query the Enterprise Manager Data Collector to obtain the new replicated virtual machine volume information.

Note

Note: After adding any new replicated volumes to the environment, it is always recommended to Rescan Arrays through this wizard so that SRM can discover the new replications. A Rescan should also be performed after a major SRM event such as performing a Planned Migration or Disaster Recovery.

Note

Note: Non-replicated volumes won't be discovered and displayed as devices in SRM. Keep this in mind as a troubleshooting tip if your datastores aren't showing up in SRM. Conversely, all Storage Center replicated volumes will be discovered as devices in SRM, even if they are not for use by vSphere (ie. replicated volumes belonging to physical Exchange, SQL, Oracle, file servers). This is by VMware design and an SRA requirement.

Creating Protection Groups

Before creating protection groups, it is recommended that a small VMFS datastore be created at the disaster recovery site to hold the **Placeholder VM** configuration files. For each virtual machine protected, SRM will create a "Shadow VM" at the opposite site serving as a placeholder for required CPU, memory, and network capacity in a disaster recovery or planned migration scenario.

Although this datastore only needs to be large enough to hold the configuration files for all the recoverable virtual machines, creating a standard sized 500 GB datastore will suffice and should not be thought of as unreasonable because Storage Center dynamic capacity will thinly provision the volume.

In most cases, only one "Placeholder" datastore per site should be required because the disaster recovery and migration processes will unregister and reregister the recovered virtual machine with the .vmx file on the recovered volume. Also important to note is that the Placeholder volume does not need to be replicated. VMware SRM does not place any data on this volume which cannot be easily regenerated within the UI.

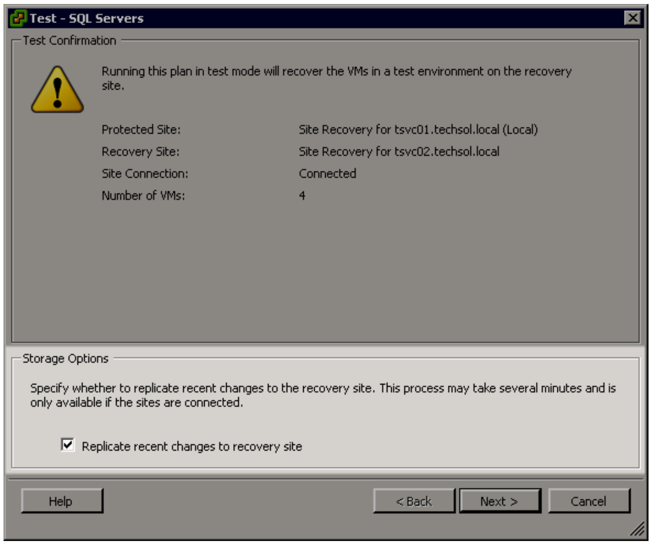
After the Placeholder datastore is created, creating protection groups follows the same general process from previous versions of SRM. Replicated datastore volumes are the foundation which protection groups are built upon. Immediately after the protection group is created, virtual machines residing on the datastore or datastores in that protection group are protected. Legacy rules apply in that once a VM is protected, it is essentially "pinned" to the datastore or datastores its .vmx and .vmdk files reside on. Moving files belonging to a virtual machine is not supported with SRM and will result in the VM no longer being protected or replicated from it's original datastore or datastores. From a design and operational standpoint, this means that automated Storage DRS (SDRS) and Storage vMotion cannot be used with SRM protected VMs. Dell Compellent Storage Center arrays offer Dynamic Block Architecture and Data Progression which provides automated sub-LUN tiering for virtual machines without interfering with SRM protection groups.

Caution: Moving protected virtual machine files will result in the virtual machine no longer being replicated or protected by SRM in its original protection group. In this case, the VM needs to be manually removed from the original protection group and added to a new protection group based on the volume the VM was migrated to.

Creating Recovery Plans

When testing or running recovery plans, SRM has no built-in mechanisms to determine whether or not the replication volumes are fully synced before the storage is prepared for the recovery. In other words, there could still be in-flight data actively being replicated to the secondary site that may influence the outcome of the recovery. This will be particularly true if you configure replication to also replicate the Active Replay.

To help ensure that all data has successfully been replicated to the secondary site, it is recommended that you check the box **Replicate recent changes to recovery site** when executing a test plan. During an actual disaster recovery cutover, this option may or may not be available. For planned migrations using SRM, this step is required to complete successfully in order to proceed.



