WHITE PAPER

Using EMC SRDF Adapter for VMware® Site Recovery Manager

Best Practices Planning

EMC²
where information lives®

Abstract

VMware Site Recovery Manager provides workflow and business continuity and disaster restart process management for VMware virtual infrastructure. The software leverages storage array replication and communicates to the replication management through a well-defined set of specifications. This white paper discusses the best practices for using VMware® Site Recovery Manager with EMC® SRDF® Adapter.

Part Number H5511

Table of Contents

Executive summary

VMware® Site Recovery Manager provides the workflow automation and process management capabilities required for ensuring business continuity and disaster restart of environments virtualized with VMware virtualization. Site Recovery Manager uses modules called storage replication adapters to leverage storage array replication. EMC has worked with VMware to create storage replication adapters for a number of EMC storage array-based replication products including EMC® SRDF®, EMC MirrorView™, EMC RecoverPoint, and EMC Celerra Replicator™ for iSCSI.

The EMC Symmetrix® Remote Data Facility (SRDF) family of replication software offers various levels of Symmetrix-based business continuance and disaster recovery solutions. The SRDF products offer the capability to maintain multiple, host-independent copies of the data. The Symmetrix systems can be in the same room, in different buildings within the same campus, or thousands of kilometers apart. By maintaining copies of the data in different physical locations, SRDF enables customers to perform a number of ancillary operations such as disaster restart with minimal impact on normal business processing.

The synergy between VMware Site Recovery Manager and EMC Symmetrix Remote Data Facility is the focus of this white paper. The white paper discusses the procedures and best practices for using VMware Site Recovery Manager with EMC SRDF Adapter and EMC Symmetrix Remote Data Facility.

Introduction

The introduction of VMware virtualization, including the VMware Infrastructure product suite, has allowed businesses to implement disaster restart and business continuity solutions even in environments where it would have been otherwise impractical by reducing the cost and complexity of the processes and infrastructure required.

VMware Site Recovery Manager builds on the benefits of VMware Infrastructure for business continuity by providing VMware administrators tools to create and manage disaster restart plans for their VMware Infrastructure. VMware Site Recovery Manager also allows VMware administrators to test the disaster restart plan without impacting the production environment.

VMware Site Recovery Manager integrates tools familiar to VMware and server administrators with storage array replication. The interaction between VMware Site Recovery Manager and the storage array replication is facilitated through the use of a storage replication adapter (SRA). The communication between VMware Site Recovery Manager and the SRA is conducted through a set of APIs specified by VMware. The storage array vendor is responsible for the development and support of the storage replication adapter.

Audience

This white paper is intended for VMware administrators, server administrators, disaster recovery architects, and storage administrators responsible for creating, managing, and testing disaster restart and business continuity operations for their VMware Infrastructure on Symmetrix DMX™ storage arrays. The white paper assumes the reader is familiar with VMware Infrastructure, EMC Symmetrix, and related software.

VMware Site Recovery Manager

VMware Site Recovery Manager provides the workflow automation and process management capabilities required for ensuring business continuity and disaster restart of VMware Infrastructure. Site Recovery Manager uses modules called storage replication adapters to leverage storage array replication. Using the storage replication adapter, the product communicates with the utility managing the replication software through a well-defined set of specifications. The protection of the VMware Infrastructure can extend from individual replicated datastores to an entire virtualized site.

VMware's virtualization of the data center offers advantages that can be extended to business continuity and disaster recovery. These include:

- The entire state of a virtual machine (memory, disk images, I/O, and device state) is encapsulated. Encapsulation stores all information about a virtual machine as files. Saving the state of a virtual machine to a file allows the transfer of an entire virtual machine to another host.
- Hardware independence eliminates the need for an exact replica of the hardware at the recovery site. Because they are hardware independent, virtual machines can be restarted on different hardware at the recovery site without requiring changes or reinstallation. This flexibility eliminates the cost of purchasing and maintaining systems that cannot be used productively.
- Hardware independence allows an image of the system at the protected site to boot from disk at the recovery site in minutes or hours instead of days.

VMware Site Recovery Manager leverages storage array-based replication between a protection site and a recovery site. The workflow that is built into VMware Site Recovery Manager automatically discovers the datastores that are replicated between the protected and recovery sites. VMware Site Recovery Manager can be configured to support bi-directional protection between two sites.

VMware Site Recovery Manager software is installed and configured on separate servers at the protection site and at the recovery site. In addition, VMware Site Recovery Manager requires the protected and recovery sites to be managed by their own VMware VirtualCenter Server. VMware Site Recovery Manager is managed within VMware VirtualCenter, providing a single point of management for virtual machines and the disaster restart process for those virtual machines.

Further information on VMware Site Recovery Manager and VMware Infrastructure can be found on the VMware website.

EMC Symmetrix Remote Data Facility (SRDF)

The EMC Symmetrix Remote Data Facility (SRDF) family of replication software offers various levels of Symmetrix-based business continuance and disaster recovery solutions. The SRDF products offer the capability to maintain multiple, host-independent, mirrored copies of data. The Symmetrix systems can be in the same room, in different buildings within the same campus, or thousands of kilometers apart. By maintaining copies of data in different physical locations, SRDF enables customers to perform the following operations with minimal impact on normal business processing:

- Disaster restart
- Disaster restart testing
- Recovery from planned outages
- Remote backup
- Data center migration
- Data replication and mobility

Base SRDF family products

The SRDF family consists of three base solutions:

- **SRDF/Synchronous (SRDF/S)** — High-performance, host-independent, real-time synchronous remote replication from one Symmetrix to one or more Symmetrix systems.
- **SRDF/Asynchronous (SRDF/A)** — High-performance extended distance asynchronous replication using a delta set architecture for optimal bandwidth utilization and minimal host performance impact.
- **SRDF/Data Mobility (SRDF/DM)** — Rapid transfer of data from source volumes to remote volumes anywhere in the world, permitting information to be shared and content to be distributed, or information consolidated for parallel processing activities.

SRDF family options

There are a number of additional options and features that can be added to the base solutions to solve specific service level requirements. These options include:

- SRDF/Automated Replication (SRDF/AR) solutions for meeting very specific, remote replication service-level requirements
- SRDF/Star for advanced multisite failover with continuous protection
- SRDF/Consistency Groups (SRDF/CG) for data consistency
- SRDF/Cluster Enabler (SRDF/CE) for integration with host-based clustering products such as Microsoft Cluster Server (MSCS) and Veritas Cluster Server (VCS)
- Concurrent SRDF for a three-site solution that replicates devices at a production site to two disparate sites
- Cascaded SRDF for a three-site, extended distance replication using a dual role device

EMC TimeFinder

The EMC TimeFinder® family of local replication allows customers to nondisruptively create and manage point-in-time copies of the data to allow operational processes such as backup, reporting, and application testing. These activities can be performed independent of the production application resources and thus maximize the service levels without impacting performance or availability. The EMC TimeFinder family includes the following products:

- **TimeFinder/Clone—**Creates full volume copies of Symmetrix DMX volumes than can be used as point-in-time copies for data warehouse refreshes, backups, online restores, and volume migrations.
- **TimeFinder/Snap—**Creates space-saving, pointer-based copies for Symmetrix DMX systems that can be used for fast and efficient disk-based restore and backups.
- **TimeFinder/Mirror—**Creates high-performance, mirror images of Symmetrix volumes that be nondisruptively split off and used as point-in-time copies for backups, restores, decision-support, or contingency uses.
- **TimeFinder/Consistency Groups—**Allows other TimeFinder family products to coordinate cross-volume and cross-system consistency to ensure application restartability.
- **TimeFinder/Exchange Integration Module—**Automates and simplifies the process of creating and managing TimeFinder replications in a Microsoft Windows Exchange Server environment.
- **TimeFinder/SQL Integration Module—**Automates and simplifies the process of creating and managing TimeFinder replications in a Microsoft Windows SQL Server environment.

EMC SRDF Adapter for VMware Site Recovery Manager

VMware Site Recovery Manager leverages storage array-based replication such as EMC SRDF to protect Virtual Infrastructure data. The interaction between VMware Site Recovery Manager and the storage array replication is managed through a well-defined set of specifications. The VMware-defined specifications are implemented by the storage array vendor in a module referred to as the Storage Replication Adapter (SRA).

EMC SRDF Adapter is a storage replication adapter that enables VMware Site Recovery Manager to interact with an EMC Symmetrix storage environment. It allows VMware Site Recovery Manager to automate storage-based disaster restart operations on Symmetrix arrays in a Symmetrix Remote Data Facility (SRDF) configuration. The EMC SRDF Adapter for VMware Site Recovery Manager supports SRDF/Synchronous and SRDF/Asynchronous modes of operation only.

The adapter includes a command line interface (CLI) command that provides the application interface to VMware Site Recovery Manger. In addition, an options file can be used to customize the adapter's behavior to suit an environment. Please consult the release notes for the EMC SRDF Adapter for VMware Site Recovery Manager for further details on the command line interface and customization options.

Installation of EMC SRDF Adapter for VMware Site Recovery Manager

The EMC SRDF Adapter for VMware Site Recovery Manager has to be installed on the server running the VMware Site Recovery Manager software. VMware Site Recovery Manager has to be installed before the EMC SRDF Adapter can be installed.

The installation of the adapter is performed using the standard Windows InstallShield utility and should be performed on both the protection and the recovery site. The software distribution consists of three files—setup.exe, SRDF_Adapter_RNs.pdf, and readme.txt. The setup.exe file is an executable that performs the installation of the EMC SRDF Adapter. The SRDF_Adapter_RNs.pdf file in the distribution is the release notes for the adapter. The readme.txt file contains directions for obtaining the latest version of the adapter and release notes.

The installation is initiated by double-clicking the setup.exe file. The installation, as shown in Figure 1, offers the user the option to restart the VMware Site Recovery Manager service. The VMware Site Recovery Manager service needs to be restarted for the software to recognize the availability of the SRDF array manager. The restart of the service can be postponed to a later time if the customer is installing multiple storage array adapters.

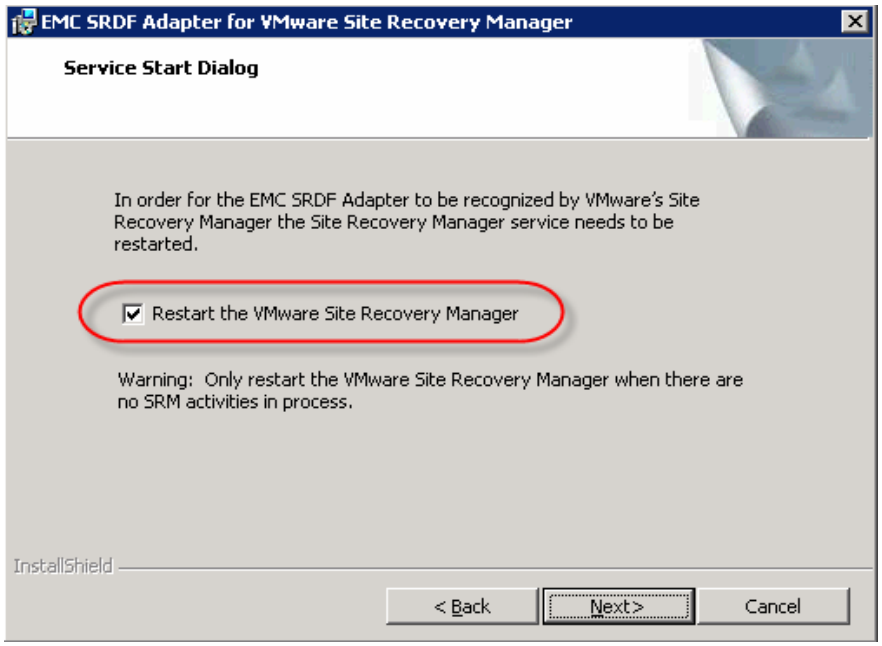

Figure 1. Installation of EMC SRDF Adapter for VMware Site Recovery Manager

The adapter, by default, is installed in the directory C:\Program Files\VMware\VMware Site Recovery Manager\scripts\SAN\EMC Symmetrix. The installer provides the user with the option of changing the name of the install directory. However, the location of the install directory is fixed by VMware Site Recovery Manager and cannot be changed.

The successful installation of the adapter results in the creation of seven files in the install directory. In addition to the adapter executable, symvmwsrm.exe, and the associated options file, symvmwsrm_options, the following files are installed:

- command.pl — provides the interface between VMware Site Recovery Manager and the symvmwsrm.exe executable
- Manifest.xml — critical information required by VMware Site Recovery Manager to manage the adapter is defined through this file

- MD5CHECKSUMS.TXT — lists the MD5 sums for symvmwsrm.exe and command.pl. The MD5 sum information can be used to verify the integrity of the install
- opensourcelicensinginfo.txt — the required listing of all open source licenses that the EMC SRDF Adapter incorporates.
- SRDF_Adapter_RNs.pdf — contains the release notes associated with EMC SRDF Adapter

The log file generated during the install is automatically deleted if the adapter is installed successfully.

Using EMC SRDF Adapter for VMware SRM

The EMC SRDF Adapter for VMware Site Recovery Manager supports DMX storage arrays running Enginuity™ code release 5x71 or later. In addition, the EMC SRDF Adapter for VMware Site Recovery Manager requires Solutions Enabler version 6.5 or later.

The EMC SRDF Adapter for VMware Site Recovery Manager utilizes EMC Solutions Enabler software to perform the discovery and management of the DMX storage arrays on behalf of VMware Site Recovery Manager. The EMC Solutions Enabler software uses in-band commands to small devices called gatekeepers to manipulate the DMX storage arrays. Therefore, EMC Solutions Enabler needs to be installed on a host that has access to gatekeepers on the storage array that contains the devices presented to the VMware Infrastructure. The simplest configuration provides the server running VMware Site Recovery Manager with direct connectivity to the storage arrays.

The more common deployment of Solutions Enabler for EMC SRDF Adapter for VMware Site Recovery Manager is anticipated to be a client-server model. In this model, the EMC SRDF Adapter utilizes the Solutions Enabler API server running on a remote host that has direct connectivity to the storage arrays. The communication between the Solution Enabler commands executed by the EMC SRDF Adapter for VMware Site Recovery Manager and Solutions Enabler API server occurs over TCP/IP network.

