Preface

Chapter 1  About Cluster Enabler

Cluster Enabler overview .............................................................. 16
  Cluster Enabler components .................................................. 19
SRDF overview .............................................................................. 20
MirrorView/S overview ............................................................... 22
Cluster Enabler common features ............................................ 25
  Multiple CE cluster management ........................................... 26
Windows Server 2008 support ................................................... 26
CE Installation Wizard ............................................................... 27
CE Configuration Wizard ............................................................ 27
Quorum model support ............................................................... 28
Delay failback ............................................................................ 28
Logging capabilities ................................................................. 30
Mount point support ................................................................. 30
SRDF/CE-specific features .......................................................... 33
  Multiple Symmetrix array support ....................................... 33
SRDF/Asynchronous compatibility ........................................... 33
SRDF/CE swap support ............................................................. 34
SRDF/CE configuration with multiple remote adapters .......... 35
CE geographic cluster system .................................................. 36
  Cluster Enabler modes of operation ....................................... 39
Pre-SRDF/CE clustering considerations .................................. 41
Microsoft Failover Clusters ....................................................... 43
  Microsoft Failover Cluster concepts ...................................... 45
Microsoft Failover Cluster modes of operation ....................... 46
Application software in a cluster environment ......................... 48
Contents

- Storage component................................................................. 102
  Adding and removing devices from a group .......................105
- Viewing information...................................................................... 106
  Displaying group information...............................................106
  Displaying node information...............................................109
  Displaying site information.................................................112
- Cluster Enabler logging.......................................................... 115
  Disk space requirements.......................................................115
  Extracting logs........................................................................116
  Changing the logging level....................................................118
  Changing the logging directory.............................................118
  Changing logging retention period.......................................118
- Restore and recovery operations.................................................. 119
  SRDF/CE recovery procedures...............................................119
  MirrorView/CE recovery procedures......................................127
- Configuring a custom resource.................................................. 131
  Using CE Manager to create a custom resource CE Group ....134
  Using CE Manager to edit a custom resource CE Group .........137

Appendix A  Manual Installation

- Manual Installation upgrade using CLI................................. 142
  Command line notes...........................................................142
  Product code GUIDs...........................................................143

Glossary..................................................................................145

Index
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview example of an SRDF/CE cluster configuration</td>
<td>17</td>
</tr>
<tr>
<td>Overview example of a MirrorView/CE cluster configuration</td>
<td>18</td>
</tr>
<tr>
<td>Basic SRDF configuration</td>
<td>21</td>
</tr>
<tr>
<td>Basic MirrorView/CE configuration</td>
<td>23</td>
</tr>
<tr>
<td>Lateral and peer nodes in SRDF backup operations</td>
<td>29</td>
</tr>
<tr>
<td>A geographically distributed two-node CE cluster</td>
<td>36</td>
</tr>
<tr>
<td>A geographically distributed four-node SRDF/CE cluster</td>
<td>37</td>
</tr>
<tr>
<td>Multiple SRDF/CE clusters supported on an SRDF link</td>
<td>38</td>
</tr>
<tr>
<td>Two-node two-cluster SRDF/CE configuration</td>
<td>40</td>
</tr>
<tr>
<td>Recommended cabling configuration</td>
<td>41</td>
</tr>
<tr>
<td>A typical two-node Microsoft failover cluster</td>
<td>44</td>
</tr>
<tr>
<td>A typical four-node Microsoft failover cluster</td>
<td>45</td>
</tr>
<tr>
<td>Cluster Enabler failover operation</td>
<td>51</td>
</tr>
<tr>
<td>Types of complete site failure</td>
<td>55</td>
</tr>
<tr>
<td>Lateral and peer nodes</td>
<td>58</td>
</tr>
<tr>
<td>MNS clusters with file share witness</td>
<td>60</td>
</tr>
<tr>
<td>Cluster Enabler Manager window</td>
<td>82</td>
</tr>
<tr>
<td>CE Manager Configuration Wizard</td>
<td>86</td>
</tr>
<tr>
<td>CE Manager expanded navigation tree</td>
<td>88</td>
</tr>
<tr>
<td>Windows Server 2008 supported quorum models</td>
<td>93</td>
</tr>
<tr>
<td>Select Quorum Disk</td>
<td>94</td>
</tr>
<tr>
<td>Create Group Wizard, Select Symmetrix Devices</td>
<td>96</td>
</tr>
<tr>
<td>Create Group Wizard, Select CLARiiON Devices</td>
<td>96</td>
</tr>
<tr>
<td>Create Group Wizard, Symmetrix Select Group Policy</td>
<td>97</td>
</tr>
<tr>
<td>Create Group Wizard, CLARiiON Select Group Policy</td>
<td>98</td>
</tr>
<tr>
<td>Modify Group Wizard, Select Devices</td>
<td>99</td>
</tr>
<tr>
<td>Modified group with added device</td>
<td>100</td>
</tr>
<tr>
<td>Example of Symmetrix storage array view</td>
<td>102</td>
</tr>
<tr>
<td>Example of CLARiiON Storage array view</td>
<td>103</td>
</tr>
<tr>
<td>CE Manager storage actions</td>
<td>105</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>31</td>
<td>CE Manager Groups component</td>
</tr>
<tr>
<td>32</td>
<td>CE Manager groups information</td>
</tr>
<tr>
<td>33</td>
<td>CE Manager Nodes component</td>
</tr>
<tr>
<td>34</td>
<td>CE Manager node information</td>
</tr>
<tr>
<td>35</td>
<td>CE Manager Sites component</td>
</tr>
<tr>
<td>36</td>
<td>CE Manager Symmetrix site information</td>
</tr>
<tr>
<td>37</td>
<td>CE Manager CLARiiON site information</td>
</tr>
<tr>
<td>38</td>
<td>Recover CE Cluster Enter Node Name</td>
</tr>
<tr>
<td>39</td>
<td>Recover CE Cluster Choose Tasks</td>
</tr>
<tr>
<td>40</td>
<td>Recover CE Cluster Change Cluster Number</td>
</tr>
<tr>
<td>41</td>
<td>Microsoft Cluster Administrator, Generic Application Resource Type</td>
</tr>
<tr>
<td>42</td>
<td>Cluster properties</td>
</tr>
<tr>
<td>43</td>
<td>Cluster properties with Generic Application</td>
</tr>
<tr>
<td>44</td>
<td>Select custom resource devices</td>
</tr>
<tr>
<td>45</td>
<td>Select Group Policy, custom resource</td>
</tr>
<tr>
<td>46</td>
<td>Microsoft Cluster Administrator, EMC_Group 4</td>
</tr>
<tr>
<td>47</td>
<td>Select devices, custom resource</td>
</tr>
<tr>
<td>48</td>
<td>Validate selection, custom resource</td>
</tr>
<tr>
<td>49</td>
<td>Summary of Group 4, custom resource</td>
</tr>
</tbody>
</table>
As part of its effort to continuously improve and enhance the performance and capabilities of the EMC product line, EMC periodically releases revisions of its hardware and software. Therefore, some functions described in this document may not be supported by all revisions of the software and hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a Cluster Enabler feature does not function properly or does not function as described in this guide, please contact the EMC Customer Support Center for assistance.

**Audience**

This guide is part of the EMC Cluster Enabler for Microsoft Failover Clusters documentation set and is intended for use by system administrators during installation, system setup, and routine operations.

*Note:* Previously, this guide was titled the *EMC SRDF/Cluster Enabler for MSCS Product Guide.*

System administrators working with Cluster Enabler must be proficient in the use of the following products:

- **Microsoft products:**
  - Windows server 2003 or 2008 Enterprise and Datacenter Editions, as installed
  - Microsoft Failover Clusters, previously referred to as Microsoft Cluster Server (MSCS)
EMC Symmetrix storage arrays, as per your Cluster Enabler product version and the following applicable software:
- Solutions Enabler (SYMCLI/SYMAPI)
- EMC Symmetrix Remote Data Facility (SRDF)
- EMC ControlCenter Symmetrix Remote Data Facility (SRDF) Manager, if installed
- EMC PowerPath, if installed

EMC CLARiiON storage arrays, as per your Cluster Enabler product version and the following applicable software:
- EMC Navisphere Manager or Navisphere CLI
- EMC MirrorView/Synchronous
- EMC PowerPath, if installed

Organization

Here is an overview of where information is located in this guide:

Chapter 1, “About Cluster Enabler,” provides a high-level overview of clustering, Microsoft Failover Clusters, SRDF, MirrorView, and how EMC Cluster Enabler provides disaster recovery protection.

Chapter 2, “Cluster Behavior,” describes cluster behavior in various operation modes.

Chapter 3, “Installation and Upgrades,” provides instructions and lists requirements for installing and configuring the EMC Cluster Enabler Manager using the installation wizard.

Chapter 4, “Using Cluster Enabler Manager,” provides instructions for using the Cluster Enabler Manager (graphical user interface).

Appendix A, “Manual Installation,” describes how to manually install the Cluster Enabler Manager using the command line interface.

Related documentation

The following documentation from EMC Corporation contains information that may be helpful in a Cluster Enabler environment.

EMC Solutions Enabler:
- 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
- EMC Solutions Enabler Installation Guide
EMC ControlCenter:
- EMC ControlCenter Installation Planning Booklet
- EMC ControlCenter Guidebook
- EMC ControlCenter Installation Guide
- Symmetrix SRDF Host Component Product Guide

EMC PowerPath:
- EMC PowerPath Product Guide
- EMC PowerPath Product Overview Whitepaper

EMC MirrorView/S:
- EMC MirrorView/Synchronous Command Line Interface (CLI) Reference
- Navisphere Manager Help

Fibre Channel:
- Symmetrix Fibre Channel Product Guide

**Related third-party documentation**

The following Microsoft documentation contains information about or related to the products discussed in this guide:

- Microsoft’s Cluster Server documentation set, especially the *Microsoft Cluster Server Administrator’s Guide*, Document No. X0327902
- *Step-by-Step Guide to Installing Cluster Service*, Microsoft Technical Library

**Conventions used in this document**

EMC uses the following conventions for special notices.

- **Note**: A note presents information that is important, but not hazard-related.

- **CAUTION**
  A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

- **IMPORTANT**
  An important notice contains information essential to operation of the software. The important notice applies only to software.
**Typographical conventions**

EMC uses the following type style conventions in this document:

**Normal**: Used in running (nonprocedural) text for:
- Names of interface elements (such as names of windows, dialog boxes, buttons, fields, and menus)
- Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, filenames, functions, utilities
- URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, notifications

**Bold**: Used in running (nonprocedural) text for:
- Names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system call, man pages

Used in procedures for:
- Names of interface elements (such as names of windows, dialog boxes, buttons, fields, and menus)
- What user specifically selects, clicks, presses, or types

**Italic**: Used in all text (including procedures) for:
- Full titles of publications referenced in text
- Emphasis (for example a new term)
- Variables

**Courier**: Used for:
- System output, such as an error message or script
- URLs, complete paths, filenames, prompts, and command syntax.

**Courier bold**: Used for:
- Specific user input (such as commands)

**Courier italic**: Used in procedures for:
- Variables on command line
- User input variables

**<>**: Angle brackets enclose parameter or variable values supplied by the user

**[]**: Square brackets enclose optional values

**|**: Vertical bar indicates alternate selections - the bar means “or”

**{}**: Braces indicate content that you must specify (that is, x or y or z)

**...**: Ellipses indicate nonessential information omitted from the example
Where to get help

EMC support, product, and licensing information can be obtained as follows.

Product information — For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to the EMC Powerlink website (registration required) at:

http://Powerlink.EMC.com

Technical support — For technical support, go to EMC Customer Service on Powerlink. To open a service request through Powerlink, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send your opinion of this document to:

techpub_comments@EMC.com
This chapter provides a high-level overview of clustering and explains how EMC Cluster Enabler provides disaster recovery protection in geographically distributed Microsoft Failover Clusters using either Symmetrix Remote Data Facility (SRDF) or CLARiiON MirrorView.

**Important:** EMC recommends reading this chapter in its entirety before installing and configuring Cluster Enabler for Microsoft Failover Clusters.

- Cluster Enabler overview ................................................................. 16
- SRDF overview .............................................................................. 20
- MirrorView/S overview ................................................................. 22
- Cluster Enabler common features ................................................. 25
- SRDF/CE-specific features ............................................................. 33
- CE geographic cluster system ...................................................... 36
- Microsoft Failover Clusters ......................................................... 43
- Application software in a cluster environment .............................. 48
Cluster Enabler overview

Cluster Enabler (CE) for Microsoft Failover Clusters is a software extension of failover clusters functionality. Cluster Enabler allows Windows Server 2003 and 2008 Enterprise and Datacenter editions running Microsoft Failover Clusters to operate across multiple connected storage arrays in geographically distributed clusters. Formerly, Microsoft Failover Clusters were called server clusters, which used Microsoft Cluster Server (MSCS). Cluster Enabler supports configurations of either SRDF-connected Symmetrix® arrays or MirrorView™/Synchronous™-connected CLARiiON® arrays.

Cluster Enabler software is available in two separate versions:

- SRDF®/Cluster Enabler (SRDF/CE) for Microsoft Failover Clusters (for use with Symmetrix storage arrays)
- MirrorView/Cluster Enabler (MirrorView/CE) for Microsoft Failover Clusters (for use with CLARiiON storage arrays)

Once configured using the EMC Cluster Enabler Manager graphic user interface (GUI), Microsoft Failover Clusters are referred to as CE clusters. SRDF/CE software can support up to 64 shared quorum disk clusters per mirrored pair. There is no limit on the number of Majority Node Set (MNS) clusters per mirrored pair.

**Important:** Symmetrix SRDF and CLARiiON MirrorView/S devices cannot be part of the same CE cluster. Mixed storage configurations are not supported.

Cluster Enabler expands the range of cluster storage and management capabilities while ensuring full business continuance protection. An iSCSI or Fibre Channel connection from each cluster node is made to its own storage array. Two storage arrays are connected through either an SRDF link (for Symmetrix arrays) or a MirrorView link (for CLARiiON arrays) to provide automatic failover of mirrored volumes during a Microsoft failover cluster node failover.