Running this plan in test mode will recover the VMs in a test environment on the recovery site.

Protected Site:	Site Recovery for tsvc01.techsol.local (Local)
Recovery Site:	Site Recovery for tsvc02.techsol.local
Site Connection:	Connected
Number of VMs:	4

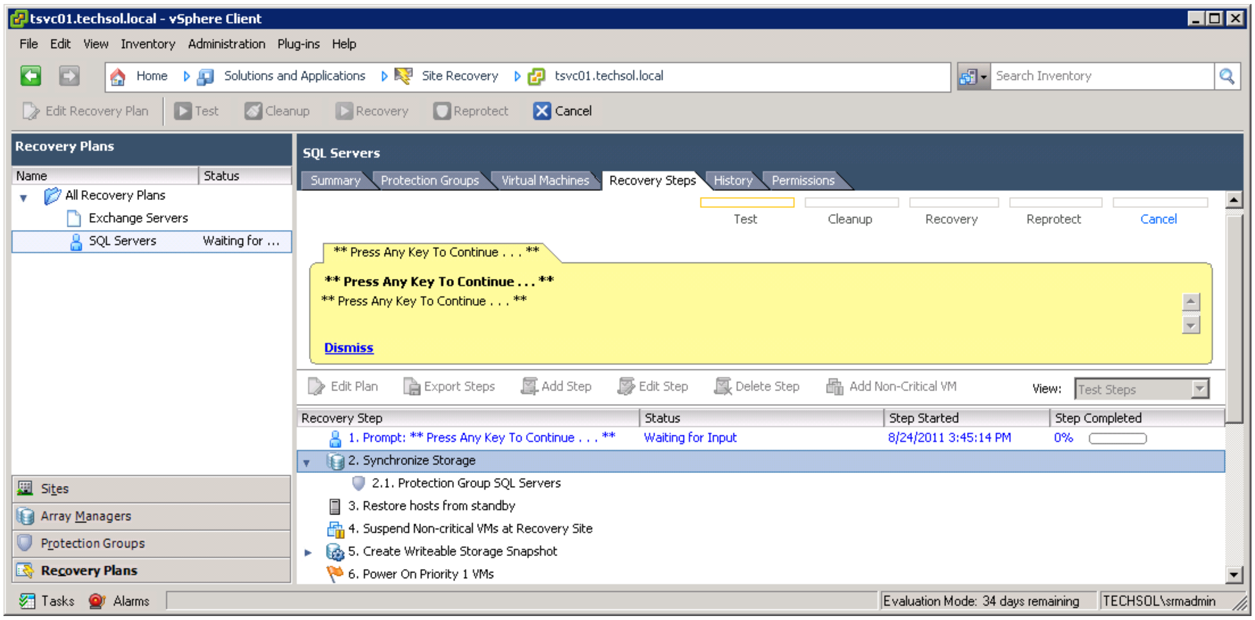
Specify whether to replicate recent changes to the recovery site. This process may take several minutes and is only available if the sites are connected.

☑ Replicate recent changes to recovery site

Figure 21. Replicate recent changes option

In addition, consider adding **Prompts** and/or SRM server-side **Commands** to the recovery plan to help ensure all data has been replicated before the subsequent **Storage** section is executed.

For example, the Compellent CompCU utility or Compellent PowerShell scripts could be integrated into the recovery plan to take current replays of all the volumes to make sure the most recent data has been replicated. An example CompCU script can be found in Appendix A of this document.



Name	Status
All Recovery Plans	
Exchange Servers	
SQL Servers	Waiting for ...

** Press Any Key To Continue . . . **

**** Press Any Key To Continue . . . ****

** Press Any Key To Continue . . . **

Dismiss

Recovery Step	Status	Step Started	Step Completed
1. Prompt: ** Press Any Key To Continue . . . **	Waiting for Input	8/24/2011 3:45:14 PM	0%
2. Synchronize Storage			
2.1. Protection Group SQL Servers			
3. Restore hosts from standby			
4. Suspend Non-critical VMs at Recovery Site			
5. Create Writeable Storage Snapshot			
6. Power On Priority 1 VMs			

Evaluation Mode: 34 days remaining

TECHSOL\srmadmin

Figure 22. Adding Prompts to the Recovery Plan

Note

Note: When the recovery plan executes, it will wait at an added **Pause** step. However, recovery plan execution will not pause at a **Command on SRM Server** step.