Figure 2 schematically depicts the environment that will be used to explain the functionality provided by EMC SRDF Adapter when used in conjunction with VMware Site Recovery Manager. It can be seen from the figure that:

- The protection site is configured with a single ESX server (licoa218), and the recovery site is configured with a single ESX server (licoa219). Although this is an unlikely configuration for production environments, the setup is sufficient for demonstration purposes.
- The VMware Site Recovery Manager and the EMC SRDF Adapter is installed on the Virtual Center server, licob123, at the protection site, and Virtual Center server, licob124, at the recovery site. EMC anticipates this configuration to be common.
- EMC Solutions Enabler software is installed on the Virtual Center server and VMware ESX server. The Solutions Enabler software on the VMware ESX server is configured to act as an EMC Solutions Enabler API server. It is important to note that EMC strongly recommends configuring at least one independent server at each site providing access to EMC Solutions Enabler API service.

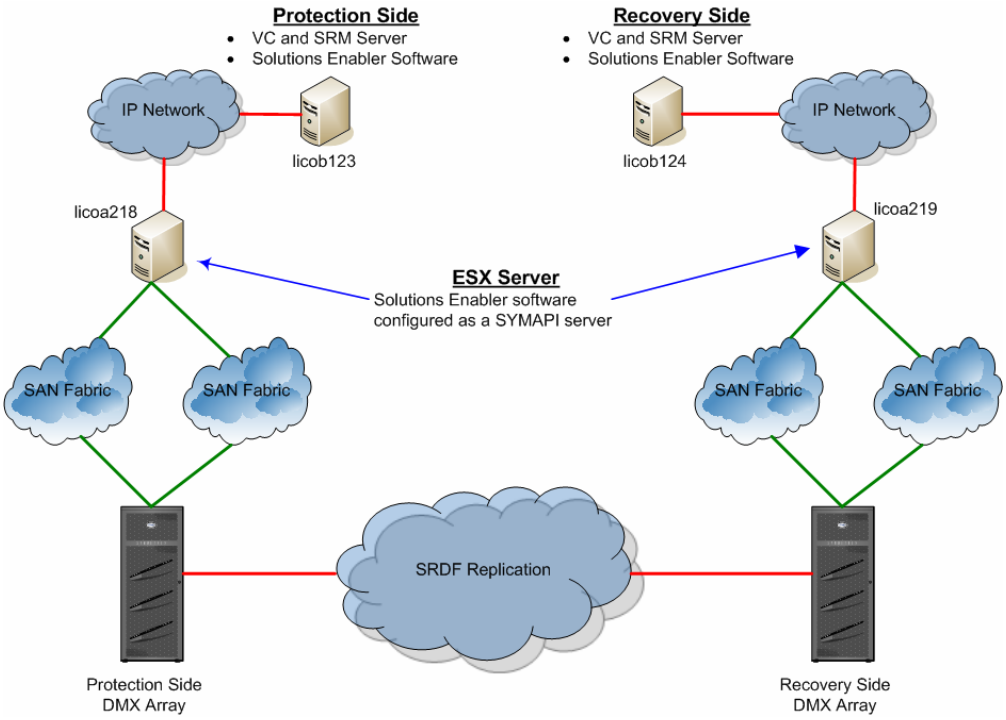

Figure 2. Example of a VMware Infrastructure environment for VMware SRM

EMC Solutions Enabler server on VMware ESX server

As discussed in the previous section, the EMC SRDF Adapter for VMware Site Recovery Manager requires access to the Solutions Enabler service running on a server that has connectivity to the DMX storage arrays. In situations where the VMware Site Recovery Manager server cannot be provided access to the DMX arrays, the VMware ESX server service console can be utilized to provide the function. EMC Solutions Enabler version 6.5 and later can be installed on the service console of VMware ESX version 3.5. The procedure to install Solutions Enabler on the VMware ESX service console can be found in the *EMC Solutions Enabler Version 6.5 Installation Guide* on Powerlink®.

Once the software has been configured, the following process should be used to configure the VMware ESX server to act as a Solutions Enabler server:

1. Change the option SYMAPI_SERVER_SECURITY_LEVEL in the file /var/symapi/config/options to SECURE. The default value for this option is ANY. Changing the security level to "SECURE" ensures that all communications with the Solutions Enabler service is encrypted.

2. Execute the command `esxcfg-firewall –o 2707,tcp,in,SYMAPI` on the service console of the VMware ESX server. This command opens the TCP/IP port used by the Solutions Enabler client when communicating with the Solutions Enabler API service running on the server.

3. The command `stordaemon install storsrvd –autostart` installs the Solutions Enabler API service daemon. The `-autostart` option ensures that the service is automatically started if the VMware ESX server is restarted.

4. The Solutions Enabler server daemon can be started on demand by running the command `stordaemon start storsrvd`.

This process should be performed on both the protection and recovery sites. It is important to note that the process to enable and use the Solutions Enabler API service on any other operating system is similar to the

one described here. Readers should consult the *EMC Solutions Enabler Symmetrix CLI Version 6.5 Command Reference* documentation available on Powerlink for further details.

For the VMware Infrastructure environment discussed in this white paper, EMC Solutions Enabler version 6.5 was installed on VMware ESX server at the protection site (licoa218) and the recovery site (licoa219). The EMC Solutions Enabler software was also configured to act as a Solutions Enabler API server utilizing the procedure described here.

Configuring EMC Solutions Enabler on the VMware Site Recovery Manager server

The EMC SRDF Adapter for VMware Site Recovery Manager utilizes Solutions Enabler commands to manage the DMX storage arrays. The EMC SRDF Adapter supports the use of a remote Solutions Enabler API server to manage the DMX storage array. However, to exploit this capability the Solutions Enabler software installed on the VMware Site Recovery Manager server has to be configured appropriately. The following procedure describes the process:

1. The file C:\Program Files\EMC\SYMAPI\config\netcnfg file should be opened for editing using an appropriate editor.

2. An entry should be added to the file defining the name of the Solutions Enabler network service and the host running the Solutions Enabler API service.

Further information on use of Solutions Enabler in a client-server configuration can be obtained in the *EMC Solutions Enabler Version 6.5 Installation Guide*, available on Powerlink.

An example of this for the VMware Infrastructure environment used for this white paper is shown in Figure 3. It can be seen from the figure that on the protection site VMware Site Recovery Manager server, a Solutions Enabler network service called licoa218 has been defined. This service is configured to use the TCP/IP protocol to communicate securely with the Solutions Enabler API service on VMware ESX server licoa218.lss.emc.com. Similarly (not depicted in the figure), a Solutions Enabler network service with the name licoa219 was defined on the VMware Site Recovery Manager server on the recovery site. That service was configured to securely access the API service on VMware ESX server licoa219.lss.emc.com[1].

[1] The recovery side Solutions Enabler network service should be defined on the host running VMware Site Recovery Manager. The error, “Failed to connect management system address while executing discoverArrays command,” will be generated by VMware Site Recovery Manager during the configuration of the arrays managers in a later step if the service is defined on the protection side. The same error is generated if an incorrect entry is made in the “SymAPI Server” field.

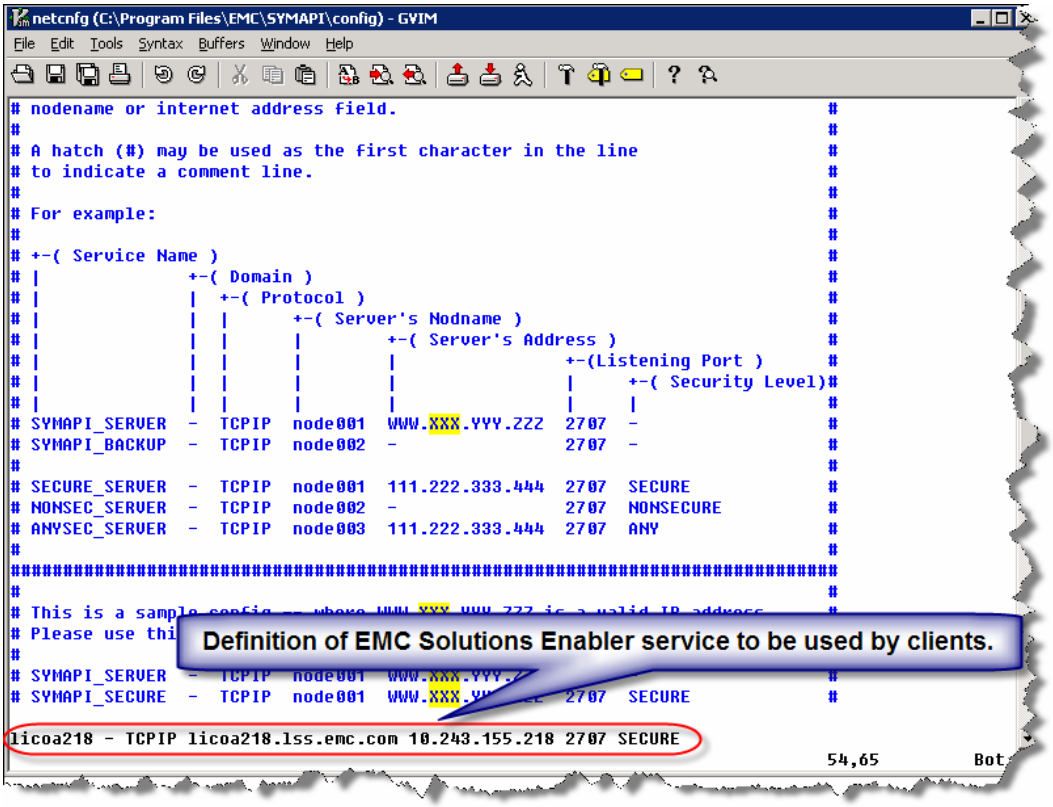

Figure 3. Defining the Solutions Enabler network service

Configuring EMC SRDF Adapter

The configuration of the EMC SRDF Adapter is performed through the "Array Managers" wizard in the VMware Site Recovery Manager plug-in. The wizard should be invoked only after the connection between the VMware Site Recovery Manager at the protection site and recovery site has been established. The process to perform this activity is beyond the scope of this white paper. Readers should consult the VMware documentation on this subject found on the VMware website.

The wizard for configuring the array managers is invoked by clicking the **Configure** button next to the Array Managers option in the Protection Setup box. The option **EMC Symmetrix** is displayed if the EMC SRDF Adapter for VMware Site Recovery Manager has been installed properly. The process to initiate the configuration of the EMC SRDF Adapter for VMware Site Recovery Manager is shown in Figure 4. Readers can perform a similar activity in their environment by following the numbers associated with each step in the process.

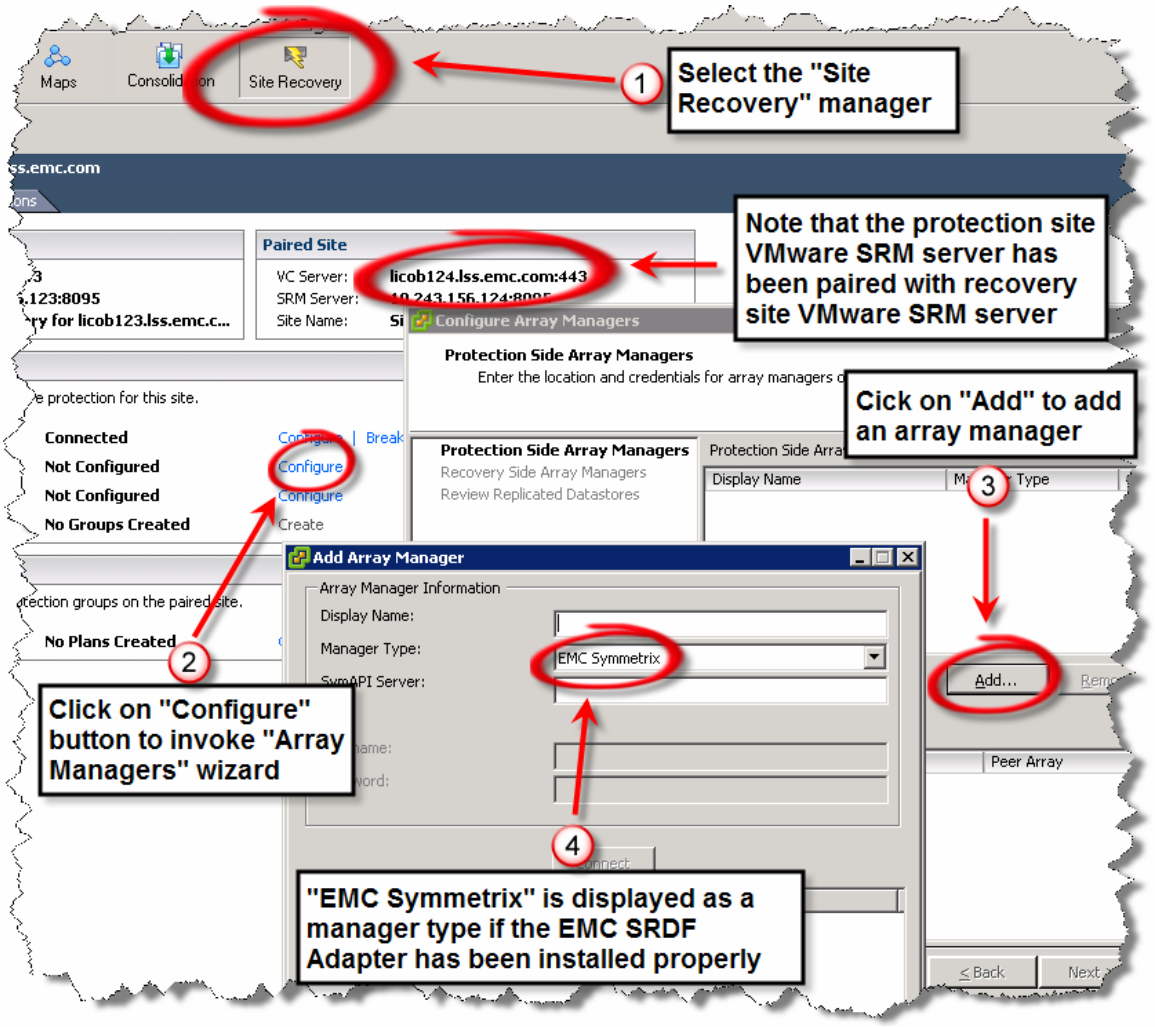

Figure 4. Initiating the Configure Array Managers wizard

The configuration of the storage arrays connected to the protection site can be determined by entering a meaningful name for the Array Manager and the EMC Solutions Enabler network service defined in the previous step and clicking **Connect**. The text **local** should be entered for the SymAPI Server name if the VMware Site Recovery Manager host has access to gatekeepers on the DMX arrays at the protection site. The discovery of the storage arrays on the protection site for the environment discussed in this white paper is shown in Figure 5 on page 13.