This connection effectively extends the distance between cluster
nodes (depending on network latency) and forms a geographically
distributed cluster with disaster-tolerant capabilities. ¹

Figure 1 on page 17 provides a graphical example of using Cluster
Enabler in an SRDF Symmetrix array environment.

Figure 2 on page 18 provides a graphical example of using Cluster
Enabler in a MirrorView/S CLARiiON array environment.

Cluster Enabler protects data from the following types of failures, 24
hour a day, 7 days a week, and 365 days per year:

- Storage failures
- System failures
- Site failures

1. The EMC Network Topology Guide provides additional information
   regarding distance restrictions for your specific configuration.
Figure 2  Overview example of a MirrorView/CE cluster configuration
Cluster Enabler overview

Cluster Enabler components

Cluster Enabler integrates Microsoft Failover Cluster software with Symmetrix or CLARiiON hardware and Solutions Enabler SYMAPI or CLARAPI software, allowing the seamless use of Symmetrix disks or CLARiiON LUNs to function as a single SCSI disk. Cluster Enabler achieves this using several components:

- **CE Manager** — An MMC-based (Microsoft Management Console) user interface that allows you to:
  - Configure operational parameters
  - Perform cluster tasks

- **CE Service** — Used for quorum device arbitration for SRDF/CE.

- **CE Resource.dll** — A .dll used by Microsoft failover cluster to perform group failover/failback operations for all group resources.

- **Quorum Filter Driver** — A component that performs arbitration or ownership protocol for the Microsoft failover cluster database quorum. Used for SRDF/CE.

- **CE WMI provider** — A Windows Management Instrumentation component that interfaces with the underlying Symmetrix or CLARiiON storage array and performs various operations such as failover, group creation, and so on, on the storage array.
The Symmetrix Remote Data Facility (SRDF) is a Symmetrix-based business continuance and disaster recovery solution sold as a separate license by EMC Corporation. In basic terms, SRDF is a configuration of multiple Symmetrix arrays whose purpose is to maintain multiple, real-time copies of logical volume data in more than one location.

SRDF duplicates production (source) site data to a recovery (target) site transparently to users, applications, databases, and host processors. If the primary site is not able to continue processing, data at the secondary site is current up to the last I/O transaction.

SRDF can be used in several key areas including, but not limited to:
- Disaster Recovery
- Remote Backup
- Data Center Migration
- SDMS—Symmetrix Data Migration Service
- Data Center Decision Solutions

When primary (source) systems are down, SRDF enables fast switch over to the recovery (target) copy of the data, allowing critical information to become available in minutes. Business operations and related applications may resume full functionality with minimal interruption.

Protecting against data loss allows the operations and applications to resume at the secondary site. SRDF can be used:
- By itself, and data processing can be resumed by powering up a standby system and manually restarting.
- In combination with more sophisticated software to automatically resume operations.

Figure 3 on page 21 illustrates a basic SRDF configuration.
SRDF/CE combines Microsoft Failover Clusters and SRDF to provide a more sophisticated solution. SRDF/CE provides an automated configuration wizard (refer to Chapter 4, Using Cluster Enabler Manager) to be used in conjunction with the Microsoft Cluster Administrator to administer the SRDF-enabled cluster.

**Note:** For greater detail on SRDF, consult the SRDF documentation set, “Related documentation” on page 10.

![Basic SRDF configuration](image)

Figure 3  **Basic SRDF configuration**

SRDF/CE supports both SRDF/Synchronous (SRDF/S) and SRDF/Asynchronous (SRDF/A) modes of transfer.
MirrorView/S overview

MirrorView/Synchronous (MirrorView/S) is a CLARiiON-based business continuance and disaster recovery solution that maintains a copy image of a logical unit (LUN) at a separate location. In the event of a serious accident or natural disaster at one location, the image at the other location is available for continuing data processing. You can quickly restore operations when a catastrophic event, such as a fire, destroys the storage media at the primary data center. By mirroring critical data to the remote site, you not only retain vital data but can also quickly restore operations by switching over to the secondary storage system.

MirrorView/S control operations are enabled and disabled through the production host for the primary storage system. Before devices can be mirror-imaged to a secondary system, a MirrorView link must be enabled between the two CLARiiON arrays. There exists two physical port connections between CLARiiON arrays, one for each storage processor. Connections must be made between the same storage processor and port for each CLARiiON array. Enabling the link allows for bi-directional I/O and control operations over either storage processor connection (MirrorView links). Figure 4 on page 23 provides an overview.

A remote mirror consists of a primary image and a secondary image. The production image (the one mirrored) is called the primary image; the copy image is called the secondary image. Each image resides on a separate storage system. The primary image receives I/O from a server called the production server; a separate storage system maintains the secondary image. This storage system can optionally have a failover/standby computer connected to it. Both storage systems can be in different domains. The client that is managing the storage system containing the primary images can fail over to the secondary image if the primary image becomes inaccessible.
MirrorView/S supports *consistency groups*. A consistency group is a set of synchronous mirrors whose secondary images need to be kept consistent with each other in order to be recoverable or crash-consistent. This allows an application to use the secondary images if the primary storage system fails.

**Figure 4** Basic MirrorView/S configuration

**Note:** For continued Cluster Enabler discussion purposes in this document, the term *device* also means LUN.
Note: The primary images of mirrors in a MirrorView/S consistency group must reside on a single storage system, and the secondary images of the mirrors must reside on a single (but different) storage system. This contrasts with volumes in a Symmetrix consistency group, which can reside on multiple storage systems.

MirrorView/CE combines Microsoft Failover Clusters and CLARiiON MirrorView/S to provide a more sophisticated failover solution. MirrorView/CE provides an automated configuration wizard to be used in conjunction with the Microsoft Cluster Administrator to administer the MirrorView-enabled cluster.

Note: For greater detail on MirrorView/S, consult the MirrorView/S documentation set (refer to “Related documentation” on page 10).
Cluster Enabler common features

Version 3.0 of Cluster Enabler for Microsoft Failover Clusters replaces the previous Version 2.2 graphic user interface (SRDF/CE for MSCS GUI). The improved GUI, now called Cluster Enabler (CE) Manager, provides several wizard processes to streamline cluster tasks and reduce the complexity of typical cluster management. Table 1 lists the various wizard processes that are now included in the CE Manager.

Table 1  Cluster Enabler Manager wizards

<table>
<thead>
<tr>
<th>Wizard</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Wizard</td>
<td>Configures failover clusters for management with Cluster Enabler</td>
</tr>
<tr>
<td>Create Group Wizard</td>
<td>Creates a CE group, adds devices and selects a group policy</td>
</tr>
<tr>
<td>Modify Group Wizard</td>
<td>Modifies a CE group to add or remove devices</td>
</tr>
<tr>
<td>Recover CE Cluster Wizard</td>
<td>Recovers a CE cluster</td>
</tr>
<tr>
<td>Change Quorum Wizard</td>
<td>Changes the quorum model of a cluster</td>
</tr>
<tr>
<td>Update Mirror Pairs Wizard</td>
<td>Updates the mirrored pairs in a cluster</td>
</tr>
<tr>
<td>Storage Discover Wizard</td>
<td>Discovers and sets up the attached storage for Cluster Enabler</td>
</tr>
</tbody>
</table>

Note: Chapter 4, Using Cluster Enabler Manager provides detailed descriptions and functionality for each wizard.

In addition to the wizard processes noted Table 1, the CE Manager provides various features that manage and monitor cluster, group, storage device, site, and node information. Chapter 4, Using Cluster Enabler Manager provides information on additional GUI features.

The following common features for both SRDF/CE and MirrorView /CE are included in Version 3.0:

- “Multiple CE cluster management” on page 26
- “Windows Server 2008 support” on page 26
- “CE Installation Wizard” on page 27
- “CE Configuration Wizard” on page 27
- “Quorum model support” on page 28
- “Delay failback” on page 28
About Cluster Enabler

◆ “Logging capabilities” on page 30
◆ “Mount point support” on page 30

The following listed features are specific to SRDF/CE:
◆ “Multiple Symmetrix array support” on page 33
◆ “SRDF/Asynchronous compatibility” on page 33
◆ “SRDF/CE swap support” on page 34
◆ “SRDF/CE configuration with multiple remote adapters” on page 35

Multiple CE cluster management

The Cluster Enabler V3.0 CE Manager lets you manage multiple CE clusters simultaneously, as long as all of the clusters are either Windows Server 2003 or 2008 clusters. To manage the cluster, CE Manager runs under the domain account. This account is part of local administrator group of every node of the cluster it manages.

Note: Mixing both Windows Server 2003 and 2008 clusters in one CE Manager session is not supported.

Windows Server 2008 support

Cluster Enabler for Microsoft Failover Clusters V3.0 now supports Windows Server 2008 Failover Clusters. The installation of Cluster Enabler requires that all nodes first be installed with the Failover Cluster feature. Cluster Enabler supports the following cluster models:

◆ No Majority: Disk Only
◆ Node Majority
◆ Node and Disk Majority
◆ Node and File Share Majority

Note: MirrorView/CE V3.0 for Windows Server 2008 supports only Node Majority, and Node and File Share Majority.

The Cluster Enabler configuration will not pass Cluster Validation Storage tests for the following reasons:
About Cluster Enabler

- Device unique identifiers are not same for both SRDF R1 and R2 devices.
- SCSI-3 persistent reservations on the R1 will not be applied to the R2.

**Note:** Cluster Enabler V3.0 does not support the Windows Server 2008 Core installation option.

---

### CE Installation Wizard

The CE Installation Wizard is a Windows Installer-based application that copies the Cluster Enabler code to the system and creates a Start menu shortcut for the EMC Cluster Enabler Manager. The CE Installation Wizard should be invoked when installing, upgrading, or removing either SRDF/CE or MirrorView/CE.

After running the Installation Wizard and rebooting, you can start EMC Cluster Enabler Manager by clicking **Start > Programs > EMC Corporation > Cluster Enabler > EMC Cluster Enabler Manager**.

**Note:** Chapter 3, Installation and Upgrades provides detailed information on the install process for your configuration using Installation Wizard.

---

### CE Configuration Wizard

Cluster Enabler provides a wizard for configuring a CE cluster. After installation, the configuration process is the first step in converting your failover clusters to geographically dispersed clusters. The Configuration Wizard will step you through the process of configuring your failover cluster for management with CE. SRDF/CE for Symmetrix arrays also allows you to configure shared quorum clusters.

**Note:** Chapter 4, Using Cluster Enabler Manager provides more information on the CE Configuration Wizard.
About Cluster Enabler

Quorum model support

Cluster Enabler supports all available quorum models in Windows Server 2003 and 2008 clusters with SRDF/CE. Cluster Enabler provides a wizard for changing the quorum model of a cluster. The Change Quorum Wizard will step you through the process of changing a cluster’s quorum model type. For Windows Server 2003, Cluster Enabler allows you to change the cluster model type between Shared Quorum, Majority Node Set (MNS), and MNS with File Share Witness. For Windows Server 2008, Cluster Enabler allows you to change the cluster model type between No Majority: Disk Only, Node Majority, Node and Disk Majority, and Node and File Share Majority. “Supported model type descriptions” on page 91 provides detailed descriptions of each model.

Note: MirrorView/CE V3.0 supports only Windows Server 2003 Majority Node Set (MNS), and MNS with File Share Witness or Windows Server 2008 Node Majority, and Node and File Share Majority.

Delay failback

Delay Failback capability is implemented as part of Cluster Enabler’s default functionality. Delay Failback automatically modifies the Preferred Owner list for each failover cluster group so that a failover will occur to a lateral node first, and if the lateral node is unavailable, to a peer node. Lateral nodes are defined as nodes connected to the same storage array. Peer nodes are defined as nodes connected to different storage arrays, located across the link from each other. Figure 5 on page 29 provides an example.

Cluster Enabler manipulates the Microsoft failover cluster (previously referred to as MSCS) Preferred Owners list whenever a group is brought online. CE then examines the group Preferred Owners list and determines which node is the lateral node. It can then modify the Preferred Owner list so the current node and its lateral partner are the first two in the list.
Figure 5  Lateral and peer nodes in SRDF backup operations

Note: In Figure 5, the Symmetrix storage configuration could also be substituted with CLARiiON arrays using MirrorView links.

Therefore, no matter which side a group is moved to, the Preferred Owner list is modified to allow a group to fail over to a lateral node, and not fail back or fail over across the link as a first option. Microsoft Failover Clusters only moves a group across the link as a last resort. This prevents the failover clusters from arbitrarily performing what amounts to a failback/failover across the link in an automatic fashion. This feature delays the actual failback of a group to a primary node, and is therefore termed delay failback.
Delay Failback runs simultaneously on all nodes. Therefore, when a group comes online on any node, the Preferred Owner list is updated, regardless of whether it is a primary or secondary device. For example, the sequence for Group \( x \) on Node 1 will be the following:

1. Delay Failback first determines if it *knows* the other nodes in the four-node cluster. This information is gathered by CE during normal operations. If not, the default feature is bypassed because it is unable to differentiate between a lateral node, peer node, and so on.

2. If Delay Failback *knows* the other nodes, then it determines if Group \( x \) has come online on Node 1.

3. If Group \( x \) has come online on Node 1, the Microsoft failover cluster Preferred Owner list is modified so that Node 1 is the first Preferred Owner, followed by the lateral node and then the peer nodes.

**Logging capabilities**

Cluster Enabler provides detailed logging features. If there is a problem with Cluster Enabler, detailed logs provide EMC Customer Support with the technical information necessary to help diagnose the problem and help Cluster Enabler engineers with debugging.

The logging facility captures detailed information, and the size and number of log files being created has increased compared to prior versions of SRDF/CE for MSCS.

The log compression and log retention features help to minimize the disk capacity utilized by log files. “Cluster Enabler logging” on page 115 provides more information.

**Mount point support**

Cluster Enabler supports mount points. By using mount points, you can overcome the limitation on drive letters, which makes it possible for a cluster to support more than 26 volumes.

For mount points to work correctly, all related disks must belong to the same cluster group. For SRDF/CE, all related disks must also belong the same RA group. If related disks are spread across multiple cluster groups, volumes cannot be brought online because cluster
groups can be online on different nodes. To avoid this scenario, Cluster Enabler first groups all related disks by identifying the mount points on a given disk and any disks upon which the given disk is mounted. Cluster Enabler then creates a parent/child relationship between the disks.