Recovery Plan Execution

Testing a Recovery Plan

Testing the recovery plan is non-disruptive to the storage replications and production volumes and VMs because the test recoveries use Storage Center **View Volumes** created from **Replays** to run the recovery plan tests. This means that when testing a recovery plan, any tests, changes, or updates can be performed on the recovered virtual machines, because they will later be discarded when the test recovery plan cleanup takes place. While the test plan is executing, production virtual machines and replication continues to run normally without interruption.

To test a disaster recovery plan, highlight the recovery plan to be tested, right click, and select the **Test** menu item:

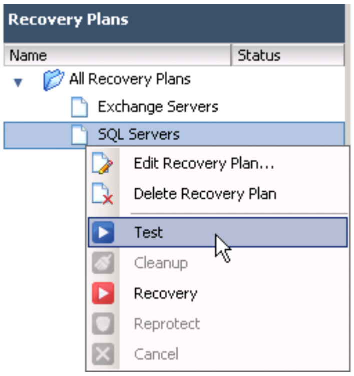


Figure 23. Test the Recovery Plan

Running a Recovery Plan

When choosing to run a **Planned Migration** or **Disaster Recovery** plan (as opposed to running a test), keep in mind ***this procedure is disruptive*** and will result in virtual machines being powered off at the primary site, replication mirrors being broken, and virtual machines being recovered at the secondary site.

In the event of a disaster or the requirement to execute a planned migration, highlight the appropriate recovery plan, right click, and choose the **Recovery** option:

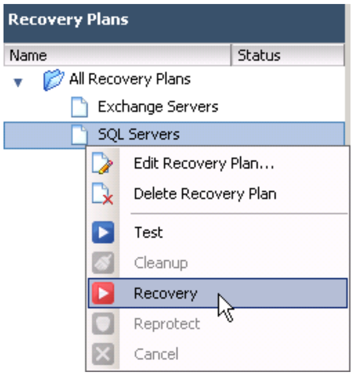
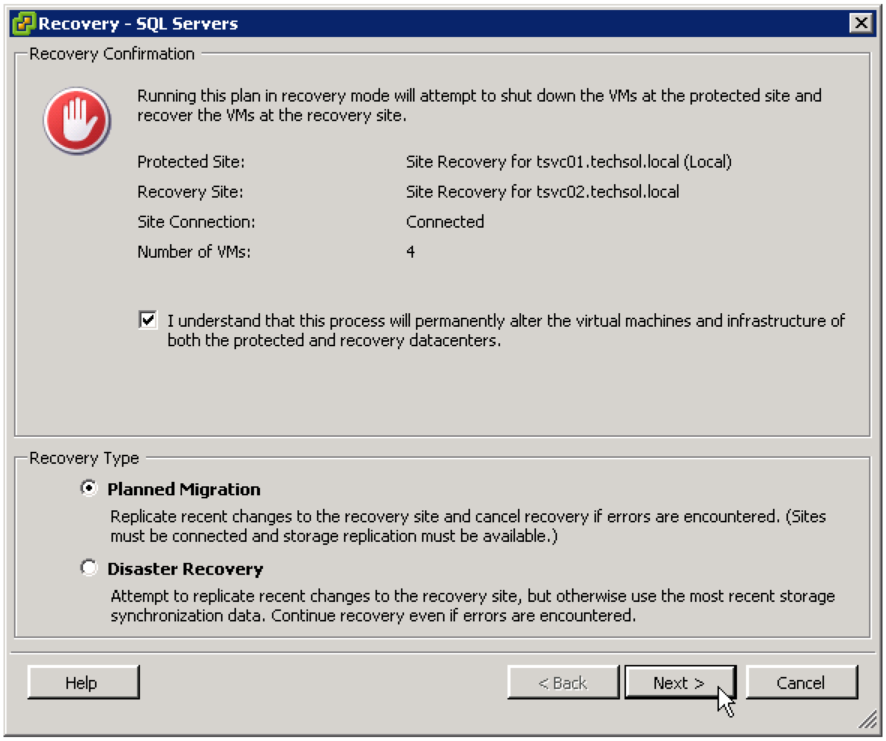


Figure 24. Running a Recovery to execute a Planned Migration or Disaster Recovery or Plan

As a safety precaution, a warning message will appear and must be acknowledged to execute a live plan.