The VMware Site Recovery Manager automatically invokes the EMC SRDF Adapter to perform a discovery of the LUNs on the storage array as soon as the new array manager is added. A successful completion of the process results in the detailed discovery of the replicated environment including the serial number of DMX arrays at the protection site and the recovery site and the number of replicated devices on the protection site DMX array. It is important to note that the number of replicated devices reported by the EMC SRDF Adapter is not necessarily equal to the replicated devices presented to the VMware Virtual infrastructure. Figure 6 on page 13 shows the results of the discovery for the VMware Infrastructure used as an example in this article.

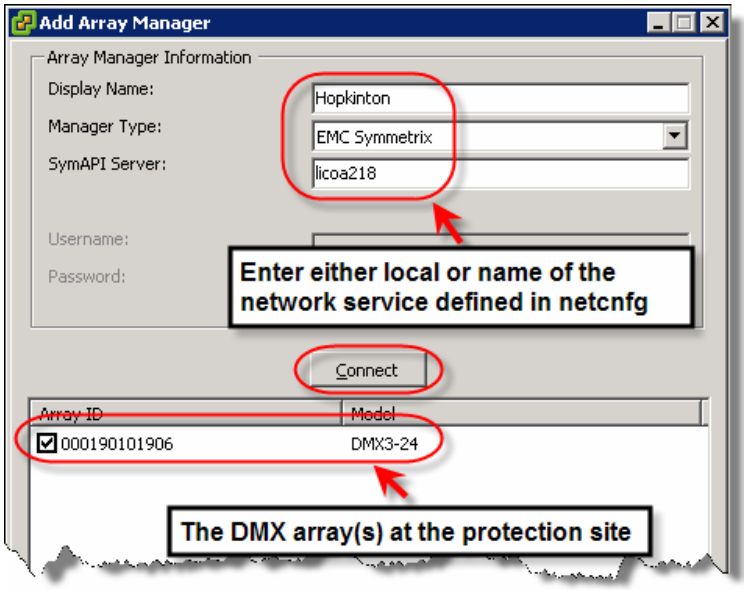

Figure 5. Adding an EMC Symmetrix array manager

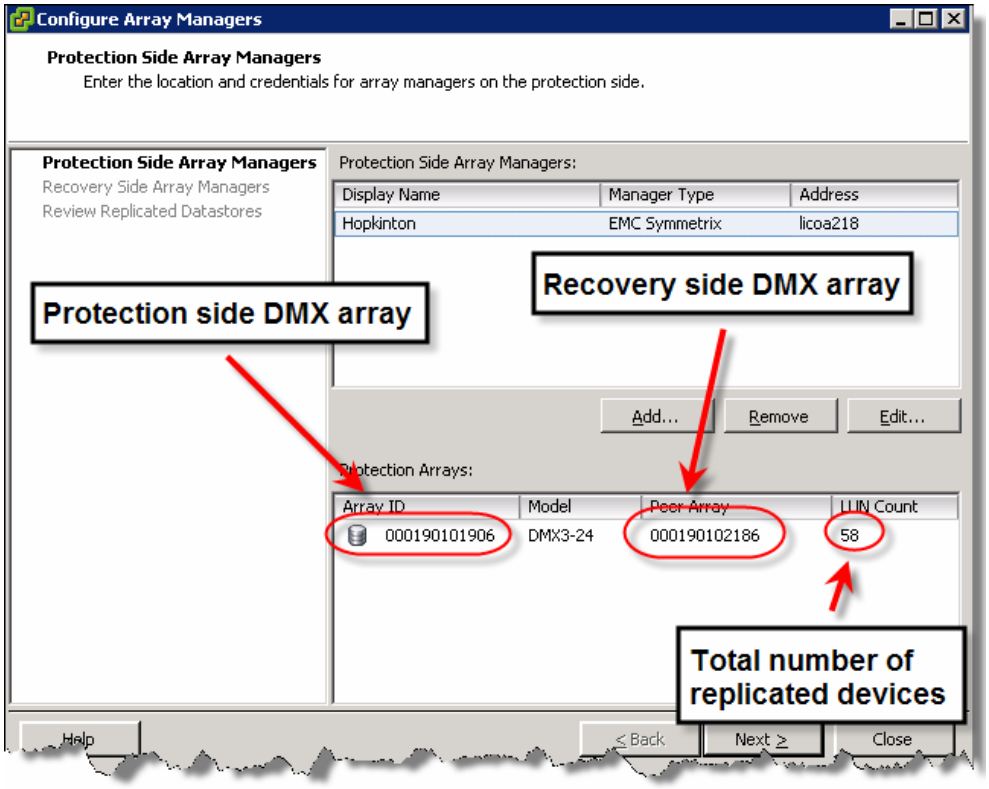

Figure 6. Display of DMX storage arrays as seen from the protection side

The recovery side array manager can be defined by clicking the **Next** button in the Configure Array Managers wizard. The process that was utilized to create the protection side array manager should be followed for the recovery side. The EMC Solutions Enabler network service configured for the recovery side should be utilized. Once the recovery side array manager is configured, VMware Site Recovery

Manager automatically reconciles the information collected from the protection and recovery side. The successful reconciliation of the information is displayed by a green checkmark next to the DMX array information. The results from the process described previously for the environment used in this white paper is shown in Figure 7.

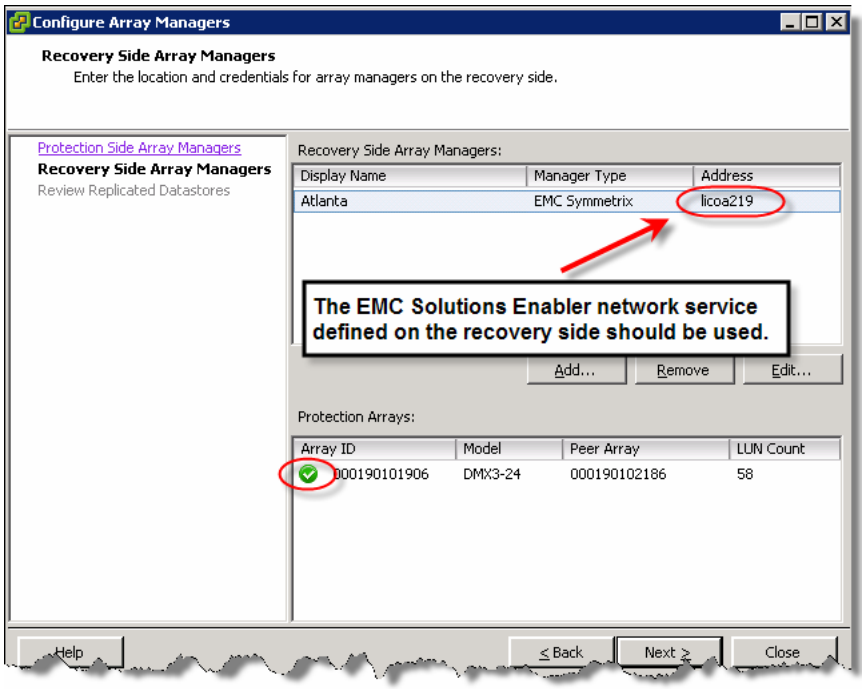

Figure 7. Display of DMX storage arrays as seen from the recovery side

The VMware datastores on the protection side that are viable candidates are displayed by VMware Site Recovery Manager when the Configure Array Managers wizard is continued. An example of this is shown in Figure 8.

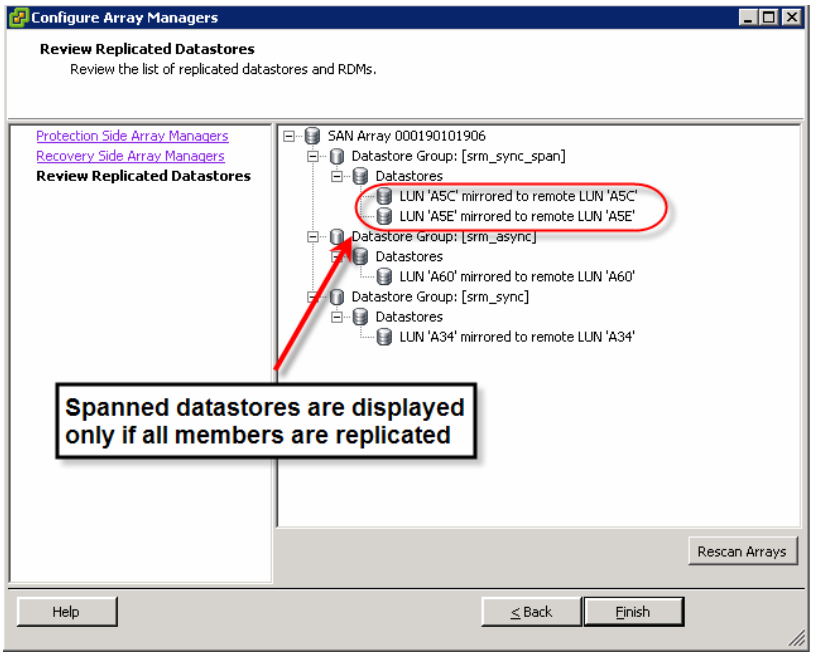

Figure 8. Display of viable datastores for protection with VMware Site Recovery Manager

VMware Site Recovery Manager does not display the mode of SRDF that protects each of the datastores. This information can be obtained by utilizing management tools for the DMX storage arrays (EMC Solutions Enabler, Symmetrix Management Console, or EMC ControlCenter®). The VMware Infrastructure environment used in this article uses both supported modes of SRDF. The datastores "srm_sync" and "srm_sync_span" are replicated with SRDF running in synchronous mode. The datastore "srm_async", on the other hand, is replicated with SRDF running in asynchronous mode.

It is important to note that VMware Site Recovery Manager does not check for the visibility of the replicated devices (or copies) to the VMware Infrastructure on the recovery site. For example, the datastore srm_sync_span on the protection site shown in Figure 8 has two devices, A5C and A5E. This datastore is replicated to devices A5C and A5E on the DMX array at the recovery site. However, as seen in Figure 9, the replicated devices are not visible to the VMware ESX server (licoa219) on the recovery site. In case of a disaster, a failover process initiated by VMware Site Recovery Manager for this datastore will not succeed. This would occur even though the EMC SRDF Adapter would succeed in initiating the failover of the impacted devices. Since recovery from that state is an arduous process, it is critical to ensure that the VMware Infrastructure at the recovery side has access to all of the appropriate devices. The VMware administrators and storage administrator must actively coordinate storage allocation or change activities to ensure the VMware Site Recovery Manager configurations are valid.

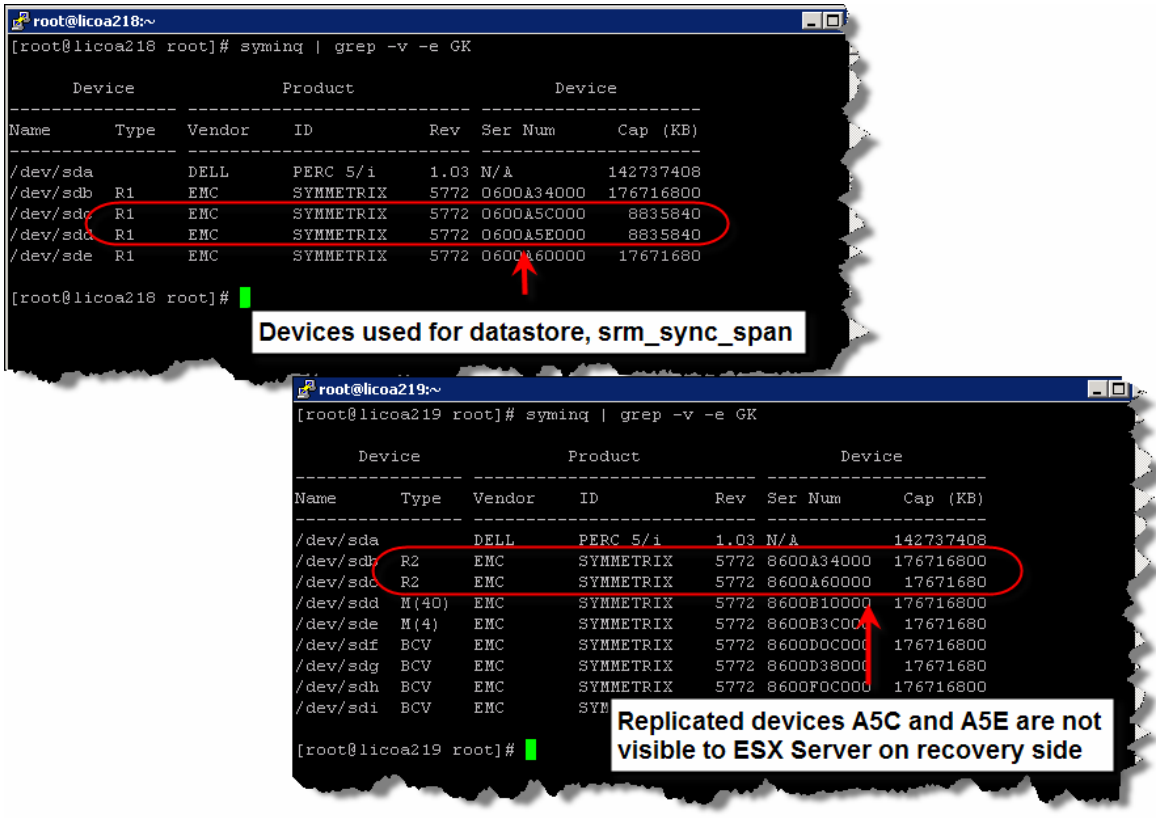

Figure 9. Display of devices presented to the VMware ESX servers

Configuring VMware Site Recovery Manager recovery plans

VMware Site Recovery Manager provides extensive functionality to configure flexible disaster restart plans. The creation and configuration of these plans are beyond the scope of this white paper. Readers should consult VMware documentation available on the VMware website for further details. However, to explain the functionality provided by EMC SRDF Adapter for VMware Site Recovery Manager during the testing and execution of the recovery plans, sample protection groups and recovery plans were created for the environment used in this article.