When a user chooses a disk to create a group (or adds a disk to an existing group), Cluster Enabler finds all related disks by traversing its parent/child relationships and adding every related disk to the group. It then adds appropriate dependencies between the disks so that the resources can be brought online in an orderly fashion.

Table 2 on page 31 illustrates a cluster example consisting of drive letters and mount points for six volumes. Using this configuration, you can see various parent/child relationships among the disks.

For example, the user chooses E:\MNT1. Therefore:

- E:\MNT1 is a mount point with E:\ as its parent.
- E:\ is a child of F:\. Thus, disk F:\ will be included in the group.
- F:\ has additional children F:\MNT2 and F:\MNT2\MNT3. Thus, the group will include these disks too.

The result of these parent/child relationships is that the group will include volumes 0BCE, 0BCF, 0BD0, 0BD1, and 0BD2. Each disk is dependent on its parent to come online. In this example, 0BCF is dependent on 0BCE, and 0BD0 is dependent on 0BCE, and so forth.

Of course, each group is also dependent on the Cluster Enabler resource.

Table 2  
Cluster mount point example

<table>
<thead>
<tr>
<th>Drive letter and mount point</th>
<th>Symmetrix volume ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>F:\</td>
<td>0BCE</td>
</tr>
<tr>
<td>F:\MNT1, E:\</td>
<td>0BCF</td>
</tr>
<tr>
<td>F:\MNT2</td>
<td>0BD0</td>
</tr>
<tr>
<td>F:\MNT2\MNT3</td>
<td>0BD1</td>
</tr>
<tr>
<td>D:\</td>
<td>0BCD</td>
</tr>
<tr>
<td>E:\MNT1</td>
<td>0BD2</td>
</tr>
</tbody>
</table>
When you delete a device, Cluster Enabler finds all related disks and deletes them too. For example, if the current mount points are F: and F:\MNT2 and F:\MNT2\MNT3, and if the device that corresponds to F:\MNT2 is deleted from the group, all three devices corresponding to F:, F:\MNT2, and F:\MNT2\MNT3 are deleted.

However, if you were to first delete mount point F:\MNT2 from the operating system and then delete its corresponding device from the group, Cluster Enabler would delete only the devices that correspond to F:\MNT2 and F:\MNT2\MNT3. The device corresponding to F:\ would be left in the group because, after the mount point deletion, it is no longer related to F:\MNT2.
SRDF/CE-specific features

This section details some of the Cluster Enabler features that are specific to SRDF/CE.

Multiple Symmetrix array support

- SRDF/Cluster Enabler for Microsoft Failover Clusters V3.0 supports the use of multiple Symmetrix arrays per cluster.

This feature provides greater flexibility to you and your storage provisioning.

SRDF/Asynchronous compatibility

SRDF/CE is compatible with EMC SRDF/Asynchronous (SRDF/A). SRDF/A is a high-performance, extended-distance asynchronous replication that uses a delta set architecture for reduced bandwidth requirements and no host performance impact.

Asynchronous mode provides a point-in-time image on the target (R2) device that is only slightly behind the source (R1) device. SRDF/A session data is transferred to the remote Symmetrix system in delta sets, eliminating the redundancy of same-track changes being transferred over the link, thereby reducing the required bandwidth. SRDF/A only needs enough bandwidth to support the average production workload versus peak workloads, provided there is enough Symmetrix cache to support the peak workloads.

SRDF/A is intended for users who require no host application impact while maintaining a consistent, restartable image of their data on the R2 side at all times.

Note: SRDF/CE always enables consistency on SRDF/A groups. SRDF/A consistency ensures that applications have a consistent copy on the remote side when they failover.

SRDF/CE supports Enginuity™ releases as outlined in the E-Lab Interoperability Navigator. At the 5x70 Enginuity level, you can specify a single SYMCLI group whose device members have been previously defined as SRDF/A enabled. Once configured, SRDF/CE automatically fails over this group to the target side as necessary. After the failover, when you want to fail back, SRDF/CE
automatically establishes a synchronous connection, waits until the data is propagated back, and then changes the SRDF mode back to asynchronous.

**Note:** SRDF/CE does not support clusters where the target (R2) side is larger than the source (R1) side. When the system fails over to the R2 side, it can never fail back since the R2 cannot resynchronize all its data back to the R1 side.

**Note:** SRDF/A is not supported for quorum group in shared quorum models. Other groups in the cluster may use synchronous or asynchronous modes as desired.

---

**SRDF/CE swap support**

An R1/R2 personality swap (or R1/R2 swap) refers to swapping the RDF personality of the RDF device designations of a specified device group, so that source R1 devices become target R2 devices and target R2 devices become source R1 devices.

R1/R2 RDF swaps are available with Enginuity Version 5567 or higher. There are two types of R1/R2 swaps: FastSwap and Dynamic Swap. A FastSwap occurs immediately after failover if the group is fully synchronized. A Dynamic Swap takes longer because after failover, the tracks are checked to determine if they are synchronized, and then the swap occurs. If you enable an R1/R2 swap for a group, SRDF/CE automatically checks during a failover to determine whether FastSwap is available. If FastSwap is available, SRDF/CE will use it. If FastSwap is not supported, SRDF/CE will automatically use Dynamic Swap.

**R1/R2 swap benefits**

This section describes several scenarios in which it is beneficial to execute an R1/R2 swap.

**Symmetrix array load balancing**

In today’s rapidly changing computing environments, it is often necessary to deploy applications and storage on a different Symmetrix array without having to lose disaster protection. R1/R2 swap can enable this redeployment with minimal disruption, while offering the benefit of load balancing across two Symmetrix storage arrays.
For example, if you want to reconfigure an SRDF/CE environment after having decided where the R1 and R2 devices will sit, this procedure will allow you to go from an active/passive configuration to active/active.

**Primary data center relocation**
Sometimes a primary data center needs to be relocated to accommodate business practices. For example, several financial institutions in New York City routinely relocate their primary data center across the Hudson River to New Jersey as part of their disaster drills. R1/R2 swaps allow these customers to run their primary applications in their New Jersey data centers. The Manhattan data centers then acts as the disaster protection site.

**Post-failover temporary protection measure**
You can regain a measure of protection after failing over to the remote site. If the hosts on the source side are down for maintenance, R1/R2 swap permits the relocation of production computing to the target site without giving up the security of remote data protection. When all problems are solved on the local Symmetrix array, fail over again and swap the personality of the devices to return to the original configuration.

**SRDF/CE configuration with multiple remote adapters**
SRDF/CE can be configured with multiple RDF links and remote adapter (RA) groups. SRDF/CE not only allows multiple RAs, but periodically tests them to ensure they are functioning. Multiple RA groups are also allowed, and these RA groups do not have to be symmetrical across all RDF links; any one RA group can be allocated over a subset of the defined RDF links.

If a situation occurs where an RDF link goes down, an event log message is posted and an entry is placed in the SRDF/CE log.
Cluster Enabler provides disaster-tolerant capabilities that enable the cluster servers to be geographically separated\(^1\). Figure 6 illustrates the hardware configuration of a two-node CE cluster solution for either Symmetrix or CLARiiON arrays.

**Note:** Although depicted in the same diagram for illustrative purposes, Symmetrix SRDF and CLARiiON MirrorView/S devices *cannot* be part of the same CE cluster.

---

1. The *EMC Network Topology Guide* provides additional information regarding distance restrictions for your specific configuration.
Network connections can provide a guaranteed maximum round-trip latency between nodes of up to 300 ms. Since many servers can connect to one storage array, it is possible to implement many clusters across this distance.

*Figure 7* illustrates the hardware configuration of a four-node SRDF/CE cluster solution.

*Figure 7*  **A geographically distributed four-node SRDF/CE cluster**

*Note:* The Symmetrix storage configuration depicted in *Figure 7* could also be substituted with CLARiiON storage arrays using MirrorView links.
Cluster Enabler provides disaster-tolerant capabilities by exploiting mirroring and failover capabilities. SRDF allows two Symmetrix arrays to be attached using direct-connect fiber. The SRDF group when built is established in synchronous or asynchronous mode.

Once attached, mirrored pairs of disks are established on the devices, with R1 (read/write) disks on one Symmetrix array and R2 (read-only) mirrors on the other arrays. Additionally, four-way mirroring can be implemented, which locally mirrors each member of the R1/R2 mirror pair.

**Note:** SRDF/CE does not support clusters where the target (R2) side is larger than the source (R1) side. When the system fails over to the R2 side, it can never fail back since the R2 cannot resynchronize all its data back to the R1 side.

A Symmetrix array can support multiple Microsoft Failover Clusters on a single Symmetrix array. Likewise, multiple CE clusters can be supported on an SRDF link. Figure 8 provides an example.

![Figure 8 - Multiple SRDF/CE clusters supported on an SRDF link](image)
Cluster Enabler modes of operation

Different cluster designs support different modes of operation and data sharing mechanisms. The configuration for a CE two-node or multinode cluster in a geographically distributed cluster environment is either active/passive or active/active. EMC defines active/passive and active/active configurations as follows:

◆ **Active/Passive**: A cluster of two nodes or more where all processing is done on one node during normal operation and the work is picked up by a remaining passive node (or nodes) only when a failure occurs on the active node. In a two-node configuration, half of the hardware is normally idle. When failover occurs, the application restarts with full performance.

*Note:* Active/passive multinode clustering provides greater flexibility than the standard active/passive Microsoft failover cluster two-node cluster by providing more options in resolving failures and load distribution after server failures. For example, in a multinode cluster, your configuration may include one or more passive (idle) servers to take over the load from other servers during a site failure, or you may distribute the load among the surviving active nodes.

◆ **Active/Active**: A cluster of two nodes or more where all nodes are running application software during normal operation. When a failure occurs on a node (or nodes), the work is transferred to a remaining node (or nodes) and restarted. The nodes that picks up the work must then handle the processing load of both systems, and performance is usually degraded. However, all the computer hardware is used during normal operation.

*Note:* The terms active/active and active/passive apply to the cluster and to the applications running on the cluster. Both the cluster software and the application software must be designed for active/active operation.

Figure 9 on page 40 presents a typical SRDF/CE two-node two-cluster configuration.
About Cluster Enabler

Figure 9  Two-node two-cluster SRDF/CE configuration

Note: The Symmetrix storage configuration depicted in Figure 9 could also be substituted with CLARiiON storage arrays using MirrorView links.
Pre-SRDF/CE clustering considerations

To ensure disaster recovery protection in an SRDF/CE-enabled cluster, consider the following prior to its installation and configuration:

- Cabling
- Booting
- SRDF coexistence

Cabling

Avoid routing all cables through the same path, both in buildings and between sites. To provide an installation with no single point of failure, use a configuration similar to Figure 10.
Booting

Currently, Microsoft Failover Clusters can only boot from separate private disks (cannot boot off the same bus). Therefore, CE nodes must contain an internal disk for booting or be attached to a nonclustered disk.

SRDF coexistence

Multiple SRDF/CE clusters can share the same SRDF pair. SRDF/CE software can extend the Symmetrix enterprise system to support up to 64 shared quorum disk clusters per Symmetrix pair. There is no limit on the number of MNS clusters per Symmetrix pair.
Microsoft Failover Clusters

Microsoft Failover Clusters is the clustering extension to Windows Server 2008 Enterprise and Datacenter editions. This is also referred to as Microsoft Cluster Server or MSCS in Windows Server 2003 Enterprise and Datacenter editions.

Microsoft Failover Clusters enables up to eight servers running the same Windows operating system in the same domain to be connected to a shared storage system. Typically, this is a RAID array on a shared SCSI storage bus. With iSCSI connections, all servers must be within 40 m of one other (each less than 20 m from the storage). With Fibre Channel connections, you can increase the distance between the two servers.

**Note:** Consult with EMC Customer Support if you need more detail.

Microsoft Failover Clusters protect against failure of production server hardware or network connections. For data protection, Microsoft Failover Clusters use a protected storage subsystem. The standard failover cluster relies on RAID 1 or RAID 5 array storage to guarantee data protection.

In a typical failover cluster containing one to eight nodes, server nodes share the application workload. Typically, in a node cluster environment with \( n \) nodes, each node serves one-\( n \)-th of the total number of disks and clients connected by a common SCSI bus. If one server node fails, one or several of the remaining nodes take ownership of all the disks and assume all the application workload.

**Note:** The number of cluster nodes supported differs between Windows Server 2003 and 2008 Enterprise and Datacenter editions. Refer to your Microsoft Windows Server documentation for your specific operating system.
Figure 11 presents a typical two-node failover cluster on Windows Server 2003 or 2008 Enterprise and Datacenter editions.

Figure 11  A typical two-node Microsoft failover cluster
Figure 12 presents a typical four-node Windows Server 2003 cluster.

**Microsoft Failover Cluster concepts**

Microsoft Failover Cluster is a loosely coupled cluster system. It is not a fault-tolerant, closely coupled system. The concept of a cluster is to take two or more, *off-the-shelf*, independent computers and set them up to work together to provide higher availability and scalability than what you can obtain using a single system. When failure occurs in the cluster, control of a disk, or resource, moves to another cluster node. This process is called a *failover*. Failovers can be initiated by a number of events, including the following:

- *Manual failover* — The moving of resources from one server to another. Done for system load balancing or for server maintenance.
- *Failover due to hardware failure* — The surviving node takes over when a server, iSCSI or Fibre Channel host bus adapter (HBA) card, or network interface card (NIC) fails.
- *Failover due to application failure* — The failure of a virtual server or IP resource can initiate the failover.
By contrast, a fault-tolerant system uses special-purpose hardware to run multiple computers in lock step, which provides nonstop computing with no data loss when a component failure occurs. Therefore, fault-tolerant systems are more expensive.

There are benefits and limitations to using a cluster architecture.

**Benefits**

Clustering provides:

- *Improved availability* by continuing to provide a service even during hardware or software failure.
- *Increased scalability* by allowing new components to be added as system load increases.
- *Simplified management of groups of systems and their applications* by enabling multiple applications on multiple servers to be managed as a single system.