Recovery - SQL Servers

Recovery Confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

Protected Site:	Site Recovery for tsvc01.techsol.local (Local)
Recovery Site:	Site Recovery for tsvc02.techsol.local
Site Connection:	Connected
Number of VMs:	4

☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery Type

● **Planned Migration**

Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

○ **Disaster Recovery**

Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

Figure 25. Running the Planned Migration or Disaster Recovery warning message

Note

Note: A Save Restore Points in Enterprise Manager and Rescan of Array Pairs in SRM should be performed after a major SRM event such as performing a Planned Migration or Disaster Recovery. This ensures SRM has the most current replication and volume information for the SRM environment before proceeding with a Reprotect.

Note

Note: In previous versions of SRM when running a disaster recovery plan, reprotecting and failback to the primary site were manual procedures. One of the new features in SRM 5.0 is automated **Reprotect** which enables the ability to **Failback**.

Warning

Warning: Do not enable VMware Storage IO Control (SIOC) on datastores protected by Site Recovery Manager. SIOC can prevent datastore unmounts leading to the failure of a Planned Migration. For more information, see Storage IO Control and SRM Planned Migration at http://blogs.vmware.com/vsphere/2012/06/sioc-and-srm.html as well as VMware KB articles 2008507, 1037393, and 2004605

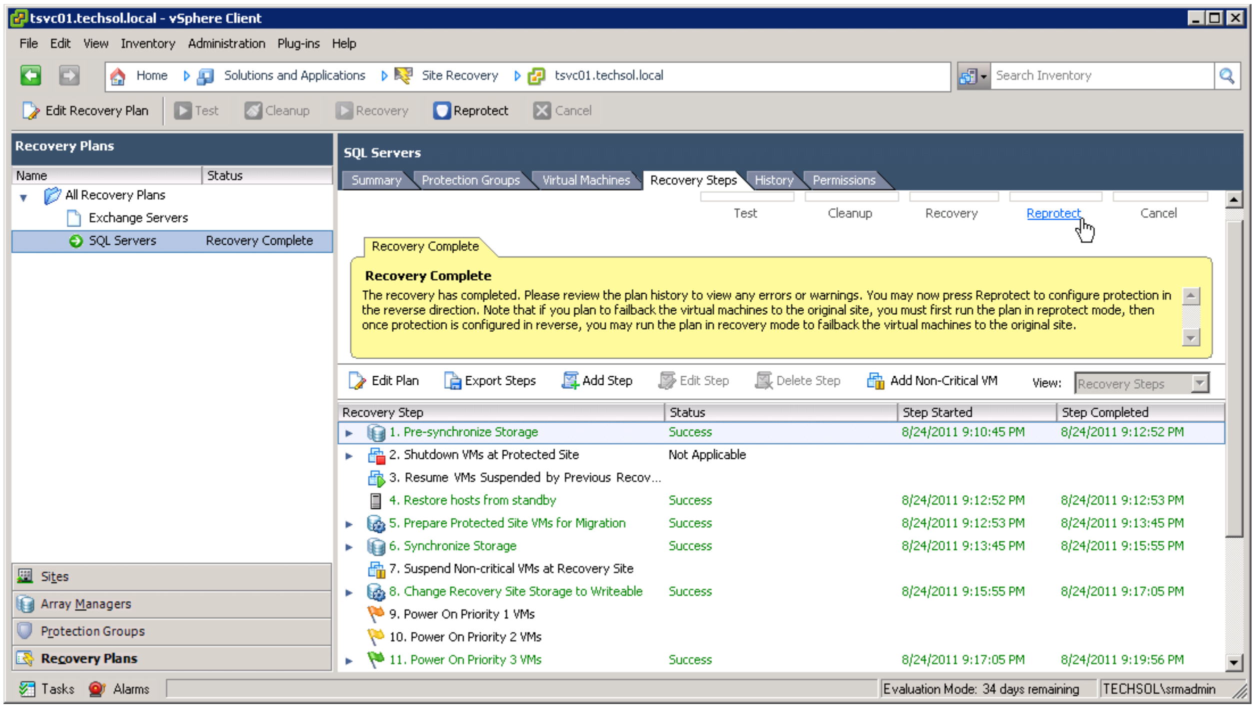
Reprotect and Failback

Overview

After virtual machines are migrated from one site to another using either the Disaster Recovery or Planned Migration features in SRM, they are in an active running state on the network at the alternate site. However, at this point they are vulnerable to a site failure with no SRM protection. This was true in previous versions of SRM and is true today in SRM 5.0. Previous versions of SRM required a manual reprotection of the virtual machines at the recovery site. SRM 5.0 automates the reprotect process and prepares the virtual machines for failback.