Three protection groups called “Synchronous Group”, “Asynchronous Group”, and “Spanned Synchronous Group” were created on the protection site to protect the datastores “srm_sync”, “srm_async”, and “srm_sync_span”, respectively. In addition, on the recovery site, three recovery plans, “Synchronous Recovery Plan”, “Asynchronous Recovery Plan”, and “Spanned Synchornous Recovery Plan” were created. Each of these plans utilized the corresponding protection group created on the protection side. The important aspects of the protection group and recovery plan configuration are shown in Figure 10 and Figure 11, respectively, for the datastore protected by SRDF/Asynchronous (srm_async). The recovery plan “Asynchronous Recovery Plan” will be utilized extensively in the following sections.

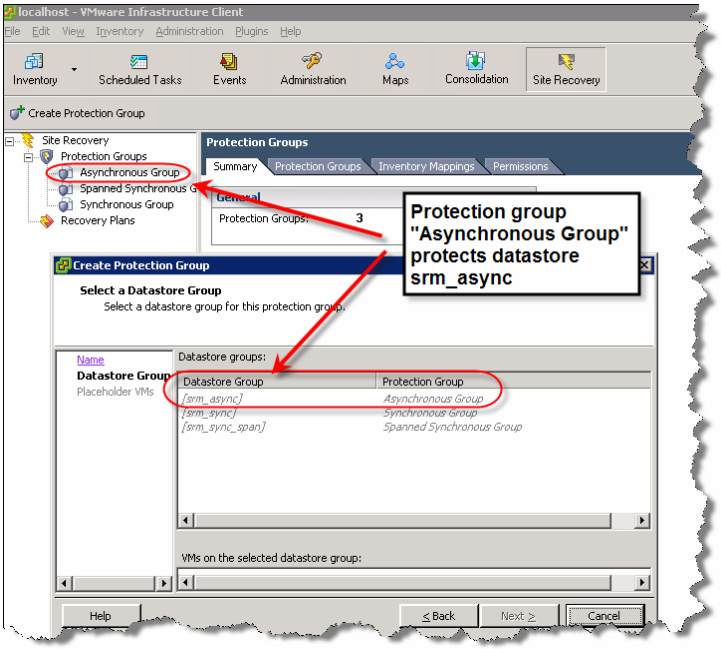

Figure 10. Display of the protection group “Asynchronous Group”

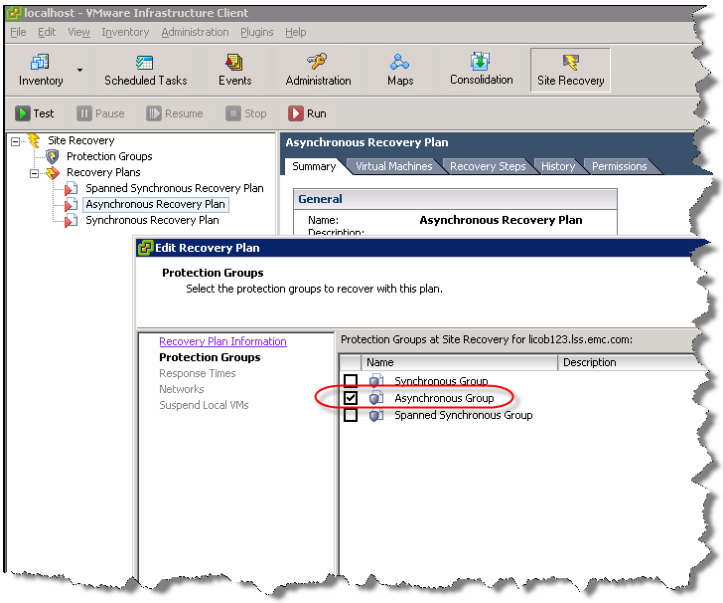

Figure 11. Display of the recovery plan “Asynchronous Recovery Plan”

Testing DR plans with VMware SRM and EMC SRDF Adapter

VMware Site Recovery Manager provides users the ability to test their recovery plans in an isolated environment. Testing recovery plans allows customers to test their disaster plans without impacting production while ensuring success in case of a true disaster. The testing of the recovery plans is achieved by leveraging the local replication technology provided by the storage arrays. Furthermore, the storage adapter provided by the vendor has to support the capability offered by VMware Site Recovery Manager. The EMC SRDF Adapter for VMware Site Recovery Manager supports the testing of recovery plans through the use of either TimeFinder/Mirror or TimeFinder/Clone technologies[2].

EMC TimeFinder and SRDF operations are normally carried out on a group of related devices. In a large environment, management of individual devices can become cumbersome. EMC Solutions Enabler simplifies the process by providing three different paradigms to manage operations—

- The user can create a logical grouping of devices in a single Symmetrix/DMX array and a single RDF (RA) group. This type of grouping is called a *device group* (DG).
- A *composite group* (CG) is a user-defined group comprised of devices that can belong to one more locally attached Symmetrix arrays and one or more RDF (RA) groups within a Symmetrix/DMX array.
- The user can create a flat file that lists all related pairs of devices. The flat file can be used as an input to various EMC Solutions Enabler commands.

EMC SRDF Adapter for VMware Site Recovery Manager supports all of the constructs provided by EMC Solutions Enabler. However, the user has to create a device group or composite group and add the appropriate devices to the group on the host running VMware Site Recovery Manager[3]. In the absence of device group or composite group EMC SRDF Adapter for VMware Site Recovery Manager automatically reverts to the use of the flat file approach to manage the devices participating in the recovery plans[4]. Further information on the EMC Solutions Enabler grouping types can be found in the *EMC Solutions Enabler Symmetrix Array Management CLI Version 6.5 Product Guide* on Powerlink.

Creating EMC Solutions Enabler device groups

The process to create device groups on the recovery side is straightforward. The process can be easily understood by using the datastore "srm_async" discussed in the earlier section as an example. As seen in Figure 8 on page 14, the datastore "srm_async" has a single DMX device A60 on the protection side replicated to device A60 on the recovery side. The following describe the necessary steps to create the device group for managing the datastore:

1. On the host running VMware Site Recovery Manager, open a command prompt and set the environment variable SYMCLI_CONNECT to the Solutions Enabler network service defined in the netcnfg file. This step can be skipped if the host is directly connected to the DMX array at the recovery side.

2. Create a device group by executing the command, `symdg –type R2 create <dg_name>`, where `<dg_name>` is the name of the device group.

3. Add the appropriate replicated device to the device group by executing the command, `symld –g <dg_name> -sid <SN> add dev <dev #>`, where `<dg_name>` is the name of the device

[2] EMC SRDF Adapter for VMware Site Recovery Manager does not support the splitting of the remote replication links to conduct tests since this compromises the customer's disaster restart position.

[3] Although EMC SRDF Adapter supports both device group and composite group, the use of composite group is warranted if and only if the grouping either spans multiple Symmetrix arrays or multiple RDF groups. Since VMware Site Recovery Manager and EMC SRDF Adapter does not support configuration that spans multiple Symmetrix arrays, the use of composite groups should be limited to the configurations that span multiple RDF groups.

[4] EMC SRDF Adapter requires creation of a device group or composite group if EMC TimeFinder/Clone technology is used for testing recovery plans.

group created in the previous step, <SN> is the serial number of the DMX array at the recovery side, and <dev #> is the device number.

4. Associate appropriate BCVs to the device group by running the command, `symbcv -g <dg_name> associate dev <dev #>`, where <dg_name> is the name of the device group created in step 2, and <dev #> is the device number for the BCV. This step should be skipped if EMC TimeFinder/Clone technology is being leveraged to test recovery plans.

5. Add the clone devices to the device group by running the command, `symld -g <dg_name> add dev <dev #> -tgt`, where <dg_name> is the name of the device group created in step 2, and <dev #> is the device number of the clone. It is important to use the "`-tgt`" option to allow EMC SRDF Adapter to correctly identify the clone devices. This step should be skipped if EMC TimeFinder/Mirror technology is being leveraged to test recovery plans.

Figure 12 shows the steps discussed above as applied to the devices hosting the datastore "srm_async". It is interesting to note that a BCV (F38) and a clone (B3C) were added to the device group created in the example. EMC SRDF Adapter supports these configurations. The adapter by default uses the BCV device during the testing of the recovery plans. However, the adapter can be directed to use the clone device by adding the option, "copy_type = CLONE" in the options file, symvmwsrm_options, discussed in previous sections.

It is important to note that the device group or the composite group has to be modified if the devices hosting the datastore changes. For example, if the existing datastore is extended by adding an replicated extent, that device should also be added to the device group or the composite group. Failure to modify the group definitions appropriately would result in a failure when the recovery plan is tested or run.

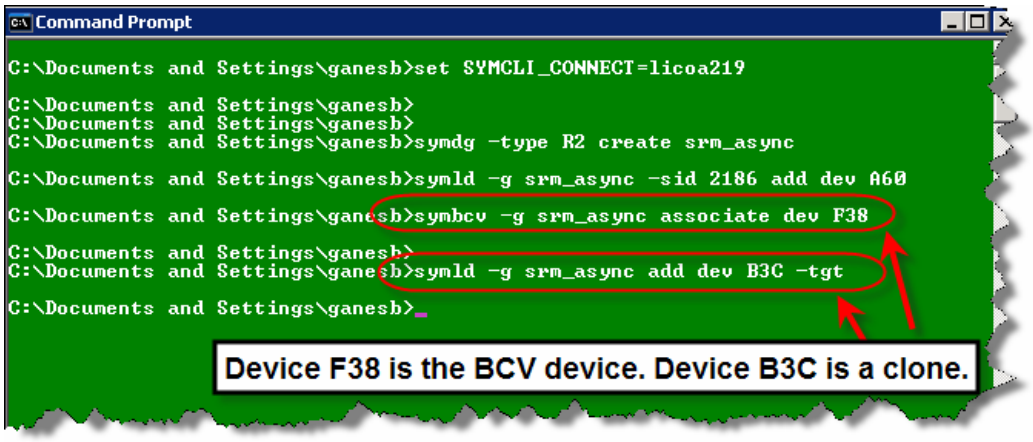

Figure 12. Creating a device group to manage testing and execution of recovery plans

Testing recovery plans using EMC TimeFinder/Clone

EMC SRDF Adapter for VMware Site Recovery Manager supports the use of EMC TimeFinder/Clone technology to test recovery plans. The following steps should be followed when testing recovery plans with EMC TimeFinder/Clone technology:

1. Ensure the target of the cloning operation is presented to the appropriate VMware ESX servers at the recovery site. Figure 13 shows the execution of this step for testing the recovery plan associated with the datastore "srm_async".

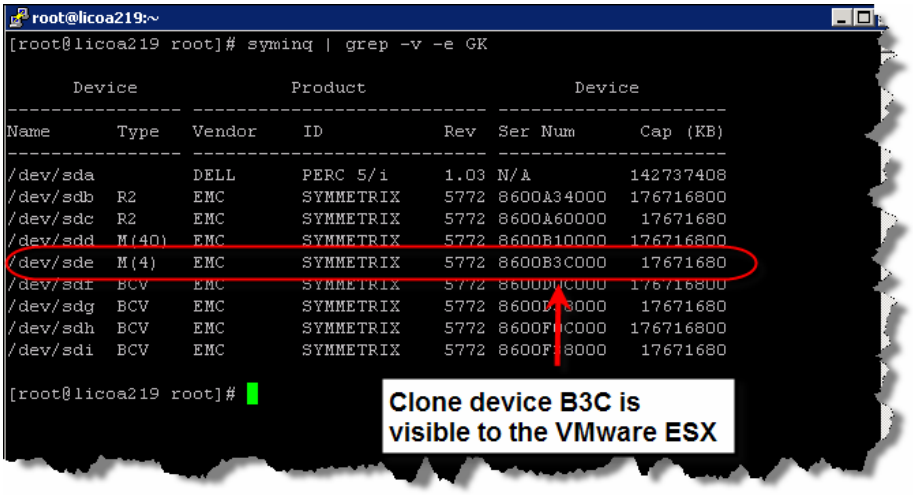

Figure 13. Determining devices presented to the ESX Server on the recovery side

2. Create a device or composite group and add the replicated device(s) and associated clone(s) to the device group using the procedure described in the previous section. In addition, there should be no pre-existing relationship between the replicated device(s) and the associated clone(s). The EMC SRDF Adapter automatically creates the relationships when needed.

3. Add the option "copy_type=CLONE" in the options file, symvmwsrm_options. This is shown in Figure 14 for the VMware Infrastructure used as an example for this white paper.