**Limitations**

Clustering cannot protect against:

- Software corruption
- Human-induced failures

*Note:* Protection of user data through backup, EMC business continuance volumes (BCVs), or other forms of offline data redundancy, remains vitally important to the reliable operation of mission-critical applications.

---

**Microsoft Failover Cluster modes of operation**

Microsoft Failover Cluster supports 16 node clusters for Windows Server 2003 or 2008 Enterprise and Datacenter Editions.

Similar to the modes of operation generally discussed for Cluster Enabler, the configuration for a failover multinode cluster in a geographically distributed cluster environment is either active/passive or active/active. “Cluster Enabler modes of operation” on page 39 provides an example.

**Availability**

Failover clusters allows active/active application operation. During normal operation, software applications can be running on both nodes. If either node fails, the applications are restarted on the remaining cluster node. This provides high availability by minimizing application downtime. Usually, it takes one to 10 minutes to fail over and restart an application on a Microsoft Failover Cluster. Restart time is highly application dependent.
**Scalability**

In addition to availability protection, cluster technology is scalable. You can add new components to the system and run the same application (accessing the same database) on multiple nodes of a cluster to deliver increased processing power. To provide scalability, data sharing is needed.

The following Microsoft URLs provide additional information on the different modes of operation and clustering concepts:


http://support.microsoft.com/kb/288778
**Application software in a cluster environment**

Software running on a cluster may, or may not, be cluster aware. When software is cluster aware, it provides a *restart* mechanism invoked whenever the application resource is moved to another node in the cluster.

Application failover requires a *restart* of the application whenever failover occurs. Restart is *not* instantaneous. Unlike a fault-tolerant computer, a distributed cluster does not provide nonstop computing. The time that restart takes, and the completeness of the recovery, is application dependent:

- For a transaction-oriented application (such as SQL or Exchange that contain both a database and transaction log files), the application provides a restart mechanism to recover work in progress. Usually a transaction log is used to record all work in progress. When a node fails, the information in host memory is lost, but the work can be reconstructed by applying the transaction log to the database to restart. This mechanism recovers all transactions completed before the failure. Transactions partially complete are lost and must be reentered.

- Applications such as Microsoft Word or Microsoft Excel provide a checkpoint capability. If the application experiences a failover, all work since the last disk checkpoint is lost.

- If an application has neither a database nor checkpoint capability, and also retains no information (or *state*) between client requests (such as a Web Browser or a Microsoft Outlook client), then it can fail over by reissuing the outstanding request. In this scenario, no work is lost, and no restart is needed on the server.

- If the application has neither a checkpoint nor restart capability, and it retains the state between client requests to the server, then it must be rerun from the beginning when the node it is running on fails.
This chapter describes Cluster Enabler behavior in various operational modes. Unless otherwise noted, Cluster Enabler behavior is described for a standard two-node cluster:

- Cluster failover operation ................................................................. 50
- Response to complete site failure .................................................... 57
- Failure behavior when using MNS with File Share Witness ....... 60
Clusters are designed to overcome failures. There are several possible failure modes in a cluster configuration. Cluster Enabler protects against more failure scenarios than local clusters can. Failure of an individual client affects only one user and is not discussed in this chapter. In a CE cluster, eight types of cluster elements can fail (singly or in combination). Figure 13 on page 51 provides a depiction of various cluster failures.

This section describes the following:

- “Cluster Enabler failover and recovery behavior” on page 52
- “Cluster Enabler unique behavior” on page 53
- “Complete site failure and recovery” on page 55
Cluster failover operation

**Figure 13** Cluster Enabler failover operation

*Note:* Although depicted in the same diagram for illustrative purposes, Symmetrix SRDF and CLARiiON MirrorView/S devices cannot be part of the same CE cluster.
The section that follows discusses how a two-node cluster responds to various combinations of element failures. Cluster response during failure modes is similar in a three- or four-node system, but a standard two-node system is used in this section for discussion purposes. The starting condition for each of these failure scenarios is:

- Both nodes are operational.
- Node 1 (N1) owns the quorum disk for Symmetrix.
- Both the public link (internode LAN link) and the private link (heartbeat link) are configured in Microsoft (MS) failover clusters as enabled for all network access.

Simply stated, the failover and recovery operations Cluster Enabler provides can be divided into situations where:

- The behavior of Cluster Enabler is the same as Microsoft failover local clusters.
- The geographic separation and disaster tolerance of Cluster Enabler causes unique behavior and provides recovery alternatives.

---

**Cluster Enabler failover and recovery behavior**

The following sections introduce Cluster Enabler failover and recovery behavior common with MS failover clusters. Figure 13 on page 51 shows the numbered callouts to these sections.

**LAN link failure (1)**

If the LAN connection between nodes fails, both servers are still available and can communicate over the heartbeat link. No failover occurs, current processing continues, and client requests from clients connected to the LAN locally continue to be serviced. Client traffic from clients connected through the LAN link fail.

**Heartbeat link failure (2)**

If the heartbeat link fails, MS failover clusters routes heartbeat messages across the public LAN. Operation of the cluster continues with no failover of resources.

**Storage link failure (3)**

“SRDF or MirrorView link failure(3)” on page 54 provides a detailed explanation.
**Host NIC failure (4)**

The host is cut off from all clients. Processing continues uninterrupted on the other host. On the failed host, client input to that host fails, but current processing activities continue. MS failover clusters detects the NIC has failed. The isolated node takes resources offline to halt processing. The other node brings the failed resources online so application failover can occur.

**Server failure (5)**

If the host node hardware fails, or the operating system crashes, all heartbeat messages to the remaining node cease. The remaining node then uses the quorum disk to discover the first host has failed. The remaining node then brings the resources of the failed node online and starts the applications recovery procedures.

**Application software failure (6)**

If an application module fails, MS failover clusters initiates a failover to the remaining node. The Cluster Enabler resource monitor is directed to make the storage resource for the failed application available on the other node to allow application failover.

**Host bus adapter failure (7)**

An HBA failure is a resource failure that triggers a cluster failover operation. If both storage arrays are still running, the failover operation completes normally.

**Cluster Enabler unique behavior**

The following sections introduce Cluster Enabler unique behavior which is different from MS failover cluster behavior. Figure 13 on page 51 shows the numbered callouts to these sections.

**Storage array failure (8)**

When a mirrored disk fails in a storage array (Symmetrix or CLARiiON), it is not visible to the host because normal operations continue with the mirror, and the failed drive is hot replaced without disturbing the host. However, if an entire storage array fails, it appears to its attached server as a resource failure indistinguishable from an HBA failure. The MS failover cluster on that server triggers a failover operation. However, because the storage array itself has failed, the remaining devices recognize that communication is lost.
and prevent failover from completing unless automatic failover is set as described in “Complete site failure and recovery” on page 55.

**SRDF or MirrorView link failure(3)**

- If the link between a Symmetrix array fails, the EMC ControlCenter® Symmetrix Manager or the Symmetrix Management Console application notices the condition and reports an error.

- If the link between a CLARiiON array fails, the EMC Navisphere® Manager application notices the condition and reports an error.

The MS failover cluster server does not notice the change (because access to existing disk resources is not disturbed) unless it tries to bring a new resource online.

SRDF link failures are noted in the Event Log, in the SRDF/CE log. MirrorView link failures are not noted in the Event Log.

If MS failover cluster or a user attempts to fail over or fail back a group, and there is no link available to perform that operation, the operation is not allowed. However, if there are multiple active lateral nodes and the groups in question are on that lateral side, lateral-to-lateral failover is permitted.

**Note:** This behavior can be overridden by enabling the Automatic Failover feature for a particular group.
Complete site failure and recovery

Local MS failover cluster In a local MS failover cluster, if an entire site fails (such as from a flood, fire, and so forth) the entire cluster fails. By contrast, with a CE cluster, each site contains only one of the two nodes in the cluster (or only one of the $n$ nodes in a multinode cluster).

CE cluster A complete site failure can be caused by either a site failure or a total communication failure. Figure 14 illustrates the two types of complete site failure.

Figure 14 Types of complete site failure

Note: Although depicted in the same diagram for illustrative purposes, Symmetrix SRDF and CLARiiON MirrorView/S devices cannot be part of the same CE cluster.
Cluster Behavior

**Site (server and storage) failures (5+8)**

Site failure occurs when the host and storage array both fail (such as from a natural disaster or human error).

**Total communication failure (1+2+3)**

A total communication failure can occur while the host and storage array remain operational (such as a backhoe digs up the cable conduit where all communications cables leave a building).

A total communication failure, while both nodes remain operational, is referred to as a *split-brain* condition and is a potential cause of logical data corruption. For example, if both sides assume the other is dead and begin processing new transactions against their copy of the data, two separate and unreconcilable copies of the data can be created.

Both nodes are isolated from each other, but not from local clients. It is impossible to determine if the other node is alive. No remote client processing is possible, but running processes continue.

**Note:** There is no way for the surviving node to determine which of these two types of failures caused the site failure.
Response to complete site failure

In Cluster Enabler, the site failure modes determine the behavior of a cluster when a failure occurs, separating the two storage arrays and suspending remote data mirroring protection.

If a complete site failure occurs, MS failover cluster on the surviving node first notices that heartbeat messages are no longer being received. MS failover cluster attempts to communicate with the other node using the LAN communication path, to see if communication is still possible.

MS failover cluster then queries the status of the disk resource and decides whether to bring the disk resources on the local node online or to set them offline. The commands to perform this query from MS failover cluster to Cluster Enabler are:

- **Is Alive?** — Determines whether a currently online resource is still healthy and can continue to be used, or whether it and all dependent cluster resources must be taken offline.
- **Online Request** — Changes the state of an offline resource to online for a failover.

Each group’s failover option setting determines how Cluster Enabler responds to queries from Cluster Service. This setting must be manually configured to select the desired failover and recovery behavior.

Inappropriate user actions that cause groups to bounce back act differently. If you attempt to move the quorum group when the SRDF link is down, the MS failover cluster destination node terminates, and the group bounces back. Active/active configurations are obviously affected because any applications on the destination node now move. This behavior is a result of the preceding behavior.

**Important:** If MS failover cluster cannot write to the quorum disk when it wants to, it terminates.

**Note:** MirrorView/CE does not support shared quorum clusters.
The Cluster Enabler site failure mode settings are:

- **Restrict Group Movement** — In an SRDF or MirrorView link failure, this setting will only attempt to move disks laterally. Figure 15 shows lateral and peer nodes. If the SRDF or MirrorView link is up, this setting has no impact.

- **Automatic Failover** — The Automatic Failover policy sets the group to allow automatic failover to another node in the event of an SRDF link failure or if both MirrorView links are down.

Whenever a failure occurs such that mirrored data protection between sites is lost (for example, the SRDF link is down or a Symmetrix array is down), Cluster Enabler responds to the failure by not allowing any new disk groups to be brought online until communication with the other node has been reestablished (unless the Automatic Failover feature is set).

**WARNING**

*Data Loss is possible for any group from Nodes 1 and 3 that is brought online with Automatic Failover if outstanding writes were not mirrored to the secondary site.*
Note: The CLARiiON storage configuration depicted in Figure 15 on page 58 could also be substituted with Symmetrix storage arrays using SRDF links.

Quorum disk-based clusters for SRDF/CE

For quorum disk-based clusters, the side that remains up with respect to a Symmetrix array is based on what node owns the quorum resource. In a site disaster, Failover clusters (MSCS) keep all nodes up on the side owning the quorum. All resources owned by the other side are moved to the surviving side.

In the quorum disk case, SRDF/CE monitors all nodes. If tracks (data) are not owed to the surviving side, then the move proceeds smoothly. If tracks are owed to the surviving side, then the Automatic Failover option is required to make the move successful. Therefore, if SRDF/CE detects a split-brain\(^1\) condition during MSCS normal group failover processing, the Automatic Failover option will cause the failing site to successfully transition to the new site.

Behavior override

In addition to the site failure mode settings, Cluster Enabler provides the ability to override the mode behavior and bring resources back online under user direction through the Automatic Failover feature. This enables you to decide where processing is allowed to continue.

If you determine that one site is actually down, and the other site remains operational, you can use the Automatic Failover feature to:

- Override the failure mode.
- Allow disk resources to be brought online, even though SRDF or MirrorView/S is not operating and there is no mirror protection of data.

CAUTION

Use the Automatic Failover feature with great care. EMC does not recommend using the Automatic Failover feature during normal non-disaster operations.

---

1. A total communication failure, while both nodes remain operational, is referred to as split-brain condition and is a potential cause of logical corruption. For example, if both sides assume that the other is dead and begin processing new transactions against their copy of data, two separate and unreconcilable copies of the data can be created.
Failure behavior when using MNS with File Share Witness

**Failure behavior and recovery**

In general, Cluster Enabler behaves similarly to a two-node cluster using a quorum disk.

The following example explains a four-node cluster for Majority Node Set with File Share Witness. **Figure 16** provides an illustrated example for either Symmetrix or CLARiiON arrays. The production nodes, Nodes 1 and 2 are at the primary site. The remote nodes, Nodes 3 and 4, are at the secondary site, and the file share node is at a third site. The cluster is configured with all the described settings.

**Primary Site**: Production volumes are mapped to Node 1 and Node 2 but accessed by one Node at any given time.

**Secondary Site**: Remote volumes are mapped to Node 3 and Node 4 and are offline until failover.

**Site 3**: File Share Witness or a Tie-Breaker Node at third site

---

**Figure 16** MNS clusters with file share witness
In the following examples, groups are cluster groups that contain one or more Cluster Enabler managed physical disk resources. The failover policy has been set to Restrict Group Movement.

**Storage failure at primary site**
- Groups on Nodes 3 and 4 remain online but cannot failover.
- Groups on Nodes 1 and 2 move to Nodes 3 and 4 but stay offline and must be brought online manually by enabling Automatic Failover.

**WARNING**

_Data Loss is possible for any group from Node 1 and 2 that are brought online with Automatic Failover, if outstanding writes were not mirrored to the secondary site._

**SRDF link failure or both MirrorView links fail**
- Groups on Nodes 3 and 4 remain online but cannot failover.
- Groups on Nodes 1 and 2 remain online but cannot failover.
- To move a group to a different node, enable Automatic Failover on the destination node.