Reprotection

Once protected virtual machines are migrated or disaster recovery failed over to the secondary site, they are unprotected. Immediately following the migration of a protected group, SRM 5.0 automates the ability to reprotect the virtual machines. It does this by performing a series of steps.



Name	Status
All Recovery Plans	
Exchange Servers	
SQL Servers	Recovery Complete

Recovery Complete

The recovery has completed. Please review the plan history to view any errors or warnings. You may now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you may run the plan in recovery mode to failback the virtual machines to the original site.

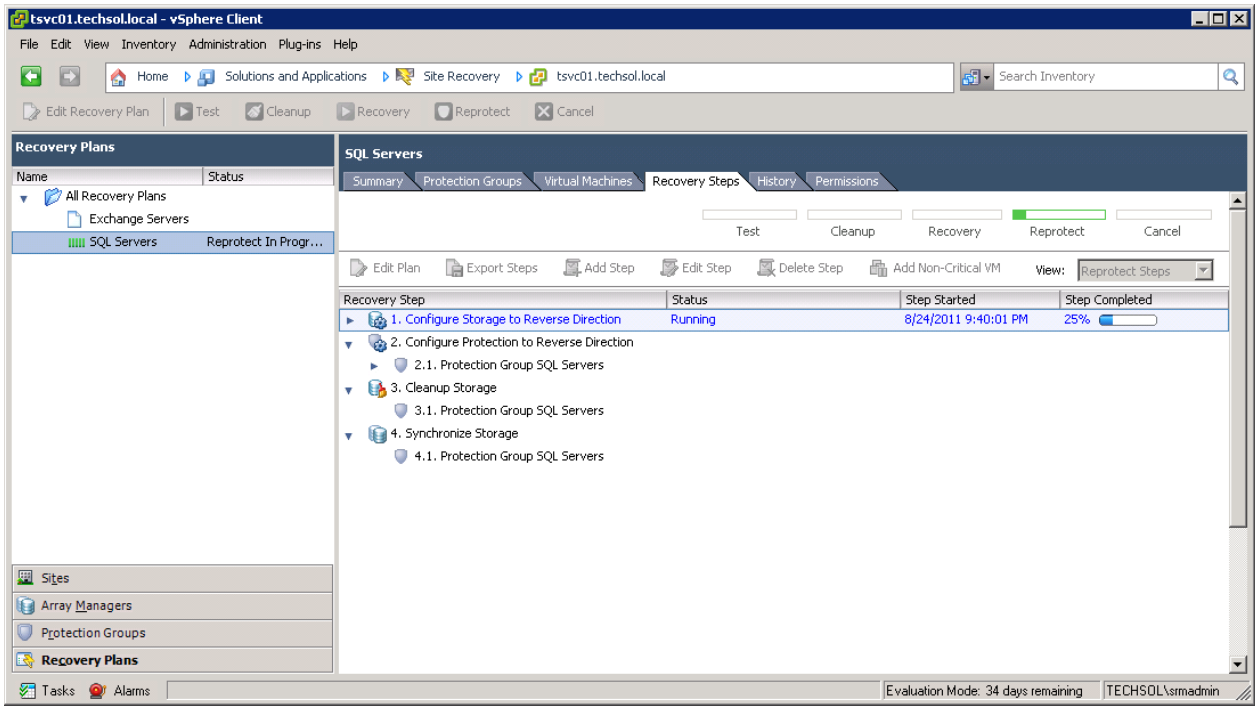
View: Recovery Steps

Recovery Step	Status	Step Started	Step Completed
1. Pre-synchronize Storage	Success	8/24/2011 9:10:45 PM	8/24/2011 9:12:52 PM
2. Shutdown VMs at Protected Site	Not Applicable		
3. Resume VMs Suspended by Previous Recov...			
4. Restore hosts from standby	Success	8/24/2011 9:12:52 PM	8/24/2011 9:12:53 PM
5. Prepare Protected Site VMs for Migration	Success	8/24/2011 9:12:53 PM	8/24/2011 9:13:45 PM
6. Synchronize Storage	Success	8/24/2011 9:13:45 PM	8/24/2011 9:15:55 PM
7. Suspend Non-critical VMs at Recovery Site			
8. Change Recovery Site Storage to Writeable	Success	8/24/2011 9:15:55 PM	8/24/2011 9:17:05 PM
9. Power On Priority 1 VMs			
10. Power On Priority 2 VMs			
11. Power On Priority 3 VMs	Success	8/24/2011 9:17:05 PM	8/24/2011 9:19:56 PM

Evaluation Mode: 34 days remaining | TECHSOL\srmadmin