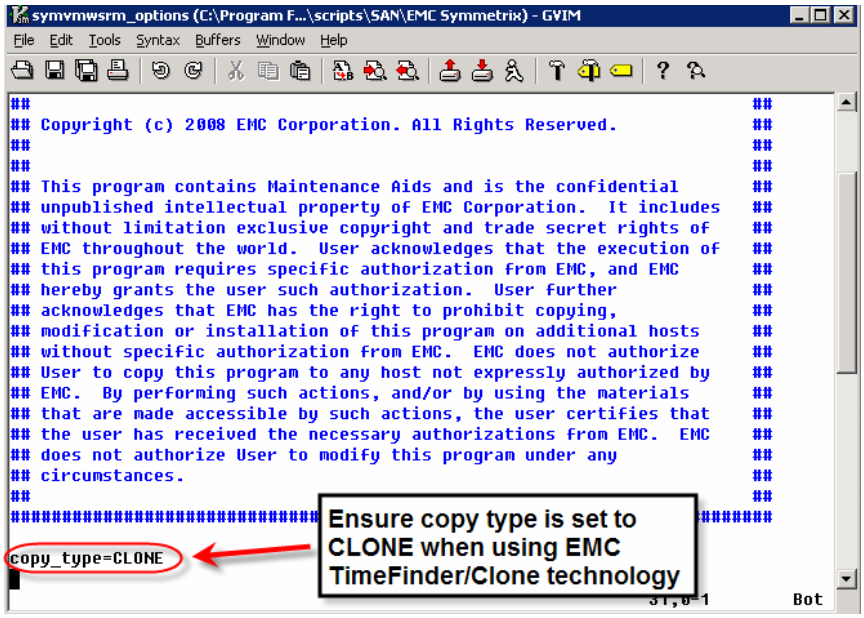

Figure 14. Directing EMC SRDF Adapter to utilize clones when testing recovery plans

4. Click the **Test** button after highlighting the recovery plan that is being tested. The EMC SRDF Adapter for VMware Site Recovery Manager automatically discovers the device group and performs appropriate EMC TimeFinder/Clone operations.

The testing of the recovery plan "Asynchronous Recovery Plan" is shown in Figure 15. It can be seen from the figure that the EMC SRDF Adapter has successfully created a local copy of the srm_async datastore using EMC TimeFinder/Clone technology. The VMware Site Recovery Manager has also successfully used

the copy of the datastore on the VMware ESX server at the recovery side and powered on a copy of the virtual machine hosted on that datastore.

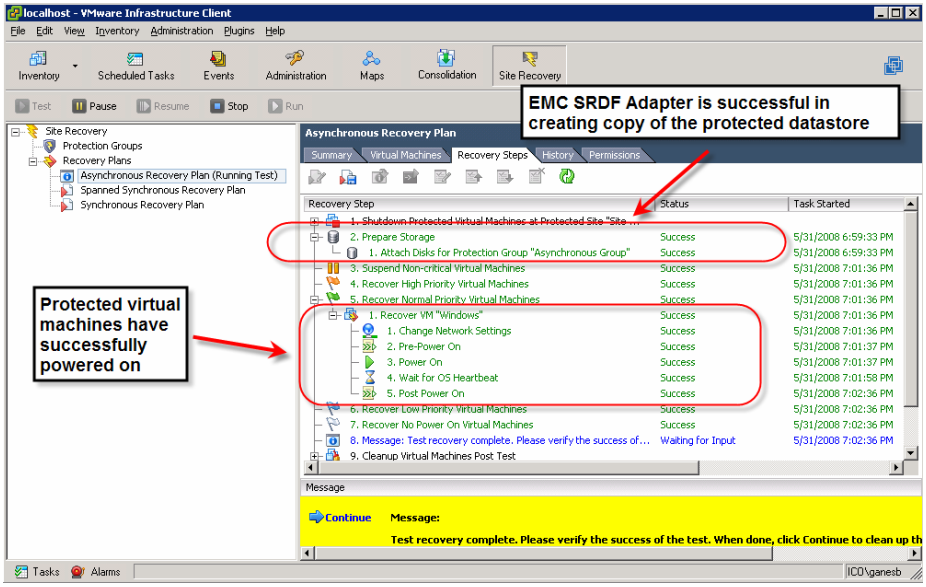

Figure 15. Running a test of a recovery plan using EMC TimeFinder/Clone technology

The state of the clone device, B3C, can be verified by utilizing a Solutions Enabler command on the host running VMware Site Recovery Manager[5]. This is shown in Figure 16.

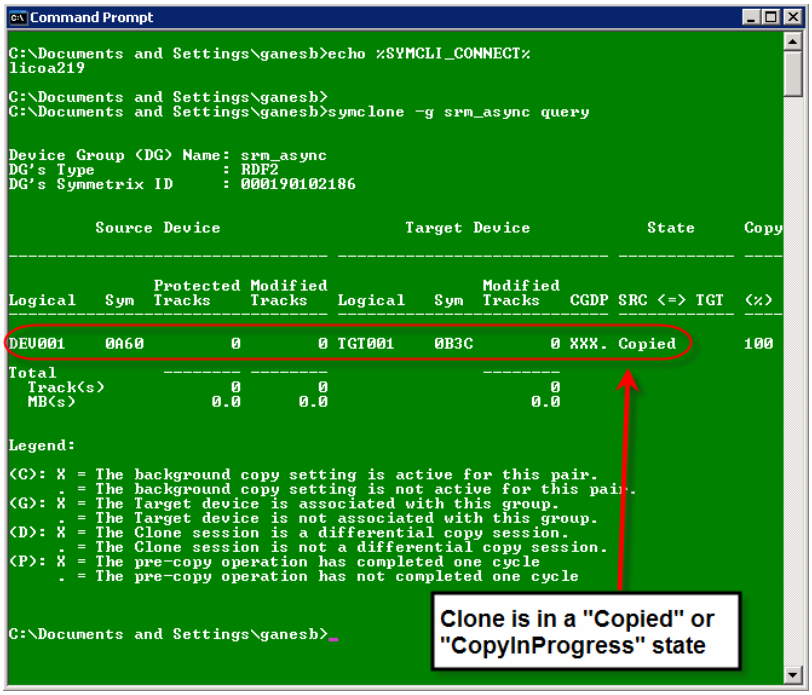

Figure 16. Determining the state of the clone device during the testing of recovery plans

[5] If needed, the variable SYMCLI_CONNECT, as described earlier, should be set to the EMC Solutions Enabler network service name defined in the file netcnfg.

The termination of the recovery plan test is accomplished by clicking the **Continue** button shown in Figure 15. As shown in Figure 17, this step automatically invokes the EMC SRDF Adapter to terminate the cloning relationship. As part of the cleanup process, VMware Site Recovery Manager deletes the datastores on the clones.

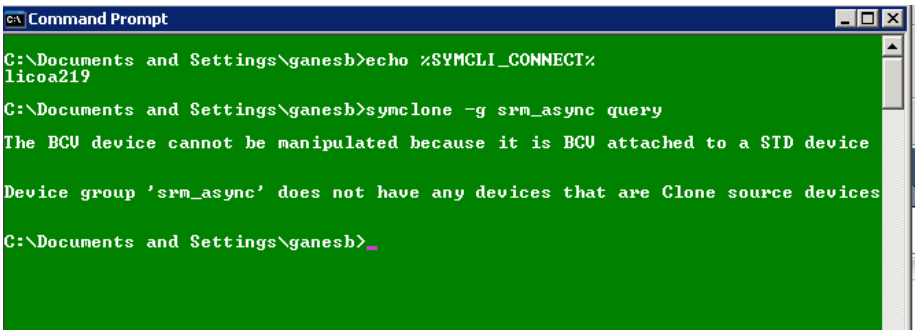

Figure 17. Termination of the clone relationship at the end of the test of recovery plan

Testing recovery plans using EMC TimeFinder/Mirror

EMC SRDF Adapter for VMware Site Recovery Manager supports the use of EMC TimeFinder/Mirror technology to test recovery plans. The following steps should be adhered to when testing recovery plans with EMC TimeFinder/Mirror technology:

1. Ensure that the correct BCVs are presented to the appropriate VMware ESX servers at the recovery site. Figure 18 shows that the BCV device, F38, associated with the datastore "srm_async" is available to the VMware ESX server at the recovery side.

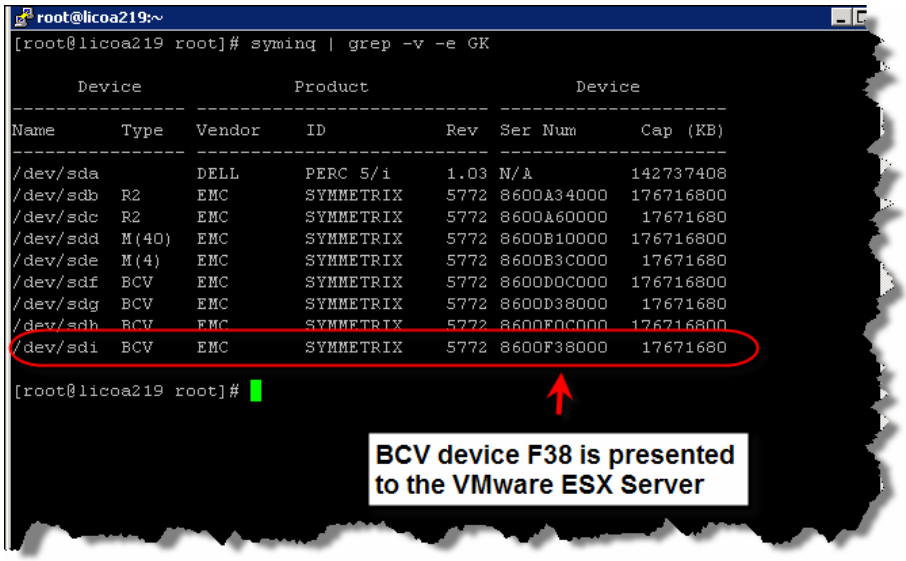

Figure 18. Determining devices presented to the ESX Server on the recovery side

2. Create a device or composite group and add the replicated device(s) and associated BCV(s) to the device group using the procedure described in the previous section. In addition, the BCV(s) should be synchronized to the replicated device(s) before the recovery plans can be tested. The EMC SRDF Adapter automatically splits the BCV(s) from the replicated device(s) when needed.

3. Ensure that the option "copy_type" does not exist in the options file, symvmwsrm_options, or is set to BCV.

4. Click the **Test** button after highlighting the recovery plan that is being tested. The EMC SRDF Adapter for VMware Site Recovery Manager automatically discovers the device group and performs appropriate EMC TimeFinder/Mirror operations.

The testing of the recovery plan "Asynchronous Recovery Plan" is shown in Figure 19. It can be seen from the figure that the EMC SRDF Adapter has successfully created a local copy of the srm_async datastore using EMC TimeFinder/Mirror technology. The VMware Site Recovery Manager has also successfully used the copy of the datastore on the VMware ESX server at the recovery side and powered on a copy of the virtual machine hosted on that datastore. A quick comparison of Figure 15 on page 20 and Figure 19 clearly shows that the underlying technology deployed to create a local replica of the datastore is masked from VMware Site Recovery Manager.

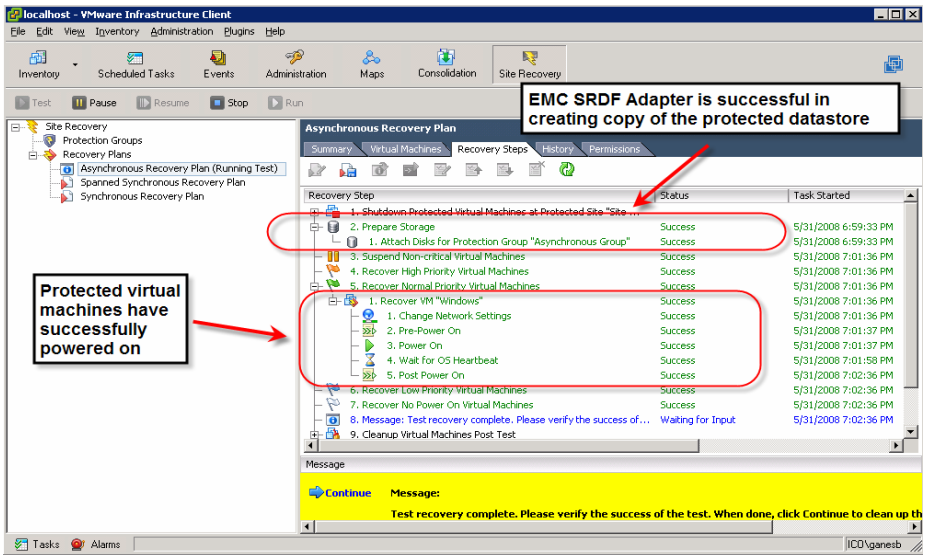

Figure 19. Running a test of a recovery plan using EMC TimeFinder/Mirror technology

The state of the BCV device, F38, can be verified by utilizing a Solutions Enabler command on the host running VMware Site Recovery Manager[6]. This is shown in Figure 20.

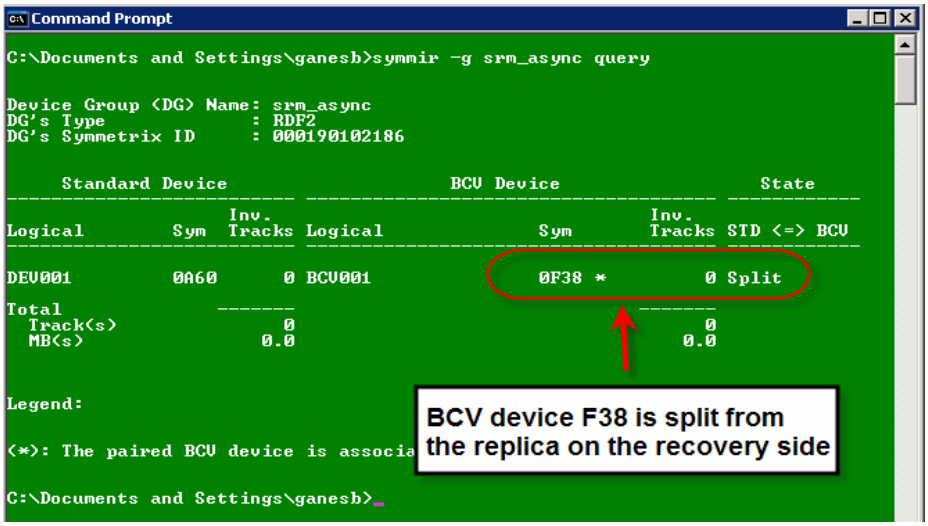

Figure 20. Determining the state of the BCV device during the testing of recovery plans

[6] If needed, the variable SYMCLI_CONNECT, as described earlier, should be set to the EMC Solutions Enabler network service name defined in the file netcnfg.