**WARNING**

_Data Loss is possible for any group that is moved with Automatic Failover if outstanding writes were not mirrored._

**Site failure (server and storage) at primary site**
- Groups on Nodes 3 and 4 remain online but cannot failover.
- Groups on Nodes 1 and 2 move to Nodes 3 and 4 but stay offline and must be brought online manually by enabling Automatic Failover.

**WARNING**

_Data Loss is possible for any group from Nodes 1 and 2 that are brought online with Automatic Failover if outstanding writes were not mirrored to the secondary site._
Cluster Behavior

**Total communication failure**

- If all nodes have connectivity to the file share witness, the cluster will take two of the nodes at one site offline.
- If only one node has connectivity to the file share witness, the cluster will take the other nodes offline.
- If no nodes have connectivity to the file share witness, the entire cluster will go offline. (See Microsoft procedures for forcing an MNS cluster node online.)
- If Nodes 3 and 4 are the surviving node:
  - Groups on Nodes 3 and 4 remain online but cannot failover.
  - Groups on Nodes 1 and 2 move to Nodes 3 and 4 but stay offline and must be brought online manually by enabling Automatic Failover.

**WARNING**

*Data Loss is possible for any group from Nodes 1 and 2 that are brought online with Automatic Failover if outstanding writes were not mirrored to the secondary site.*
This chapter provides instructions for upgrading to and installing Cluster Enabler software using the InstallShield Wizard. It also describes how to uninstall:

- Cluster Enabler installation overview ............................................. 64
- InstallShield Wizard .......................................................................... 72
- Upgrade procedures .......................................................................... 74
- Uninstalling Cluster Enabler ............................................................ 79
Cluster Enabler installation overview

This chapter describes how to install Cluster Enabler for Microsoft Failover Clusters Version 3.0 on the supported Microsoft Windows Server 2003 or 2008 systems and provides instructions on how to upgrade your existing supported SRDF/Cluster Enabler for MSCS software to Version 3.0. It also describes how to uninstall the Cluster Enabler Version 3.0 software.

In most cases, installation and upgrades should be performed using the InstallShield Wizard as described in the various sections of this chapter. In certain upgrade scenarios, where scripting is employed for complex configurations, the installation upgrade may be performed using a command line interface method. This method of installation is described in Appendix A, Manual Installation and should only be performed by advanced users of this product and system administrators.

The CE InstallShield Wizard provides a user-friendly alternative to the more difficult manual installation and configuration. It is recommended that you contact EMC Customer Support for assistance if any of the following issues are applicable:

◆ You have applications already layered with dependencies.
◆ You need other devices online.
◆ You are not confident about installing and configuring new software within the context of Windows Server 2003 or 2008, Microsoft Failover Clusters, and Symmetrix arrays with SRDF or CLARiiON arrays with MirrorView.

Before you begin

Before you begin to install or upgrade Cluster Enabler, read the following installation requirements and considerations:

◆ The supported versions of SRDF/CE that may be upgraded to Cluster Enabler Version 3.0 using the InstallShield Wizard include only SRDF/Cluster Enabler for MSCS Versions 2.1.x and above. If you have an older unsupported version that you would like to upgrade, contact your EMC representative for assistance or proceed with a clean install after uninstalling the older version.
**Note:** For a clean install, all existing clusters will have to be reconfigured and any unique settings in SRDF/CE will be lost.

- There are three Windows processor architectures that are supported:
  - x86
  - x64 (AMD64 and Intel EM64T)
  - IA64 Itanium (only supported for SRDF/CE)

**Note:** Microsoft does not support mixed architecture clusters. All nodes must be the same Windows architecture.

- Installation of Cluster Enabler requires a reboot of the system for the configuration to take effect. After installation, you may choose the restart option or postpone your restart until a more convenient time.
- Installation on Windows Server 2003 systems requires that a minimum of SP2 (Service Pack) first be installed.
- Installation on Windows Server 2003 requires that Microsoft .NET Framework Version 2.0 first be installed.
- Installation on Windows Server 2008 requires that all nodes first be installed with the Failover Cluster feature.
- Cluster Enabler Version 3.0 requires that a minimum version of Solutions Enabler 6.5 first be installed.
- Upgrades scenarios where the storage is being replaced is not supported. Existing clusters must first be migrated to the new storage array using the Symmetrix Replace feature before upgrading to Cluster Enabler Version 3.0.
- Configurations where the cluster node is zoned to both local and remote storage arrays are not supported. Before upgrading to Version 3.0, you must first remove the remote Symmetrix array and perform a discovery process for both SRDF/CE and SYMCLI.
- For upgrade scenarios, the cluster quorum type can only be changed before or after the upgrade.
- As part of the upgrade procedure, the CE Configuration Wizard accepts an optional checkpoint file (reglist.txt) as input to migrate settings from previous versions of SRDF/CE.
Note: For information on converting existing clusters to CE clusters, refer to the CE Configuration Wizard in Chapter 4, Using Cluster Enabler Manager.

- The InstallShield Wizard only performs upgrade tasks for Windows Server 2003 upgrades.

---

Getting started with Symmetrix arrays

The following steps are provided only as a high-level overview to getting started with Symmetrix and SRDF/CE:

1. Prepare the Symmetrix array, RDF, and cluster node hardware.
2. Install any necessary drivers, EMC Solutions Enabler, and EMC SRDF/CE 3.0 on cluster nodes.
3. Configure the Symmetrix storage and mask LUNs to all cluster nodes.
4. Ensure that all SRDF devices that the cluster uses are in a synchronized or consistent state and write-enabled.
5. Map the R1 devices to all lateral nodes and the R2 devices to all peer nodes in the cluster. Symmetrix arrays that are both local and remote to a node are not supported. Reboot the nodes.
6. Open the Microsoft Disk Administrator and initialize all R1 devices. If possible format all R1 devices to NTFS format.
7. Nodes are grouped under Site. All nodes in a site shall have same devices mapped. For example, a given R1 device shall be mapped to all nodes in Site 1 and the corresponding R2 device shall be mapped to all nodes in Site 2. Add the appropriate device mappings to the rest of the nodes.
8. Ensure that all devices in a given group are of the same type (for example, either R1 or R2).
9. Verify that the SRDF link is operational by performing a failover to the R2 side. Open Microsoft Disk Administrator to check that the R2 device labels are the same as the R1 device labels. Then perform a failback and write-enabled the R1 devices on the node.
10. Create at least a single node failover cluster. Preferably create the cluster using all lateral nodes on the R1 side.
11. On Windows Server 2008, ensure all devices in a cluster group are write-enabled on the node which owns the group in the cluster.

12. Use the SRDF/CE 3.0 configuration wizard to complete the cluster configuration and add R2 side nodes.

Getting started with CLARiiON array

The following configuration and installation instructions are provided only as a high-level overview to getting started with CLARiiON arrays and MirrorView/CE.

**MirrorView/Cluster Enabler V3.0 notes**
- CLARiiON arrays that are both local and remote to a node are not supported.
- Asynchronous replication groups are not supported.
- Use Navisphere Manager or the NaviCLI to create mirror relationships between devices before attempting to setup groups using MirrorView/CE.

**Installation preparation**
For MirrorView/Cluster Enabler to work correctly, the following steps must be performed before installing the MirrorView/CE software on all of the CLARiiON arrays.

1. Servers that will be cluster nodes should be configured with basic connectivity to one of the arrays in the environment. This includes HBAs, PowerPath®, and array registration.

2. Ensure that all nodes are installed with Microsoft .NET framework Version 2.0.

3. The CLARiiON arrays that will be used with MirrorView/CE must be of the CX3 family running FLARE® code release 26 or higher and must be configured with the MirrorView/S licenses.

4. Setup a Majority Node Set Cluster using the Microsoft Cluster Administrator on one of the nodes that will be part of the cluster. At this time, MirrorView/CE only supports Majority Node Set type clusters and does not support Shared Quorum clusters. Ensure that the cluster includes all the nodes that are required to be part of the cluster.
5. Setup synchronous mirrors using the Navisphere Manager on the CLARiiON arrays that will be associated with the cluster. When these mirrors are setup, it is important that administrators ensure that the primary and secondary devices of the mirrors are mapped to the nodes that have access to the CLARiiON array hosting the device. Devices can be created on primary node of the cluster. Do not configure any MirrorView/S Consistency Groups as part of this step.

*Note:* Mirrorview/CE does not support Asynchronous, therefore only Synchronous mirrors should be created.

6. In the Navisphere domain, set up a Navisphere user for the cluster. The username should be unique, so that cluster activity can be identified in the storage processor logs. Set user attributes as **Scope – Global** and **Role – Manager**.

7. Install Solutions Enabler Version 6.5, or later, on all the nodes of the cluster where MirrorView/CE will be installed. Use the following command to add Solutions Enabler licenses for Base and Cluster Enabler.

   ```
   C:\Program Files\EMC\Symcli\bin\symlmf
   ```

8. Identify the IP addresses for each of the CLARiiON array’s storage processors (SP/A and SP/B), which are attached to the node. For this example, two storage processors are connected to the node and have the following IP addresses:

   - 172.23.201.42 - SPA for local storage
   - 172.23.201.43 - SPB for local storage
   - 172.23.201.44 - SPA for remote storage
   - 172.23.201.45 - SPB for remote storage

9. Issue the following command on all the nodes of the cluster:

   ```
   symcfg auth list
   ```

   This should return an empty list. But if it does return a list of IP addresses and usernames, then you need to check if any of them match the IP addresses that you identified in step #8.

10. For each CLARiiON array that is visible to the cluster (not just the node), issue the following commands in the exact order. Hostname can be the IP address of the storage processor. Username and Password should be for the cluster created in step 6.
symcfg auth add -hostname <SPA> -username <SPA username> -password <SPA Password>

symcfg auth add -hostname <SPB> -username <SPB username> -password <SPB Password>

Note: It is important to remember that the order of the authorization list be maintained (for example, the first entry should be that of SPA and the subsequent entry should be that of SPB).

11. After completing all previous steps, install the MirrorView/CE software on all cluster nodes of the cluster. “Clean install” on page 73 provides installation instructions.

**Install MirrorView/CE Cluster Enabler on all nodes**

To install MirrorView/CE, run the setup.exe program. This opens the CE Installation Wizard. The wizard detects if the install is a new install or an upgrade. The wizard is designed to step you through the installation process. Follow the install steps as prompted in the wizard. It is recommended that you reboot the nodes as suggested by the installation program after each install is complete.

**Configure CLARiiON CE cluster groups**

1. Ensure that the CLARiiON Navisphere and Solutions Enabler software is installed on all of the nodes.

2. Use the CLARiiON Navisphere Manager to configure a few named mirrors (for example, TestMir, TestMir1, and so on). For this step, use devices on the CLARiiON array that are mapped to the node by a drive letter. If there is no mapping, create a mapping using Diskadmin. Make sure that the disk is configured as a Windows basic disk and not as a dynamic disk. Ensure that the disks are formatted as NTFS.

3. If a cluster is not already configured, configure a Majority Node Set (MNS) cluster on the nodes that make up the cluster. Ensure that the cluster is up and running.

4. Click the **Configure CE Cluster** link or select the option from the pull-down action menu in the CE Manager GUI to configure a CE cluster. The CE Configuration Wizard opens. Specify the cluster name or enter a period(.) for the name of the cluster. The configuration wizard will automatically discover the storage and perform other necessary configuration steps.
5. Once the CE cluster has been configured and a configuration reboot has completed, run the CE manager and expand the Groups option. You should only see Cluster Group in the list of groups. You will see all failover cluster (MSCS cluster) groups.

6. Right-click Groups and select Create Group. Give a name for the group and click Create. The create screen displays the mirror pairs that were created in step 2. Check the list of devices that you want to create a group with and follow the Wizard screens accepting the default options. The group create may take a while; once the group create is complete, click Groups and you will see the group that you created.

7. Open the Microsoft failover cluster GUI to view the CE group that you just created under Groups. The group is usually shown as online on one of the nodes of the cluster.

8. Right-click on the group that you created and click Move Group. This will initiate a failover of the group from the node on which it was online to another node in the cluster. If the move is successful, the group will come online on another node within the cluster.

9. Repeat configuring groups with other mirrors to be managed with MirrorView/CE.

---

**Setting up devices on Windows Server 2008**

On Windows Server 2008, all disks must first be added to Failover Cluster Management before they can be configured for Cluster Enabler. By default, Failover Cluster assigns all disks to a group called "Available Storage". You must ensure that Failover Cluster can bring these disks online before using them in Cluster Enabler.

Follow these steps to correctly set up devices on the Windows Server 2008:

1. Choose the appropriate instructions from the following three scenarios as listed below for disks shown in Available Storage:
   a. If there are no disks in Available Storage, ensure that all disks to be added are write enabled on the same site (for example, site A).
   b. If there are already disks in Available Storage and you want to add more disks, ensure that all disks to be added are write enabled on the same site where Available Storage is online.
c. If some existing disks in Available Storage are not online, move them to the site where the Available Storage is online. If this does not solve the problem, then you need to do the following:

a. Remove those disks from Available Storage.

b. Move all groups and devices to the same node in Failover Cluster. Manually move the corresponding devices to ensure that devices are write enabled on the node that you are moving the group to.

c. Evict all peer nodes.

2. Ensure that you have access to the disks where they are write enabled. If not, you must reboot and re-format them.

3. Right click Storage in Failover Cluster Management, select Add a Disk. All available disks should be displayed. You can select disks to add to the cluster. All added disks will be in the group Available Storage. Verify that all disks are online in Available Storage.

4. The devices should now be available for use in Cluster Enabler.
InstallShield Wizard

The Cluster Enabler InstallShield Wizard is launched by double-clicking on the `setup.exe` file icon, which is included on your software CD or download. The InstallShield Wizard automatically detects all previous versions of Cluster Enabler and proceeds with the installation upgrade according to the detected version number and installation location. This section contains instructions for performing a clean install.

Upgrade types

If a previous supported version is detected, a dialog box in the InstallShield Wizard will ask you to select the type of upgrade to perform.

**Upgrade this node and prepare cluster**

This option should be used on only one node in the cluster. The install detects the checkpoint file (reglist.txt) and warns the user if it is not present. The checkpoint file is then moved to the new installation directory. The CE cluster resources and resource type are deleted from the cluster. The previous version is uninstalled and Cluster enabler V3.0 is installed.