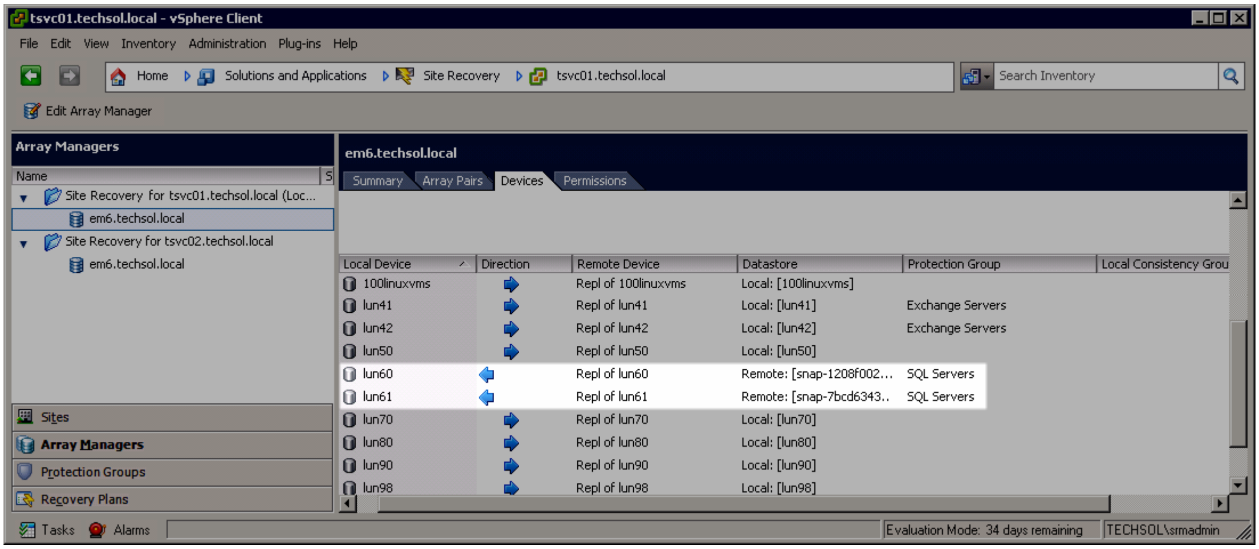
Figure 26. A successfully completed Recovery is ready for Reprotect

During a Reprotect, SRM commands the SRA to reverse storage replication for each of the datastores/volumes in the protection group in the opposite direction. The protection group, which was originally set up at the primary site is migrated to the secondary site. Placeholder VMs, which were originally set up at the secondary site, are now created at the opposite site (which can now be considered the new recovery site) on it's respective placeholder datastore.



Recovery Step	Status	Step Started	Step Completed
1. Configure Storage to Reverse Direction	Running	8/24/2011 9:40:01 PM	25%
2. Configure Protection to Reverse Direction			
2.1. Protection Group SQL Servers			
3. Cleanup Storage			
3.1. Protection Group SQL Servers			
4. Synchronize Storage			
4.1. Protection Group SQL Servers			

Figure 27. Reprotecting virtual machines workflow in SRM 5.0



Local Device	Direction	Remote Device	Datastore	Protection Group	Local Consistency Grou
100linuxvms	→	Repl of 100linuxvms	Local: [100linuxvms]		
lun41	→	Repl of lun41	Local: [lun41]	Exchange Servers	
lun42	→	Repl of lun42	Local: [lun42]	Exchange Servers	
lun50	→	Repl of lun50	Local: [lun50]		
lun60	←	Repl of lun60	Remote: [snap-1208f002…	SQL Servers	
lun61	←	Repl of lun61	Remote: [snap-7bcd6343..	SQL Servers	
lun70	→	Repl of lun70	Local: [lun70]		
lun80	→	Repl of lun80	Local: [lun80]		
lun90	→	Repl of lun90	Local: [lun90]		
lun98	→	Repl of lun98	Local: [lun98]		