The termination of the test of the recovery plan (Figure 19) by clicking the **Continue** button, as shown in Figure 21, automatically invokes the EMC SRDF Adapter to re-establish the BCV with the source device.

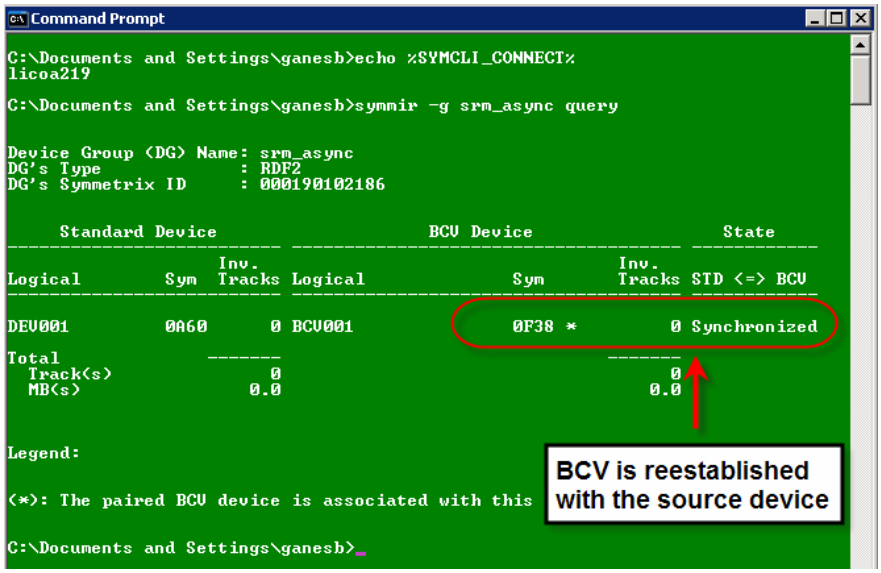

Figure 21. Re-establishing the BCV device at the end of the test of the recovery plan

Executing recovery plans during disasters

VMware Site Recovery Manager provides workflow and process management to automate the restart of a VMware Infrastructure environment in the event of a disaster. VMware Site Recovery Manager is not targeted as a tool for non-disaster workload management between different sites for the following reasons:

- The failback process from the recovery site back to the protection site requires additional configuration and some manual processes. The last section of this white paper discusses the procedure.
- The failover from the protection site to the recovery site involves the resignaturing of the protected datastores. When the failback from the recovery site to the protection site occurs, the protection site VMware ESX servers views the failed back datastores as snapshots. A manual process to recover from this situation is tedious. However, as discussed later, this can be addressed by using VMware Site Recovery Manager to orchestrate a failback.
- There is no support for replication topologies that involve replication fan-in and fan-out, which enterprise environments normally use to optimize their storage environment.
- The current software does not support consistency concepts that span multiple storage arrays. These configurations are frequently encountered in large enterprises.

The EMC SRDF Adapter for VMware Site Recovery Manager provides maximum flexibility when recovery plans are executed. The EMC SRDF Adapter automatically tries to perform a dynamic swap of the replication process before reverting to read-write enablement of the devices at the recovery side. The dynamic swap of the replication process, if possible, simplifies the failback from the recovery side to the protection side at a later time. However, this activity is possible only if the DMX array at the protection side survives and continues to communicate with the DMX storage array at the recovery side.

Figure 22 shows the results from the execution of the recovery plan, "Asynchronous Recovery Plan," discussed earlier. It can be seen from the figure that the execution of the test plan took approximately seven minutes, of which approximately four minutes were spend in manipulating the storage devices. The time required for restarting the VMware Infrastructure depends strongly on the number of protected virtual machines. The time reported for attaching the disks includes the time for rescanning the HBA. In the example discussed herein, and as shown in Figure 23 on page 24, the manipulation of the device pairs by

EMC SRDF Adapter took approximately one minute (the time difference between the start of the “Prepare Storage for Recovery” task and the “Rescan All HBA” task). Therefore, it is obvious that the EMC SRDF Adapter is highly optimized to perform the failover as quickly as possible, and contributes an insignificant amount of time to the overall process.

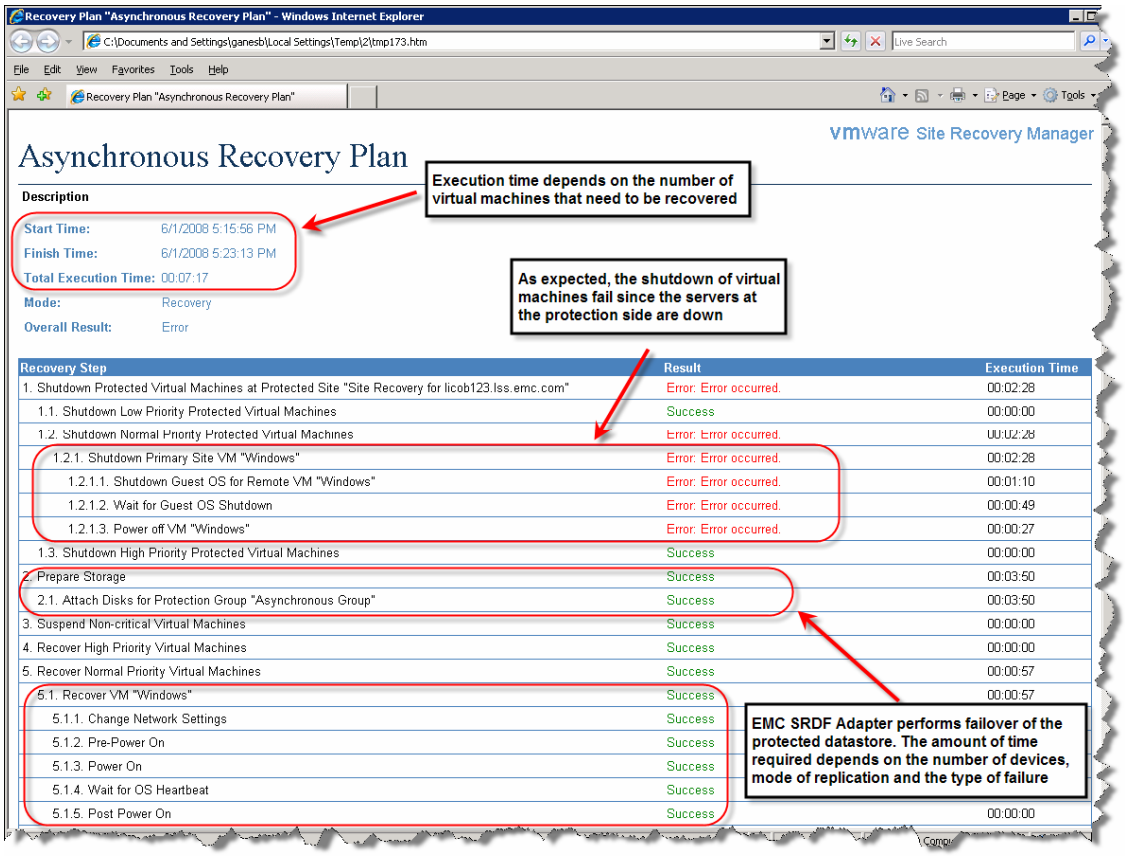

Figure 22. Report from VMware Site Recovery Manager after execution of a recovery plan

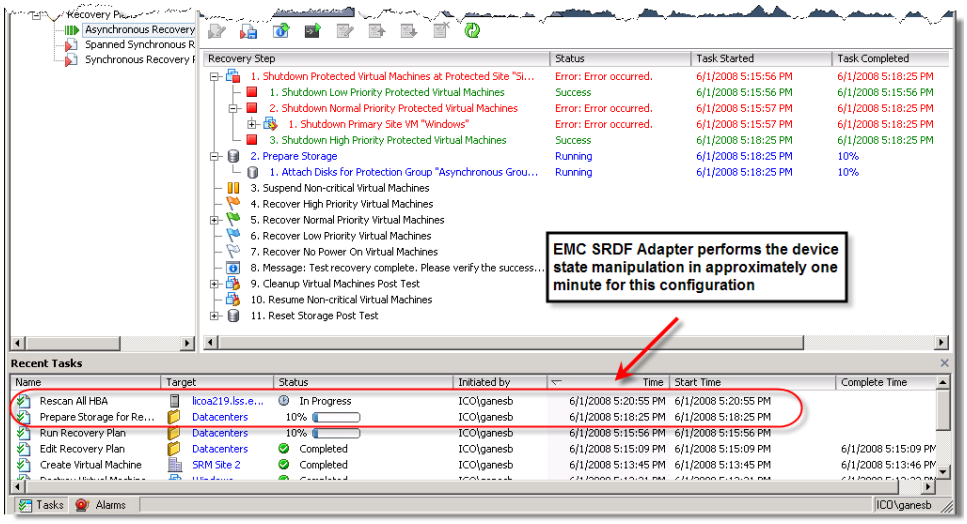

Figure 23. Display showing the time required for EMC SRDF Adapter to fail over devices

The state of the replication for the impacted devices, as shown in Figure 24, can be determined by utilizing the EMC Solutions Enabler commands for managing EMC SRDF. Comparing the contents of the figure with Figure 21 on page 23 shows that the device group type has changed from RDF2 to RDF1. The change occurred since EMC SRDF Adapter was successful in swapping the personality of the devices associated with the datastore srm_async. This can also be determined by noticing the fact that remote Symmetrix/DMX is now reported as 190101906, which is the serial number of the DMX array at the protection side. The serial number of the DMX array at the recovery site, 190102186, is reported as the source storage array. EMC SRDF Adapter also automatically maintains the mode of the replication. Since the replication from the protection side to the recovery side was conducted using SRDF/Asynchronous, the mode of SRDF after performing the swap is changed to SRDF/Asynchronous. This fact is highlighted in Figure 24.

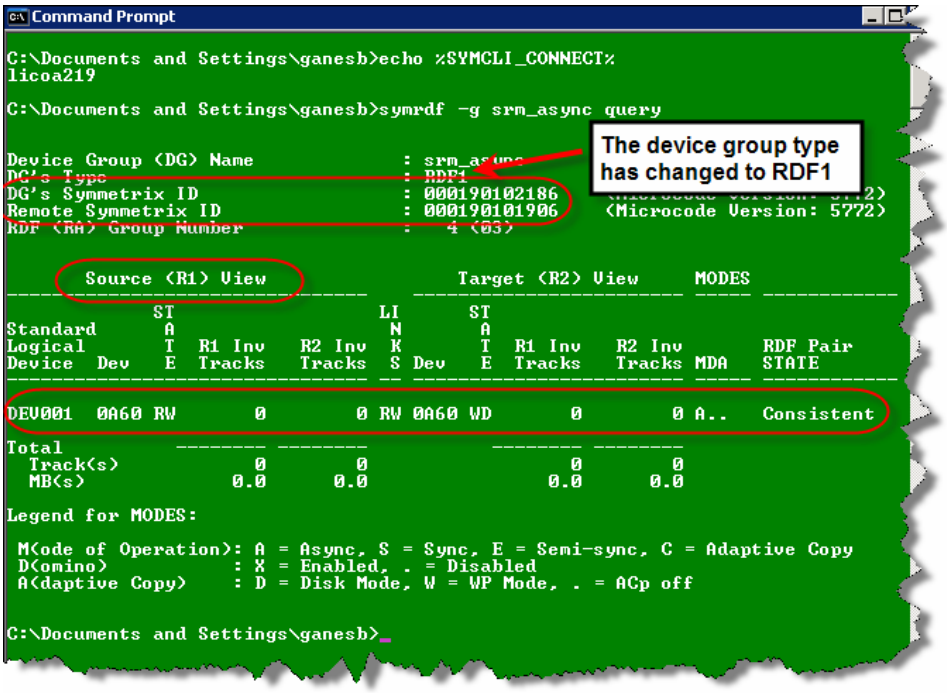

Figure 24. Querying the status of the SRDF state after executing a recovery plan

Figure 25 shows the output of `symrdf query` after executing the recovery plan. The recovery plan was executed after simulating a complete site failure. In this case, the DMX array at the recovery side cannot communicate with the storage array on the protection side. The lack of communication between the two arrays can be seen in the output of the command (denoted by the state "Partitioned").

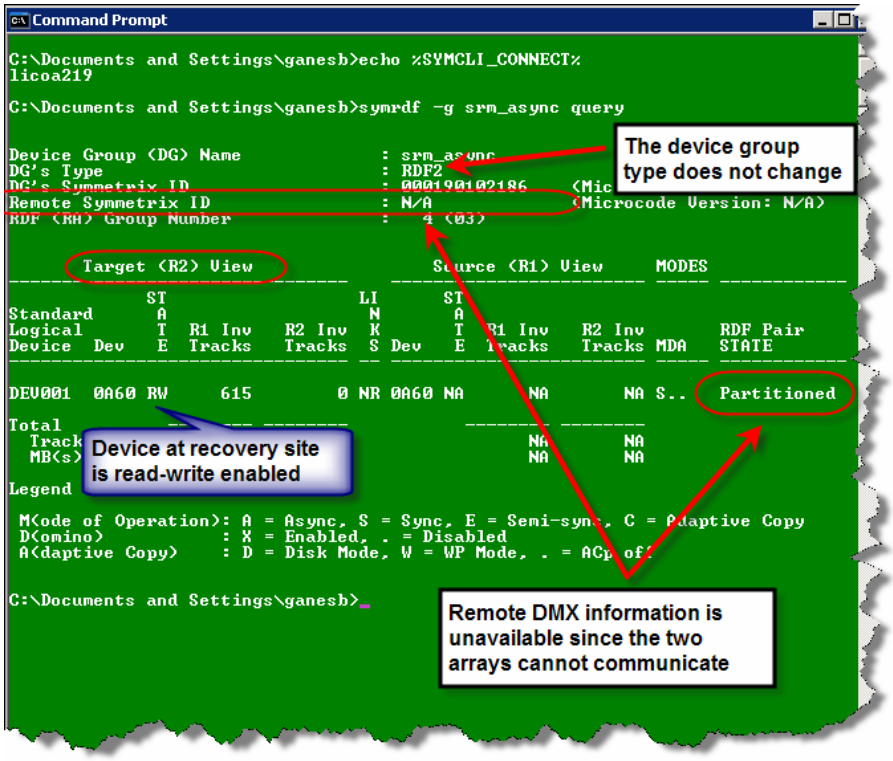

Figure 25. Querying the status of the SRDF state after complete protection site failure

EMC SRDF Adapter for VMware Site Recovery Manager automatically determines the state of the RDF devices and enables the appropriate devices on the recovery site for read-write access. This is highlighted in Figure 25.