**Upgrade this node**

This option will uninstall the previous version and install CE 3.0.

**IMPORTANT**

“Upgrade procedures” on page 74 provides detailed upgrade instructions for your specific system.

**Clean install**

Note that the clean install option is useful if a previous version uninstall did not completely clean up the system. Installing CE 3.0 along side an earlier version is not supported. The older version must be uninstalled first. “Uninstalling Cluster Enabler” on page 79 provides instructions.
Clean install

Before installing be sure to review the requirements and considerations listed in “Before you begin” on page 64.

To install EMC Cluster Enabler, download the appropriate version of CE for Microsoft Failover Clusters Version 3.0 software from the Powerlink website (SRDF/CE or MirrorView/CE). To install the software:

1. Open the installation CD or download the kit from Powerlink and extract the files to a temporary directory.

2. Navigate to your operating system’s directory (either x64 or x86) and run the setup.exe file to launch the executable. This will open the first page of the InstallShield Wizard. Click Next.

3. Read the license agreement and select I accept the terms in the license agreement. Click Next. If you do not accept, the software will not be installed and you will be prompted to close the wizard.

4. Choose a destination folder location for where to install the program files. It is recommended that you choose the default location as shown. Click Next.

5. Click Install to proceed with the installation.

6. The Windows security message appears, “Would you like to install this device software?”. Click Install.

7. The wizard is now ready to begin installing the files. Click Install.

8. Your system must be restarted for the configuration changes to take effect. Click Yes to restart the system immediately or No to manually restart the system at a later time of your choosing.

Repair installation

For upgrades, the SRDF/CE V3.0 InstallShield Wizard includes a program maintenance option that can be to repair previous installation errors. Select this option to fix missing or corrupt files, shortcuts and registry entries.
Upgrade procedures

Examples in this section use a 4 node shared quorum cluster where nodes A and B are on the production R1 side and nodes C and D are on the recovery R2 side. If a cluster only has 2 nodes, skip steps for nodes B and D. MNS and File Share Witness procedures are similar.

Windows 2003 SRDF/CE v2.x cluster to CE v3.0

Use the following procedure to upgrade your existing Windows Server 2003 cluster from SRDF/CE Version 2.x to Cluster Enabler Version 3.0. You should plan your upgrade accordingly, as it will result in an outage for the cluster. While the cluster is being upgraded, stop the cluster service on the remote nodes so that a failover of SRDF/CE managed storage can not occur:

1. Move all cluster groups to node A. This node will be the focus for upgrading the cluster.

2. On node A, start the SRDF/CE Configuration utility and create a checkpoint file to save registry settings. By default, the upgrade process moves this file to the new Cluster Enabler installation directory. Close the SRDF/CE Configuration utility.

3. Stop the SRDF/CE and Cluster service on all other nodes B, C, and D.

4. Using Microsoft Cluster Administrator, evict remote cluster nodes C and D. This will prevent an accidental RDF failover.

5. On node A run the setup.exe in the CE v3.0 kit to open the InstallShield Wizard.

6. Select Upgrade this node and prepare cluster. The installer will automatically deconfigure SRDF/CE leaving the cluster intact.

7. Reboot node A when prompted by the wizard. This will cause a cluster outage.

8. Check that the cluster starts and all groups come online on node A.

IMPORTANT

Complete steps 9 through 11 on all remaining nodes.
9. Run CE v3.0 setup.exe in the CE v3.0 kit to open the InstallShield Wizard.

10. Select Upgrade this node.

11. Reboot the node when prompted by the wizard.

12. On node A, start the CE v3.0 Cluster Enabler Manager and click the Configure CE Cluster link.

13. Check Upgrade and verify that the path to the RegList.txt checkpoint file you created in step 2 is correct.

14. Specify only lateral nodes A and B when configuring the cluster.

15. Complete the Configure CE Cluster Wizard and reboot nodes as prompted.

16. Confirm that all cluster groups can be brought online and be moved between lateral nodes A and B.

17. Start the Cluster Enabler Manager and select the Configure CE Cluster link again.

18. Add remaining remote nodes C and D, and reboot nodes as prompted.

19. Confirm that all cluster groups can be moved to the remote nodes.

---

**Windows 2003 SRDF/CE V2.x cluster to a Windows 2008 CE V3.0 cluster**

Use the following procedure to upgrade your existing Windows Server 2003 cluster from SRDF/CE Version 2.x to new Windows Server 2008 hardware and Cluster Enabler Version 3.0. You should plan your upgrade accordingly, as it will result in an outage for the cluster. While the cluster is being upgraded, stop the cluster service on the remote nodes so that a failover of SRDF/CE managed storage can not occur:

**IMPORTANT**

This procedure assumes that you have completely new hardware for the 2008 nodes.

1. Choose an existing SRDF/CE node as the template for the migration.
2. Start the **SRDF/CE Configuration** utility and create a checkpoint file to save registry settings. By default, the upgrade process moves this file to the new Cluster Enabler installation directory. Close the **SRDF/CE Configuration** utility.

3. Copy the checkpoint file (RegList.txt) to a location available to the new cluster nodes, either a network share or removable media. The checkpoint file will be created in the SRDF/CE install directory which is typically: `C:\Program Files\EMC\SRDF-CE\`

**IMPORTANT**

Complete steps 4 and 5 on all new cluster nodes.

4. Run CE V3.0 `setup.exe` in the CE v3.0 kit to open the InstallShield Wizard.

5. Reboot when prompted by the wizard.

6. Start Microsoft Failover Cluster Manager on node A of the new cluster and configure a cluster as per Microsoft procedures and include only lateral nodes A and B.

7. Migrate cluster settings from the old cluster using the Microsoft Failover Cluster Migration wizard as per Microsoft procedures.

8. Stop the SRDF/CE and Cluster service on all old cluster nodes.

9. Bring all groups online on new cluster nodes.

10. Start the Cluster Enabler V3.0 Cluster Enabler Manager on node A and select the **Configure CE Cluster** link.

11. Check **Upgrade** and verify that the path to the `RegList.txt` checkpoint file you created in step 2 is correct.

12. Specify all nodes A, B, C, and D.

13. Complete the Configure CE Cluster Wizard and reboot nodes as prompted.

14. Confirm that all cluster groups can be brought online and be moved between lateral and remote nodes.

**IMPORTANT**

Use the following two steps to deconfigure the old cluster nodes on each node.
15. From the command prompt, run the following command:

    cluster.exe node NodeName /forcecleanup

(where NodeName is the name of the node)
16. Uninstall SRDF/CE and reboot when prompted.

Windows 2003 SRDF/CE V2.x cluster to a Windows 2008 CE V3.0 cluster

Use the following procedure to upgrade your existing Windows Server 2003 cluster from SRDF/CE Version 2.x to existing Windows Server 2008 hardware and Cluster Enabler Version 3.0. You should plan your upgrade accordingly, as it will result in an outage for the cluster. While the cluster is being upgraded, stop the cluster service on the remote nodes so that a failover of SRDF/CE managed storage can not occur:

**IMPORTANT**

This procedure reuses the existing nodes by migrating the R1 production site to Windows 2008 first.

1. Choose an existing SRDF/CE node as the template for the migration.
2. Start the SRDF/CE Configuration utility and create a checkpoint file to save registry settings. By default, the upgrade process moves this file to the new Cluster Enabler installation directory. Close the SRDF/CE Configuration utility.
3. Copy the checkpoint file (RegList.txt) to a location available to the new cluster nodes, either a network share or removable media. The checkpoint file will be created in the SRDF/CE install directory which is typically: C:\Program Files\EMC\SRDF-CE\.
4. Move all cluster groups to the remote nodes C and D.
5. Using Microsoft Cluster Administrator, evict nodes A and B.

**IMPORTANT**

Complete steps 6 through 9 on nodes A and B.

6. Install Microsoft Windows 2008 as per Microsoft procedures.
7. Install the Failover Clusters feature.
8. Run Cluster Enabler V3.0 setup.exe in the CE v3.0 kit to open the InstallShield Wizard.

9. Reboot when prompted by the wizard.

10. Start the Microsoft Failover Cluster Manager on node A of the new cluster. Configure the cluster as per Microsoft procedures and include only lateral nodes A and B.

11. Migrate the cluster settings from the old cluster on nodes C and D using the Microsoft failover cluster migration wizard as per Microsoft procedures.

12. Stop the SRDF/CE and Cluster service on old cluster nodes C and D.

13. Bring all groups online on the new cluster nodes.

**IMPORTANT**

Complete steps 14 through 17 on nodes C and D.


15. Install the Failover Clusters feature.

16. Run Cluster Enabler V3.0 setup.exe in the CE v3.0 kit to open the InstallShield Wizard.

17. Reboot when prompted by the wizard.

18. Start the CE v3.0 Cluster Enabler Manager on node A and choose the **Configure CE Cluster** link.

19. Check **Upgrade** and verify that the path to the RegList.txt checkpoint file you created in step 2 is correct.

20. Specify all nodes A, B, C and D.

21. Complete the Configure CE Cluster Wizard and reboot nodes as prompted.

22. Confirm that all cluster groups can be brought online and be moved between lateral and remote nodes.
Uninstalling Cluster Enabler

There are three supported scenarios for uninstalling Cluster Enabler from a configured cluster:

1. To remove some cluster nodes and leave CE on the remaining cluster nodes:
   a. Open Microsoft Cluster Administrator.
   b. Ensure no cluster resource groups are owned by the nodes you will remove. Move any owned resource groups to a different node.
   c. Right-click the nodes to remove and choose **Stop Cluster Service**. Wait for the cluster service to stop on the nodes as indicated by a red X.
   d. Right-click the nodes you want to remove and choose **Evict**. Evicting a node will uninstall the cluster service on that node and remove that node from the cluster.
   e. After evicting nodes, open CE Manager and right-click the **cluster name**. Choose **Storage Discover** and follow through the procedure steps to complete the Storage Discover Wizard.

   **Note:** If CE Manager is already open, perform a refresh before running the Storage Discover Wizard.

   f. Uninstall CE from the evicted nodes. Use the **Add/Remove Programs** utility in the Control Panel to remove CE for MSCS. Reboot when prompted to complete the uninstall.

2. To Uninstall CE from all nodes of the cluster and deconfigure the CE cluster. The Windows Server failover cluster will be maintained:
   a. Right-click only the remote nodes and choose **Evict**.
   b. After evicting nodes, open CE Manager and right-click the **cluster name**. Choose **Storage Discover** and follow through the procedure steps to complete the Storage Discover Wizard.

   **Note:** If CE Manager is already open, perform a refresh before running the Storage Discover Wizard.

   c. From the CE Manager, select **Deconfigure CE**.
d. Uninstall CE from all nodes. Use the Add or Remove Programs utility in the Control Panel to remove Cluster Enabler. Reboot when prompted to complete the uninstall.

3. To Uninstall CLuster Enabler from all nodes of the cluster and destroy the cluster:

   a. Destroy the cluster using Microsoft Cluster Administrator.

   b. Uninstall CE from all nodes. Use the Add or Remove Programs utility in the Control Panel to remove CE. Reboot when prompted to complete the uninstall.
This chapter provides instructions for using the Cluster Enabler Manager graphical user interface.

- Getting started using the CE Manager ........................................... 82
- Using the CE Configuration Wizard ............................................... 85
- Managing a CE cluster .................................................................. 89
- Managing a CE cluster group ....................................................... 95
- Storage component .................................................................... 102
- Viewing information ................................................................... 106
- Cluster Enabler logging ................................................................. 115
- Restore and recovery operations .................................................. 119
- Configuring a custom resource .................................................... 131
Getting started using the CE Manager

The Cluster Enabler (CE) Manager GUI (graphic user interface) allows you to configure your Microsoft Failover Clusters (or MSCS clusters) for disaster recovery protection. The CE Manager allows you to set up and configure disk-based resources to automatically move geographically dispersed resource groups back and forth.

The CE Manager provides several wizards to assist you in completing various cluster tasks. The first step towards managing disaster recovery for distributed failover clusters is to run the Configuration Wizard to configure a CE cluster.

The Cluster Enabler Manager window

The CE Manager window shown in Figure 17 contains a menu bar, two views, and a navigation tree. After cluster configuration, the navigation tree can be expanded to show four separate components: Groups, Storage, Sites, and Nodes.
Cluster Enabler wizards

Wizards are a series of dialog boxes that step you through the completion of a complex task. The Cluster Enabler Manager provides several wizards, as follows:

Configuration Wizard
The Configuration Wizard is used to configure a CE cluster. The configuration process is the first step towards managing disaster recovery for distributed failover clusters. The Configuration Wizard will step you through the process of configuring your failover cluster for management with CE. “Using the CE Configuration Wizard” on page 85 provides detailed instructions for using the wizard.

Storage Discover Wizard
The Storage Discover Wizard automatically discovers and sets up the attached storage. The storage discovery process should be performed after any changes have been made to the storage configuration. “Storage Discover Wizard” on page 89 provides detailed instructions for using the wizard.

Update Mirror Pairs Wizard
The Update Mirror Pairs Wizard steps you through the process of discovering storage, updating the storage configuration, validating the storage groups, and setting up the storage group definitions in the cluster properties database to update the mirrored pairs in a cluster. “Update Mirrored Pairs Wizard” on page 90 provides detailed instructions for using the wizard.

Change Quorum Wizard
The Change Quorum Wizard steps you through the process of changing a cluster’s quorum model type. “Change Quorum Model Wizard” on page 91 provides detailed instructions for using the wizard.

Create Group Wizard
The Create Group Wizard steps you through the process of creating a CE Group, adding devices and selecting a group policy. “Create Group Wizard” on page 95 provides detailed instructions for using the wizard.

Modify Group Wizard
The Modify Group Wizard steps you through the process of adding or removing devices in a CE group. “Modify Group Wizard” on page 99 provides detailed instructions for using the wizard.
Recover CE Cluster Wizard

The “Recover CE Cluster Wizard” on page 124 is used to automatically recover and restore a CE cluster.
Using the CE Configuration Wizard

Cluster Enabler provides a wizard for configuring a CE cluster. The configuration process is the first step towards managing disaster recovery for distributed failover clusters. The Configuration Wizard will step you through the process of configuring your failover cluster for management with CE.