Figure 28. SRM 5.0 reverses device/datastore/volume replication during a Reprotect

Failback

Failback is no more than an SRM term which describes the ability to perform a subsequent Disaster Recovery or Planned Migration after a recovery and reprotect have already been successfully performed. The benefit that Failback brings in SRM 5.0 is the automated ability to move back and forth between sites with minimal effort. This can facilitate a number of use cases including the ability to perform production processing live in the disaster recovery site, resource balancing, and improved disaster recovery infrastructure ROI.

⚠ Caution

Caution: An Enterprise Manager Data Collector Server needs to be running at the site opposite of protected virtual machines in the event of a site failure for SRM to function. Keep this in mind if you are planning on using SRM 5.0’s new planned migration feature.

Conclusion

VMware vSphere, SRM 5.0 and Dell Compellent Storage Center combine to provide a highly available business platform for automated disaster recovery with the best possible RTO and RPO, as well as planned migrations for your virtualized datacenter.

Appendix A – Example Scripts

CompCU Script: TakeReplay.cmd

Description: This is an example of a script which can be folded into an SRM Recovery Plan. The script leverages the Compellent Command Utility (CompCU) to take replays of the source replication system volumes to make sure that the most current replay is replicated to the DR site.

```
"C:\Program Files\Java\jre6\bin\java.exe" ^
                -jar c:\scripts\compcu.jar ^
                -host 192.168.1.10 ^
                -user Admin ^
                -password mmm ^
                -c "replay create -volume 'Volume_Name_1' -expire 60"


"C:\Program Files\Java\jre6\bin\java.exe" ^
                -jar c:\scripts\compcu.jar ^
                -host 192.168.1.10 ^
                -user Admin ^
                -password mmm ^
                -c "replay create -volume 'Volume_Name_2' -expire 60"
```

This script will connect to a Storage Center with an IP address of “192.168.1.10” with a username of “Admin” and a password of “mmm” to take a replay of “Volume_Name_x” with a replay expiration set to 60 minutes.

Note: The ^ symbols are used in this script for line continuation and readability, but could be excluded if the entire command is placed on one line.

The Compellent Command Utility download, and its associated documentation, can be found in the Compellent Knowledge Center. See Appendix B.

PowerShell Script: TakeReplay.ps1

Description: This is an example of the same script from above which can be folded into an SRM Recovery Plan, but written in PowerShell. The script leverages the Compellent's Storage Center Command Set Shell to take replays of the source replication system volumes in an effort to make sure that the most current replay is replicated to the DR site.

```
$SCHostname = "sc12.techsol.local"

$SCUsername = "srmadmin"

$SCPassword = ConvertTo-SecureString "mmm" -AsPlainText –Force

$SCConnection = Get-SCConnection -HostName $SCHostname -User $SCUsername -Password
$SCPassword

New-SCReplay (Get-SCVolume -Name "lun40" -Connection $SCConnection) -MinutesToLive 1440 -
Description "Replay w/ 1 day retention" -Connection $SCConnection
```

This PowerShell script will connect to a Storage Center with a host name of "sc12.techsol.local" with a username of "srmadmin" and a password of "mmm" to take a replay of "lun40" with a replay expiration set to 1 day.

Note: It is easiest to run this PowerShell script from the Compellent Storage Center Command Set Shell which automatically loads Compellent's Compellent.StorageCenter.PSSnapin snap-in. However, this script can be run from any PowerShell prompt provided the Compellent.StorageCenter.PSSnapin snap-in is manually loaded or loaded as part of the PowerShell profile.

Appendix B – Additional Resources

Compellent Resources

- Compellent Home Page
  - http://www.compellent.com
- Compellent Knowledge Center
  - http://kc.compellent.com

VMware Resources

- VMware Home Page
  - http://www.vmware.com
- VMware Knowledge Base
  - http://kb.vmware.com
- VMware Technology Network
  - http://communities.vmware.com/
- VMware Documentation
  - http://www.vmware.com/support/pubs/