Based on the previous discussion, it should be clear to astute readers that EMC SRDF Adapter for VMware Site Recovery Manager hides the complexity of deciding the most appropriate course of action in the event of a disaster. Furthermore, the adapter also selects the action that provides the easiest mechanism for the customer to fail back from the recovery side to the protection side.

Failback from the recovery site to the protection site

VMware Site Recovery Manager does not provide fully automated failback from the recovery side to the protection side. The failback process requires manual intervention and depends on the type of failure that necessitated the execution of the recovery plan. The type of failures can be broadly classified into three categories:

- Temporary failure of the compute environment at the protection site. In this type of failure, the DMX array on the protection site continues to communicate with the recovery site. As discussed in the previous section, in this failure scenario, the EMC SRDF Adapter for VMware Site Recovery Manager automatically reverses the replication from the recovery site to the protection site.
- Temporary failure of the protection site in which there is a complete disruption to the services. The EMC SRDF Adapter for VMware Site Recovery Manager read-write enables the appropriate devices at the recovery site when recovery plans are executed. When the protection site VMware Infrastructure and storage environment is restored, the state of the SRDF link is equivalent to performing a split of the SRDF link.
- Permanent failure of the protection site results in a complete destruction of the equipment. The recovery from such a state is no different from the initial setup of VMware Site Recovery Manager. The only difference is the recovery site would be treated as the protection site and vice versa. Therefore, recovery from catastrophic failures will not be discussed in this white paper.

The following sections describe the procedures that need to be invoked to successfully fail back from the recovery site to the protection site. The procedures only present the activities that need to be performed on the storage array and the VMware Infrastructure environment. It is important to note that a number of other activities may have to be performed on IT components such as storage area and IP networks before full services can be restored at the protection site.

Temporary failure of the compute environment

The EMC SRDF Adapter for VMware Site Recovery Manager automatically performs a dynamic swap of the SRDF relationship if the communication links between the DMX arrays at the protection and recovery site remain available. The results after the execution of the recovery plan in this type of failure scenario was discussed in the section, "Executing recovery plans during disasters" on page 23. The anticipated state of the devices after the execution of the recovery plan can be viewed in Figure 24.

When the VMware Infrastructure environment at the protection site is restored, the VMware ESX server at the protection site cannot access the devices it previously had access to. VMware VirtualCenter, therefore, reports all of the virtual machines hosted on the failed over datastores as "inaccessible." Furthermore, all datastores that were successfully failed over to the recovery site during the disaster are no longer available to the VMware ESX servers at the protection site. An example of this is shown in Figure 26.

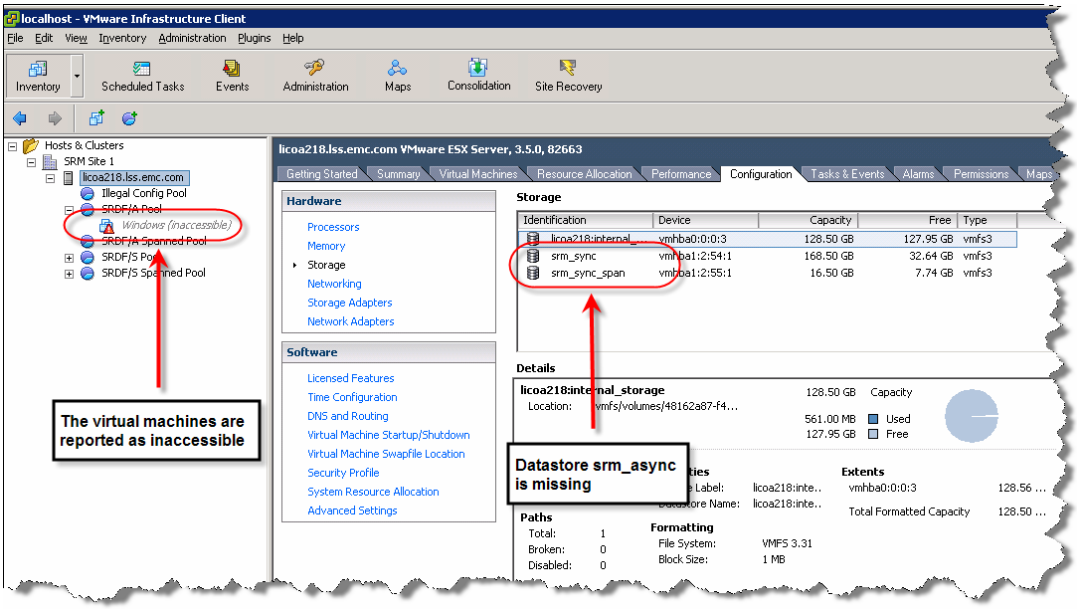

Figure 26. VMware Infrastructure environment at the protection site

The following process needs to be followed to fail back from the recovery site:

1. At the protection site, remove all virtual machines associated with the failed over datastore from the inventory by right-clicking on the virtual machines and selecting the option **Remove from Inventory**.[7]

2. On the recovery site, ensure that the RDF states for the devices that would be failed back are in a "Synchronized" (for SRDF/Synchronous) or "Consistent" (for SRDF/Asynchronous) state. An example of this was shown previously in Figure 24. Please contact EMC support if any other state is reported. Furthermore, do not continue with the rest of the procedure if the state of the device pairs is different.

[7] Special permissions assigned to the virtual machines may be lost during this process. The customer should note these permissions so they can be restored later.

3. VMware Site Recovery Manager can be leveraged to fail back from the recovery site to the protection site. This is possible since the failover from the protection site to the recovery site resulted in the swap of the devices' RDF personalities. The datastore srm_async that was failed over in the previous section will be used to describe the failback process. On the VMware Site Recovery Manager server at the recovery site, define an array manager using the process described in the section titled, "Configuring EMC SRDF Adapter"[8].

4. A new protection group should be defined on the VMware Site Recovery Manager Server at the recovery site. A recovery plan utilizing the protection group should then be created on the VMware Site Recovery Manager at the protection site. The procedure to create protection groups and recovery plans is beyond the scope of this white paper. Readers should consult VMware documentation available on the VMware website for further details. However, to elucidate the failback process, as shown in Figure 27, the protection group and recovery plan were created for the "srm_async" datastore that was failed over.

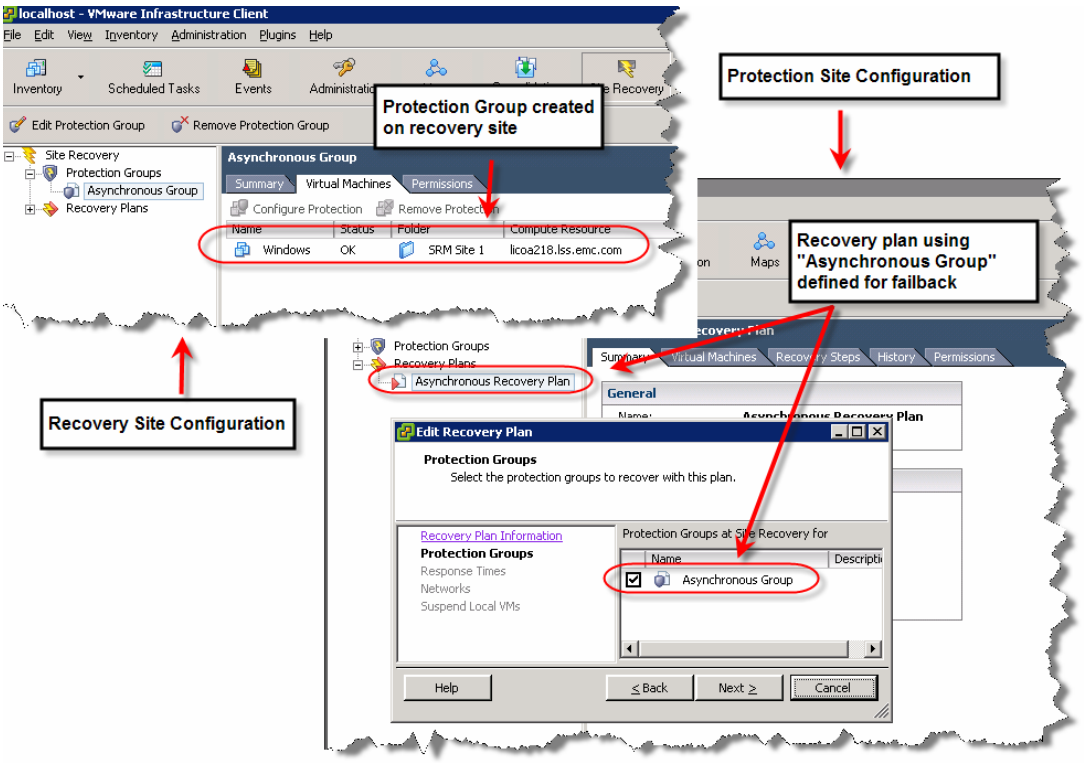

Figure 27. Failing back from the recovery site to the protection site

5. The failback from recovery site to the protection site can be initiated by executing the recovery plan at the appropriate time. The failback process automatically shuts down the impacted virtual machine at the recovery site to ensure no data loss occurs during the failback process.

6. Once the failback process successfully completes, the protection groups and recovery plans created for the failback process should be deleted. Furthermore, since the failover and failback process resignatures the impacted datastores, the protection group originally created for the datastore on the protection site and the associated recovery plan created on the recovery site are no longer valid. This

[8] This step is unnecessary if the VMware Site Recovery Manager has been configured for bi-directional support. If bi-directional configuration is in place, the failed over datastores can be discovered by performing a rescan of the array in the VMware Site Recovery Manager user interface.

can be seen in Figure 28. The impacted protection group and recovery plan should be deleted and re-created.

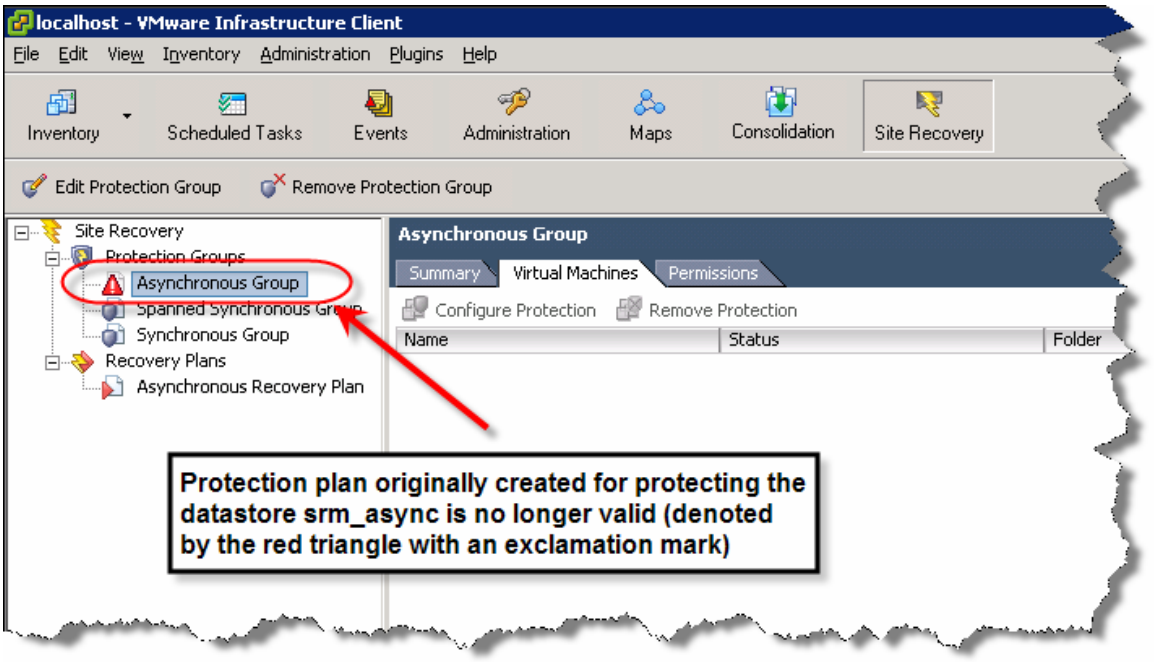

Figure 28. Invalidation of the protection group originally created at the protection site

Temporary failure of the protection site

The EMC SRDF Adapter for VMware Site Recovery Manager cannot perform a dynamic swap of the SRDF relationship when the communication links between the protection and recovery site are disrupted. The results after the execution of the recovery plan in this type of failure scenario were discussed in the section "Executing recovery plans during disasters" on page 26. The anticipated state of the devices after the execution of the recovery plan can be viewed in Figure 25 on page 26.

When the VMware Infrastructure environment at the protection site is restored, as seen in Figure 29, the VMware ESX server at the protection site has read-write access to the devices. The user can power on the virtual machines at the protection site, resulting in changed data at both the protection and recovery site. The only way to recover from that situation is to ignore the changes to one of the two sites, thus causing data loss. Therefore, it is critical to ensure that the power state of the virtual machines at the protection site is not manipulated after the protection site is restored.