If any of the steps in wizard configuration process fail, the wizard will display a list of the specific errors for each node on a Summary page. Note each error to be corrected and click Finish to exit the wizard. After the listed summary problems have been fixed, launch the configuration wizard again to configure the CE cluster.

Note: Whether running Windows Server 2003 or 2008, the applicable Microsoft Failover Clusters (MSCS clusters) or Failover Clusters must be installed on at least one node prior to configuring a cluster.

Follow these steps to configure a CE cluster using the Configuration Wizard:

1. Select the EMC Cluster Enabler icon from the Navigation Console Tree and click the Configure CE Cluster link in the center pane. This opens the first page of the Configuration Wizard. The Configuration Wizard can also be launched using the right-click or Action menus.

2. The Enter cluster name page appears. Enter a Cluster Name or Node Name in the space provided and click Configure. If you do not know the cluster name, you can click Browse to browse an active directory of clusters. Select a cluster name from the list and click OK, then click Add. Click Configure. If you do not enter a name and click Configure, the default will automatically detect the current clusters on the server and continue. Figure 18 on page 86 shows the first page of the Configuration Wizard.

Note: Select Upgrade only if you have upgraded your system from Cluster Enabler Version 2.1 and above. This will enable your existing CE clusters to be configured through the wizard. This is explained in “Upgrade procedures” on page 74.
3. The Current Nodes page appears listing the current nodes in the cluster. To add a node, enter the node name and click **Add**. If you do not know the node name, you can click **Browse** to browse an active directory of computers. Select a computer name from the list and click **OK**, then click **Add**. Click **Next**.

4. The Validating System Setup process begins. This automated step validates the system configuration by checking that the appropriate versions of Solution Enabler, Cluster Enabler, and Microsoft Failover Clusters (or MSCS) are installed and configured. Upon the Validation Complete notification, click **Next**.
Using the CE Configuration Wizard

5. The Storage Discovery process begins. This automated step performs a storage discovery for each cluster node to identify the locally-attached and remotely-attached storage. Upon the Discover Completed notification, click Next.

   **Note:** If the storage discovery process fails, the wizard will list the storage discovery errors for each node on the Summary page. Note each error to be corrected and click Finish to exit the wizard.

6. The Storage Setup process begins. This automated step performs a storage setup for each cluster node. Upon Setup of Storage Configuration Completed, click Next.

   **Note:** If the storage setup process fails, the wizard will list the storage setup errors for each node on the Summary page. Note each error to be corrected and click Finish to exit the wizard.

7. The Validating Groups process begins. This automated step performs a group validation for each converted failover cluster group. Upon Validated Groups, click Next.

   **Note:** If the validating groups process fails, the wizard will list the validation errors for each node on the Summary page. Note each error to be corrected and click Finish to exit the wizard.

8. The Summary page appears. Upon Configuration Wizard Completed Successfully, click Finish to exit the wizard.

9. After exiting the CE Configuration Wizard, Cluster Enabler will connect to the newly configured cluster. Once connected to the cluster, you will notice that the configured cluster node is now visible in the navigation tree, located in the left pane.

10. Double-click the cluster icon to expand the cluster and view the following folders: Groups, Storage, Sites, and Nodes. You are now ready to begin managing your cluster. Figure 19 on page 88 shows an example view of the expanded CE Manager navigation tree.
Adding nodes

Adding new nodes is also accomplished through using the CE Configuration Wizard. The CE Configuration Wizard steps you through the process of adding a cluster node for management with CE. New nodes must be added using CE Manager and not Microsoft Failover Cluster.
Managing a CE cluster

Once your CE cluster has been configured using the CE Configuration Wizard, you are ready to begin managing the cluster. Even after you exit Cluster Enabler and close the application, your cluster will remain configured unless you perform a deconfigure or delete action on the cluster.

Follow these instructions to begin managing your cluster.

1. Select the EMC Cluster Enabler icon from the Navigation Console Tree and click the Manage CE Cluster link in the center pane. The Manage CE Cluster option can also be launched by using the right-click or Action menus.

2. Enter the cluster name in the selection box. If you do not enter a name, the default will automatically connect to a cluster accessible on the server. Click OK.

3. Once connected to the cluster, you will notice that the configured cluster node is now visible in the navigation tree located in the left pane. Double-click the cluster icon to expand the cluster and view the following folders: Groups, Storage, Sites and Nodes. You are now ready to begin managing your cluster.

Cluster Enabler Manager allows you to perform the following cluster management actions on configured clusters. When a particular action is accessed, the appropriate wizard process is launched to assist you in completing the task.

Storage Discover Wizard

The Storage Discover Wizard helps you to automatically discover and setup the attached storage. The storage discovery process should be performed after any changes have been made to the storage configuration.

Follow these steps to automatically discover and set up your attached storage using the Storage Discover Wizard:

1. Select the Cluster icon from the Navigation Console Tree and select Action and Storage Discover from the menu bar. This opens the first page of the Storage Discover Wizard. The Storage Discover Wizard can also be launched by using the right-click or Action menus.
2. The Storage Discovery page appears. Upon the Discover Completed notification, click **Next**.

**Note:** If any storage discovery process fails, the wizard will list the discovery errors for each node on the Summary page. Note each error to be corrected and click **Finish** to exit the wizard.

3. The Storage Setup page appears. Upon the Set up of Storage Configuration Completed notification, click **Next**.

4. The Summary page appears. Upon the Discovered all Nodes notification, click **Finish** to exit the wizard.

5. Cluster Enabler will then refresh the CE cluster to reflect any storage changes.

---

**Update Mirrored Pairs Wizard**

The Update Mirrored Pairs Wizard helps you update the mirrored pairs in a cluster. This wizard steps you through the various processes of discovering storage, updating the storage configuration, validating the storage groups, and setting up the storage group definitions in the cluster properties database to update the mirrored pairs in a cluster.

Follow these steps to update the mirrored pairs in a cluster using the Update Mirror Pairs Wizard:

1. Select the **Cluster** icon in the navigation tree and select **Action**, **More Actions...** and **Update Mirror Pairs** from the menu bar. The Update Mirror Pairs Wizard can also be launched using the right-click or Action menus.

2. The first page of the Update Mirror Pairs Wizard opens and begins the Storage discovery process. Upon the Discover Complete notification, click **Next**.

3. The Storage setup process begins setting up the storage configuration. Upon the Setup of Storage Configuration Completed notification, click **Next**.

4. The Validating Groups process begins validating each group in the cluster. Upon the Validated Groups notification, click **Next**.
5. The Updating Storage Mirror Relationships process begins updating the mirrored pairs in the groups. Upon the Update mirror pairs for groups notification, click **Next**.

6. The Summary page appears. Upon Update Mirror Pairs Completed Successfully, click **Finish** to exit the wizard.

---

**Change Quorum Model Wizard**

The Change Quorum Wizard changes the quorum model of a cluster. This wizard will step you through the various processes of changing a cluster’s quorum model type. For Windows Server 2003, Cluster Enabler allows you to change the cluster model type between Shared Quorum, Majority Node Set (MNS), and MNS with File Share Witness. For Windows Server 2008, Cluster Enabler allows you to change the cluster model type between No Majority: Disk Only, Node Majority, Node and Disk Majority, and Node and File Share Majority.

**Note:** MirrorView/CE V3.0 supports only Windows Server 2003 Majority Node Set (MNS), and MNS with File Share Witness or Windows Server 2008 Node Majority, and Node and File Share Majority.

**Supported model type descriptions**

Microsoft has introduced the following new terminology and quorum options for Windows Server 2008:

- **Shared Quorum** is now referred to as **No Majority: Disk Only**
- **Majority Node Set (MNS)** is now referred to as **Node Majority**
- **MNS with File Share Witness** is now referred to as **Node and File Share Majority**
- A new mode on 2008 is **Node and Disk Majority**

**Shared Quorum** or **No Majority: Disk Only** — This quorum model can sustain failures of all nodes except one (if the disk is online). In the event of a quorum disk failure using this quorum model, the entire cluster would shut down if the quorum disk is lost.

**Majority Node Set** or **Node Majority** — This cluster model is recommended for clusters with an odd number of nodes. The cluster can sustain failures of half the nodes (rounding up) minus one. For example, a seven node cluster can sustain three node failures.
MNS with File Share Witness or Node and File Share Majority — This cluster model is recommended for clusters with special configurations. It works in a similar way to Node and Disk Majority, but instead of a witness disk, this cluster uses a witness file share. Note that if you use Node and File Share Majority, at least one of the available cluster nodes must contain a current copy of the cluster configuration before you can start the cluster. Otherwise, you must force the starting of the cluster through a particular node.

**Note:** Windows Server 2003 only supports 2-node clusters with this quorum model.

Node and Disk Majority — This cluster model is recommended for clusters with an even number of nodes. It can sustain failures of half the nodes (rounding up) if the witness disk remains online. For example, a six node cluster in which the witness disk is online could sustain three node failures. It can sustain failures of half the nodes (rounding up) minus one if the witness disk goes offline or fails. For example, a six node cluster with a failed witness disk could sustain two (3-1=2) node failures.

**Using the Change Quorum Wizard**

Once your Microsoft cluster has been configured as a CE cluster, you must use this wizard for all quorum model changes. If your configured CE clusters are Shared Quorum or No Majority: Disk Only model type, you can use this wizard to change the selected quorum disk. You can also use this wizard to change the file share for configured CE clusters of Majority Node Set with File Share Witness or Node and File Share Majority model types.

**Note:** To change the quorum model to "Node and File Share Majority" in Windows Server 2008, you must first update the FileShare permissions to add the Cluster Name and allow "Change" and "Read" permissions for the file share. Your windows documentation provides instructions on changing permissions for FileShare.

Figure 20 on page 93 shows the first page of the Change Quorum Wizard for Windows Server 2008.
Change Quorum Model example

The following example steps through the processes of changing a Majority Node Set cluster to a Shared Quorum cluster for Windows Server 2003.

Follow these steps to change the quorum model type of a cluster using the Change Quorum Wizard:

1. Select the **Cluster** icon in the navigation Console tree and select **Action**, **More Actions**... and **Change Quorum Model** from the menu bar. The Change Quorum Model Wizard can also be launched by using the right-click or Action menu.

2. Cluster Enabler automatically begins by reading the storage configuration.

3. Once the storage configuration has been read, the first page of the Change Quorum Wizard opens. Select the **New Cluster Model** radio button for the model you want to convert the cluster to. In this example, we are changing the cluster model from a Majority Node Set cluster to a Shared Quorum cluster. Click **Next**.
4. The Select Quorum Disk page opens. Select the quorum disk that you want to use for the quorum disk-based cluster. Figure 21 on page 94 shows an example. Click Next.

![Select Quorum Disk](image)

- **Figure 21 Select Quorum Disk**

5. The Select Cluster Number page appears. The wizard will automatically generate a list all of the available cluster numbers. From the Select a Cluster Number scroll box, select the Cluster Number that you want to use for the cluster. Click Next.

   Note: Check the Show All Cluster Numbers box to view all of the cluster numbers both used and unused for the system. Do not select a number that is already used.

6. The Validate Cluster Model process automatically begins validating the chosen cluster model. Upon the Validation of Cluster Model Successfully notification, click Next.


8. The Summary page appears. Upon the Changed Cluster Model Successfully notification, click Finish to exit the wizard.

9. In the Cluster Enabler Manager, select the Cluster icon, notice that the Cluster Type is now Shared Quorum.
Managing a CE cluster group

Cluster Enabler Manager provides several group actions for managing CE cluster groups. There are two automation wizards available for groups, the Create Group Wizard and the Modify Group Wizard. The Create Group Wizard steps you through the process of creating a CE cluster group. The Modify Group Wizard allows you to edit an existing cluster group by adding or removing devices to and from the group. The group action features also allow you to deconfigure a CE group to convert it back to a cluster group or to delete a group.

Create Group Wizard

The Create Group Wizard will step you through the process of creating a CE Group, adding devices and selecting a group policy.

Follow these steps to create a CE Group using the Create Group Wizard:

1. Select the Groups icon from the Navigation Console Tree and select Action and Create Group from the menu bar. This begins the process of reading the storage configuration. After the storage has been read, the first page of the Create Group Wizard opens. The Create Group Wizard can also be launched using the right-click or Action menus.

   Note: A mirror needs to be present on the array before attempting to create a group. Run the Storage Discover Wizard to detect a newly created mirror.

2. The Enter Group Name page appears. Enter a unique Group Name in the space provided and click Create. Click Cancel to abort the operation and close the wizard.

3. The next wizard page prompts you to select devices for inclusion in the new group. Select the desired devices from the list shown by clicking in the select boxes. Selected devices are identified by the checked box. Click Next. Figure 22 on page 96 and Figure 23 on page 96 show example wizard pages for adding devices.

   Note: Selecting the RA Group will automatically select Async Group to show SRDF/Asynchronous devices.
Using Cluster Enabler Manager

**Figure 22** Create Group Wizard, Select Symmetrix Devices

**Figure 23** Create Group Wizard, Select CLARiiON Devices
4. The Select Group Policy page appears. From the pull-down menu, select your desired policy for the group. You can select either the **Restrict Group Movement** or **Automatic Failover**. Once selected, click **Next**. Figure 24 on page 97 shows an example of the SRDF/CE wizard page. Figure 25 on page 98 shows an example of the MirrorView/CE wizard page.

The *Restrict Group Movement* selection restricts the group from failing over to a peer node. In an SRDF or MirrorView link failure, this setting will only attempt to move disk laterally. If the link is up, this setting has no impact.

The *Automatic Failover* policy sets the group to automatically failover to another node in the event of a node or network failure.

![Create Group Wizard, Symmetrix Select Group Policy](image)
5. The Summary page appears. Upon Group Created Successfully, click **Finish** to exit the wizard.

6. Cluster Enabler automatically begins refreshing the CE Cluster. Upon completion of the refresh, you should see the group that you created listed under Groups. If you do not see the newly created group, select **Action** and **Refresh** from the menu bar. The Refresh action can also be accessed from the right-click or Action menus.
The Modify Group Wizard will step you through the process of adding or removing devices in a CE group.