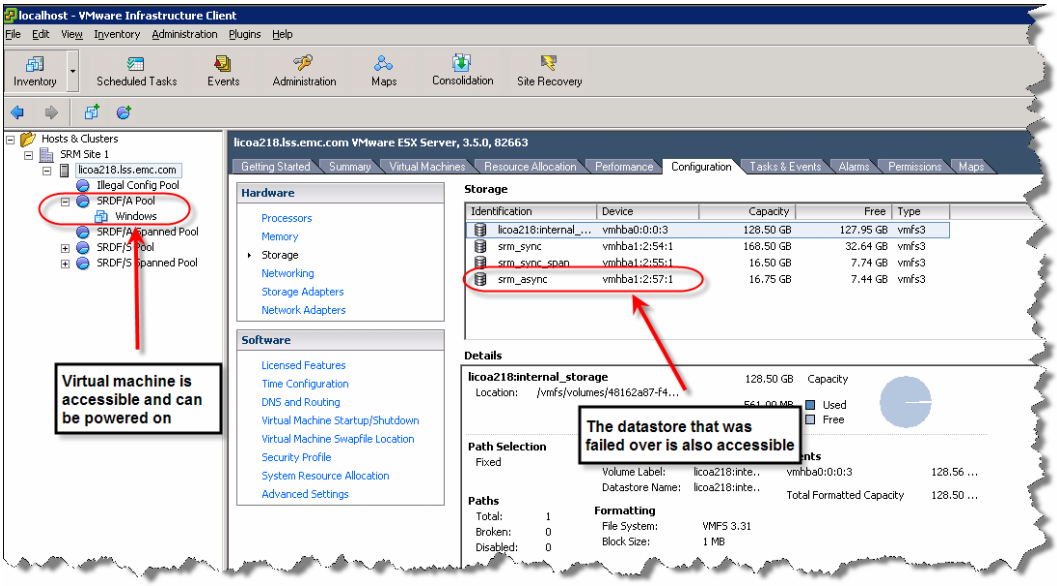

Figure 29. Virtual Infrastructure environment at the protection site after it is restored

The procedure described in the previous section can be used when recovering from a complete site failure. However, before the procedure is utilized, additional steps are required to bring the devices into an appropriate state since the personality of the devices was not swapped during the failover. The following additional steps need to occur before the procedure described in the previous section is used:

1. On the recovery site, ensure that the RDF state for the devices that would be failed back is in a "Split" state. An example is shown in Figure 30. Please contact EMC support if any other state is reported. Furthermore, do not continue with the rest of the procedure if the state of the device pairs is different.

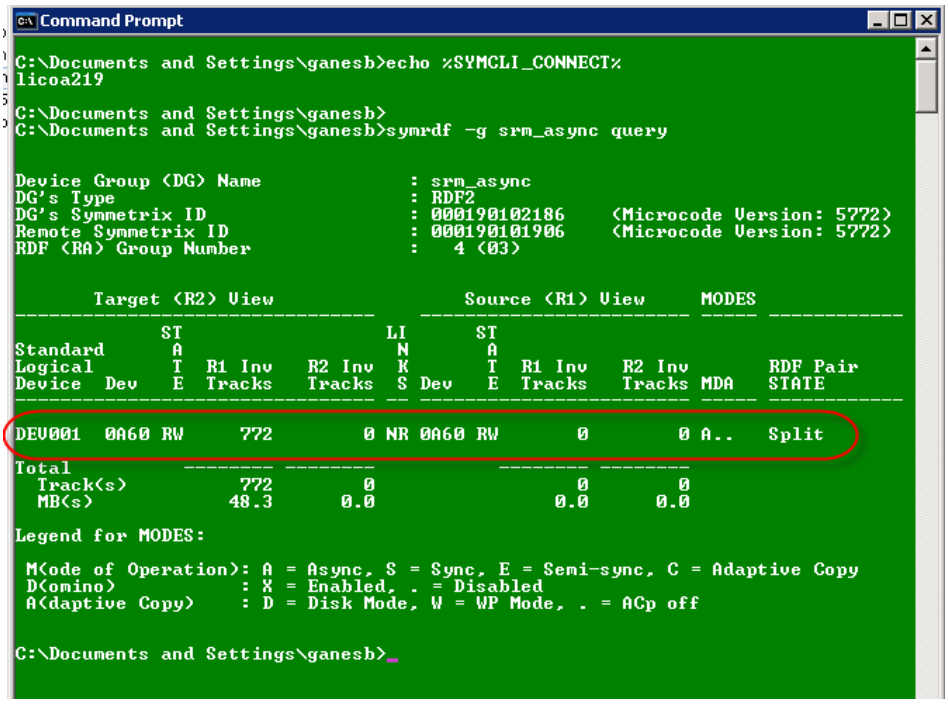

Figure 30. The state of the SRDF device pair after restoration of the DMX array at the protection site

2. The personality of the devices needs to be swapped, and the replication restarted before the failback process can begin. The personality of the devices can be swapped only if the device with the R1 personality is changed to a read-only state. The command, "`symdev –sid <SN> -nop write_disable dev <dev #>`", where `<SN>` is the serial number of the DMX array at the protection site, and `<dev #>` is the R1 device, write disables the appropriate devices at the protection site. This is shown in Figure 31 for the device pair associated with the datastore srm_async.

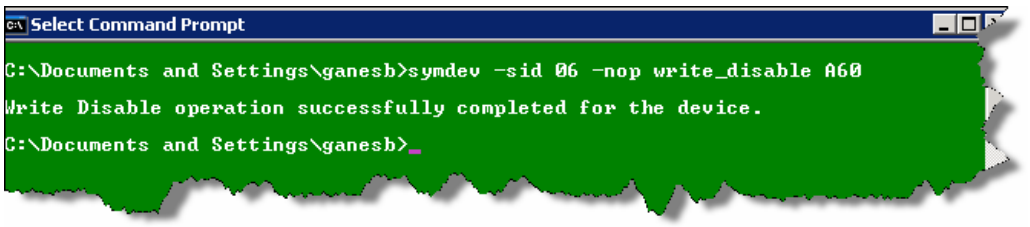

Figure 31. Write disabling R1 devices impacted by the failback procedure

3. The command, "`symrdf –g <dg_name> -nop swap`", where `<dg_name>` is the name of the device group, should be used to swap the personalities of the devices. This is shown in Figure 32 for the devices associated with the srm_async datastore.

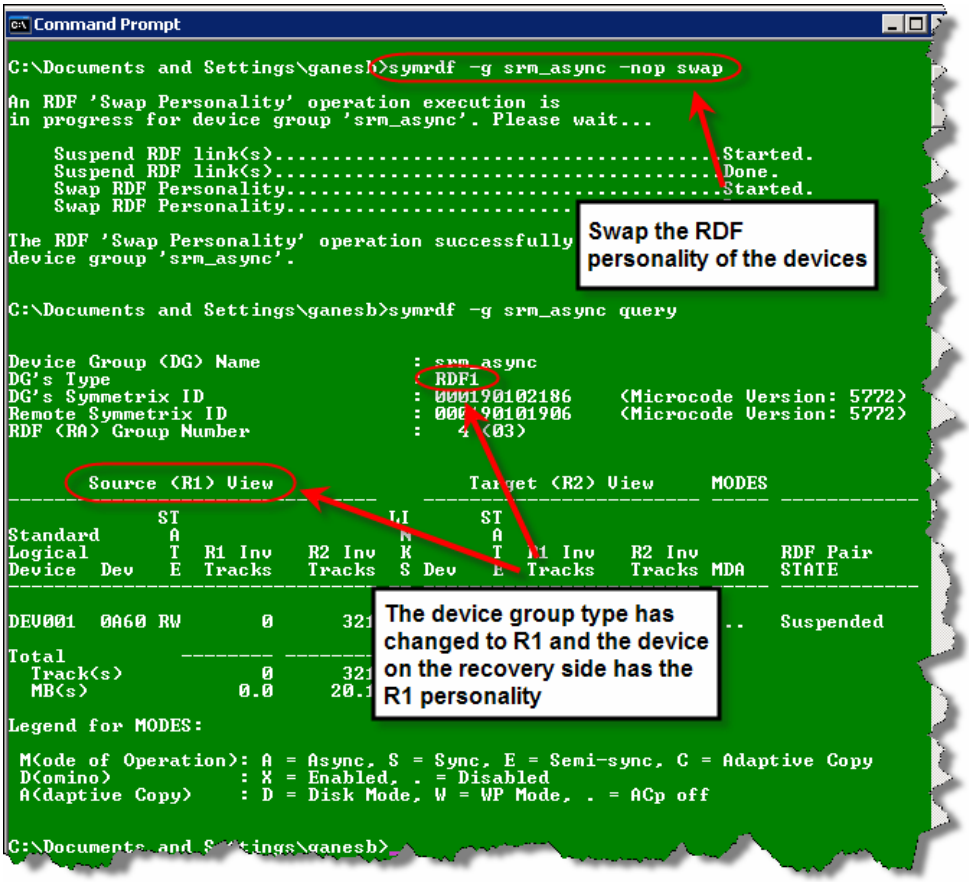

Figure 32. Performing device personality swaps

4. The replication from the recovery site to the protection site can be restarted at this point by executing the command, "`symrdf –g <dg_name> -nop establish`", where `<dg_name>` is the name

of the device group associated with the datastore that is being failed over. This step as applied to the srm_async datastore devices is shown in Figure 33.

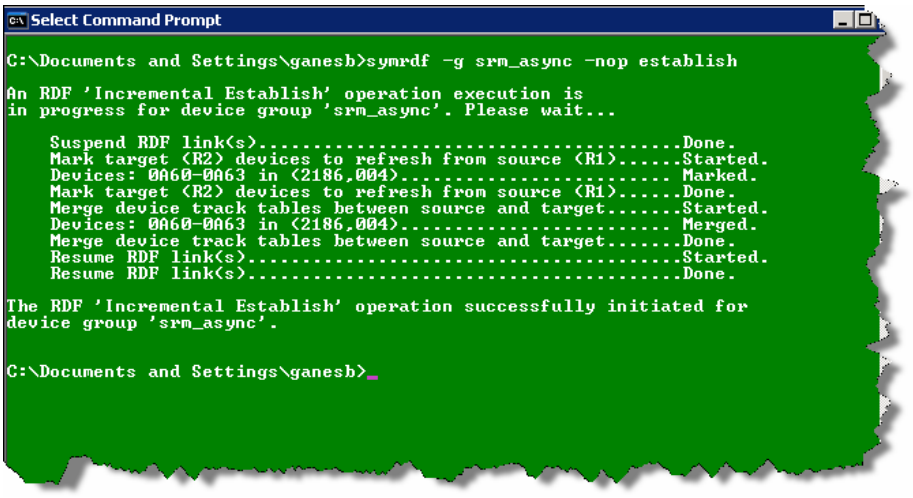

Figure 33. Restarting the synchronization of the data from the recovery site

5. The state of the RDF links after the resynchronization process for the devices associated with the datastore srm_async is completed and is shown in Figure 34. A quick comparison with Figure 24 on page 25 clearly shows that the state of the devices and the RDF links are equivalent. Therefore the procedure listed in the previous section ("Temporary failure of the compute environment") can now be used to fail back the datastore from the recovery site to the protection site.

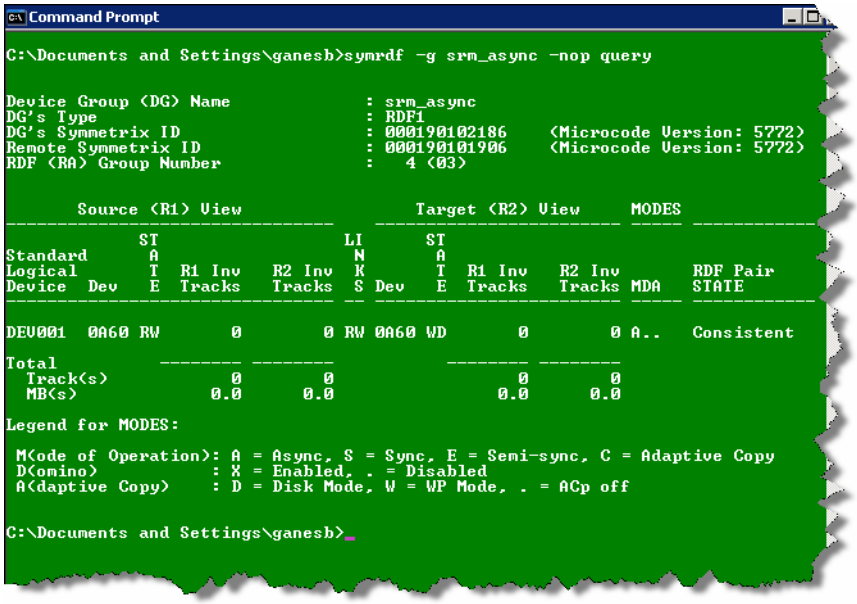

Figure 34. Querying the state of replication and the status of RDF links

Conclusion

VMware Site Recovery Manager in conjunction with EMC SRDF Adapter simplifies the creation and management of business continuance and disaster restart plans for VMware Infrastructure on EMC Symmetrix storage arrays. The integrated solution also allows customers to test their business continuance plan with minimal impact on the production environments. VMware Site Recovery Manager with EMC

SRDF Adapter leverages industry-leading and best-of-breed remote replication software, EMC SRDF, and local replication software, EMC TimeFinder, to protect customers' VMware Infrastructure.

References

- *VMware Infrastructure 3 Documentation: Introduction to VMware Infrastructure*
- *VMware Infrastructure 3 Documentation: Basic System Administration*
- *VMware Infrastructure 3 Documentation: ESX Server 3 Configuration Guide*
- *VMware Infrastructure 3 Documentation: Fibre Channel SAN Configuration Guide*
- *VMware Site Recovery Manager Administration Guide*
- *EMC Symmetrix Remote Data Facility (SRDF) Product Guide*
- *EMC Solutions Enabler Installation Guide*
- *EMC Solutions Enabler Symmetrix Array Management CLI Product Guide*
- *EMC Solutions Enabler Symmetrix SRDF Family CLI Product Guide*
- *EMC Solutions Enabler Symmetrix TimeFinder Family CLI Product Guide*

VMware, Inc. 3401 Hillview Ave Palo Alto, CA 94304 USA Tel: 1-877-486-9273 Fax: 650-427-5001www.vmware.com

vmware®

EMC²
where information lives®