Follow these steps to add or remove devices from a CE Group using the Modify Group Wizard:

1. Select the **Groups** icon in the navigation tree and select **Action** and **Modify Group** from the menu bar. This begins the Storage Synchronization process. After the storage has finished synchronizing, the first page of the Modify Group Wizard opens. The Modify Group Wizard can also be launched using the Right-click or Action menus.

2. From the Select Devices page, select the Action from the pull-down menu for either **Add Devices** or **Delete Devices**. Depending on your selection, a list of available devices that can be added or removed will display. Select the desired devices from the list shown by clicking in the select boxes. Selected devices are identified by the checked box. Click **Next**. Figure 26 shows this wizard page.
3. The Validate Selection page appears, click **Next** to validate your selection or click **Cancel** to abort the action.

4. The Summary page appears. Upon Group Modified Successfully, click **Finish** to exit the wizard.

5. Cluster Enabler automatically begins refreshing the CE cluster. Upon completion of the refresh, you should see the updated group information reflecting the devices added or deleted. If you do not see the updated group information, select **Action** and **Refresh** from the menu bar. The Refresh action can also be accessed from the right-click or Action menus. Figure 27 displays a summary of the modified group from this example.

![Figure 27 Modified group with added device](image)

### Deconfigure a CE group

To deconfigure a CE group, select a **group** listed under the Groups icon located in the Navigation Console Tree and select **Action** and **Deconfigure CE Group** from the menu bar. The deconfigure option can also be accessed by using the Right-click or Action menus. A dialog box pop-up will appear asking you to confirm the action. Click **Yes** to convert the group or **No** to abort the action.

**CAUTION**

If the group is deconfigured, CE failover support to the remote nodes will no longer be operational. To make group failover operational again, you will need to reconfigure the cluster group using the CE Configuration Wizard in the CE Manager.
Delete a CE group

To delete a CE group, select a group listed under the Groups icon located in the Navigation Console Tree and select Action and Delete Group from the menu bar. The delete group option can also be accessed using the Right-click or Action menus. A dialog box pop-up will appear asking you to confirm the action. Click Yes to delete the group or No to abort the action.

Note: Deleting a CE group deconfigures the group and then removes it from the cluster.
**Storage component**

Selecting the Storage icon from the navigation tree allows you to view the attached storage device information for each storage array. Select a storage array to view the summary information columns in the center pane. **Figure 28** shows the CE Manager Storage component view for a Symmetrix array.

**Figure 28** Example of Symmetrix storage array view
Figure 29 shows the CE Manager Storage component view for CLARiiON.

Table 3 on page 103 lists the heading information that is displayed for Symmetrix and CLARiiON storage arrays.

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The Symmetrix or CLARiiON array ID (such as, Symmetrix+00187900830 or CLARiiON+AMP00070902744).</td>
</tr>
<tr>
<td>Version</td>
<td>For Symmetrix arrays, displays the Enginuity version. For CLARiiON, displays the FLARE version.</td>
</tr>
</tbody>
</table>
| Device ID             | For Symmetrix arrays, shows all SRDF R1/R2 device IDs that are mapped to any cluster member node.  
                         | For CLARiiON arrays, shows all MirrorView/S primary and secondary device IDs that are mapped to any cluster member node. |
| Cluster Group Name    | Indicates the CE Group name to which the device belongs.                                                                                  |
| Device Group Name     | Indicates the SYMAPI device group name to which the device belongs; derived from Cluster Group name.                                      |
### Table 3  Storage component displayed information (continued)

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consistency Group Name</td>
<td>Indicates the consistency group name to which the remote CLARiiON mirror belongs; derived from Cluster Group name.</td>
</tr>
<tr>
<td>Owning Node</td>
<td>If a device belongs to a cluster group, the owning node information is obtained directly from Microsoft Failover Cluster (MSCS). Otherwise, the owning node is a node where the device is write-enabled.</td>
</tr>
<tr>
<td>Mount Points</td>
<td>Indicates the mount point of the physical drive on the owning node.</td>
</tr>
<tr>
<td>Sync State</td>
<td>For Symmetrix arrays, indicates the RDF state for the group. The <em>EMC Solutions Enabler SRDF Family CLI Product Guide</em> provides a listing of all possible RDF states. For CLARiiON arrays, indicates the CLARiiON consistency group state. Navisphere Manager Help or the <em>EMC MirrorView/Synchronous Command Line Interface (CLI) Reference</em> provides a listing of all possible states.</td>
</tr>
<tr>
<td>Device Status</td>
<td>For Symmetrix arrays, indicates the SRDF R1/R2 device status. The possible device status states are Ready, Not Ready, and Write-Disabled. For CLARiiON arrays, indicates the MirrorView/S Primary/Secondary device status. The possible device status states are Online, Offline, and Write-Disabled.</td>
</tr>
<tr>
<td>Capacity MB</td>
<td>Shows the device capacity in megabytes.</td>
</tr>
<tr>
<td>Swap Capable</td>
<td>Shows whether the device is swap capable (True or False).</td>
</tr>
<tr>
<td>Async Capable</td>
<td>Shows whether the device is asynchronous capable (True or False).</td>
</tr>
<tr>
<td>WWN</td>
<td>Displays the devices World Wide Name (WWN).</td>
</tr>
<tr>
<td>Logical Device</td>
<td>Shows the logical device name (if applicable).</td>
</tr>
<tr>
<td>RDF Type</td>
<td>For Symmetrix arrays, shows the RDF device type of R1 or R2.</td>
</tr>
<tr>
<td>RA Group</td>
<td>For Symmetrix arrays, indicates the RA group to which the group belongs.</td>
</tr>
<tr>
<td>R1 Invalid Tracks</td>
<td>For Symmetrix arrays, indicates the number of invalid R1 track (if any).</td>
</tr>
<tr>
<td>R2 Invalid Tracks</td>
<td>For Symmetrix arrays, indicates the number of invalid R2 track (if any).</td>
</tr>
<tr>
<td>RDF Async Lag Time</td>
<td>For Symmetrix arrays, indicates the lag time between the target (R2) device and the source (R1) device in an SRDF/Asynchronous environment.</td>
</tr>
<tr>
<td>Device Config</td>
<td>For CLARiiON arrays, displays the current CLARiiON device configuration.</td>
</tr>
</tbody>
</table>
Using Cluster Enabler Manager

Adding and removing devices from a group

From the storage view, when you select a device listed in the center pane, you can add or remove it from the group by clicking the **Add to Group** or **Remove from Group** icons displayed in the right Action pane. **Figure 30** displays the storage actions located in the right action pane.

![CE Manager storage actions](image)

<table>
<thead>
<tr>
<th>Device State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For CLARiiON, displays whether the disk is bound or unbound to a consistency group.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For CLARiiON, displays the device role as primary or secondary in a remote mirror.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MV Async</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For CLARiiON, this column is not currently applicable as asynchronous transfer is not supported in this release of Cluster Enabler.</td>
<td></td>
</tr>
</tbody>
</table>

**Table 3** Storage component displayed information (continued)

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device State</td>
<td>For CLARiiON, displays whether the disk is bound or unbound to a consistency group.</td>
</tr>
<tr>
<td>Device Role</td>
<td>For CLARiiON, displays the device role as primary or secondary in a remote mirror.</td>
</tr>
<tr>
<td>MV Async</td>
<td>For CLARiiON, this column is not currently applicable as asynchronous transfer is not supported in this release of Cluster Enabler.</td>
</tr>
</tbody>
</table>

**Figure 30** CE Manager storage actions

When you select the action, Cluster Enabler opens the “Modify Group Wizard” at the validation step. Click **Next** to add or remove your selection. The **Summary** dialog box appears. Upon Group Modified Successfully, click **Finish** to exit the wizard.
Viewing information

Cluster Enabler allows you to view certain summary information about CE Groups, Storage, Sites and Nodes. This information is displayed in the center pane as you select each of the icons located in the navigation tree. “Storage component” on page 102 describes the storage information and available actions. Summary information for Groups, Nodes, and Sites are described below.

Displaying group information

Selecting the Groups icon from the navigation tree allows you view group information for all configured CE cluster groups in the center pane. Double-clicking on a specific group displays summary information for that group. Figure 31 displays the CE Manager group component.

![CE Manager Groups component](image)

Selecting a specific group icon from the navigation tree allows you view the group summary information columns for each configured CE cluster group in the center pane. Figure 32 on page 107 displays the CE Manager group information for a specific group.
Figure 32  **CE Manager groups information**

Table 4 lists the heading information that displays for CE Groups.

**Table 4  **Groups component displayed information**

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Group Name</td>
<td>Indicates the CE Group name to which the device belongs.</td>
</tr>
<tr>
<td>Device Group Name</td>
<td>Indicates the SYMAP device group name to which the device belongs; derived from Cluster Group name.</td>
</tr>
<tr>
<td>Consistency Group Name</td>
<td>Indicates the consistency group name to which the remote CLARiiON mirror belongs; derived from Cluster Group name.</td>
</tr>
<tr>
<td>Owning Node</td>
<td>Shows the failover cluster node name that owns the particular group. This information is obtained directly from MS Failover Cluster (MSCS). Only groups that are part of the cluster will display.</td>
</tr>
<tr>
<td>Sync State</td>
<td>For Symmetrix arrays, indicates the RDF state for the group. The <em>EMC Solutions Enabler SRDF Family CLI Product Guide</em> provides a listing of all possible RDF states, For CLARiiON arrays, indicates the CLARiiON consistency group state. Navisphere Manager Help or the <em>EMC MirrorView/Synchronous Command Line Interface (CLI) Reference</em> provides a listing of all possible states.</td>
</tr>
<tr>
<td>Devices</td>
<td>Listed by disk resource name in the cluster.</td>
</tr>
<tr>
<td>Cluster Resource Name</td>
<td>Listed by physical disk resource name.</td>
</tr>
</tbody>
</table>
Using Cluster Enabler Manager

Table 4  Groups component displayed information (continued)

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner Device ID</td>
<td>The Symmetrix or CLARiiON device ID mapped to the owning node (such as, ODEC, ODED).</td>
</tr>
<tr>
<td>Owner Storage ID</td>
<td>The Symmetrix or CLARiiON array ID (such as, Symmetrix+00187900830 or CLARiiON+AMP00070902744).</td>
</tr>
<tr>
<td>Mount Points</td>
<td>Indicates the mount point of the physical drive on the owning node.</td>
</tr>
</tbody>
</table>

Clicking the **Display Events** icon option in the action pane displays event information in the lower tier of the center pane. **Table 5** lists the heading information that displays for CE Groups events.

Table 5  Groups event information

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>Shows the date and time that the recorded event occurred.</td>
</tr>
<tr>
<td>Computer Name</td>
<td>Indicates the computer name on which the event occurred.</td>
</tr>
<tr>
<td>Group Name</td>
<td>Indicates the group name to which the event occurred.</td>
</tr>
<tr>
<td>Message</td>
<td>Displays a detailed message of the event type.</td>
</tr>
</tbody>
</table>
Displaying node information

Selecting the **Nodes** icon from the navigation tree allows you view node information for all nodes in the center pane. Double-clicking on a specific node displays summary information for that node. **Figure 33** displays the CE Manager nodes component.

**Figure 33**   CE Manager Nodes component
Selecting a specific node icon from the navigation tree allows you view the node summary information columns for each node in the center pane. Figure 34 displays the CE Manager node information for a specific node.

![CE Manager node information](image)

**Table 6**  
<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the node name.</td>
</tr>
<tr>
<td>OS Name</td>
<td>Displays the Windows operating system (such as, 2003 SP2).</td>
</tr>
<tr>
<td>OS Version</td>
<td>Displays the Windows operating system version (such as, 5.2.3790).</td>
</tr>
<tr>
<td>System Type</td>
<td>Displays the Windows system type (such as, X86).</td>
</tr>
<tr>
<td>Cluster Group Name</td>
<td>Indicates the CE Group name to which the device belongs.</td>
</tr>
</tbody>
</table>
Clicking the **Display Events** icon option in the action pane displays event information in the lower tier of the center pane. Table 7 lists the heading information that displays for CE Node events.

### Table 6  Nodes component displayed information (continued)

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Group Name</td>
<td>Indicates the SYMAPI device group name to which the device belongs; derived from Cluster Group name.</td>
</tr>
<tr>
<td>Consistency Group Name</td>
<td>Indicates the consistency group name to which the remote CLARiiON mirror belongs; derived from Cluster Group name.</td>
</tr>
<tr>
<td>Owning Node</td>
<td>Shows the failover cluster node name that owns the particular group. This information is obtained directly from MS Failover Cluster (MSCS). Only groups that are part of the cluster will display.</td>
</tr>
<tr>
<td>Sync State</td>
<td>For Symmetrix arrays, indicates the RDF state for the group. The <em>EMC Solutions Enabler SRDF Family CLI Product Guide</em> provides a listing of all possible RDF states, For CLARiiON arrays, indicates the CLARiiON consistency group state. Navisphere Manager Help or the <em>EMC MirrorView/Synchronous Command Line Interface (CLI) Reference</em> provides a listing of all possible states.</td>
</tr>
<tr>
<td>Devices</td>
<td>Listed by cluster resource name.</td>
</tr>
</tbody>
</table>

### Table 7  Node event information

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>Shows the date and time that the recorded event occurred.</td>
</tr>
<tr>
<td>Computer Name</td>
<td>Indicates the computer name on which the event occurred.</td>
</tr>
<tr>
<td>Group Name</td>
<td>Indicates the group name to in which the event occurred.</td>
</tr>
<tr>
<td>Message</td>
<td>Displays a detailed message of the event type.</td>
</tr>
</tbody>
</table>
Displaying site information

Selecting the Sites icon from the navigation tree allows you view site information for all sites in the center pane. Double clicking on a specific site displays summary information for that site. Figure 35 on page 112 displays the CE Manager Site component.

![CE Manager Sites component](image)

Figure 35 CE Manager Sites component

Selecting a specific site icon from the navigation tree allows you view the site summary information columns for each site in the center pane. Figure 36 on page 113 displays the CE Manager site information for a Symmetrix site.
Using Cluster Enabler Manager

Figure 36  CE Manager Symmetrix site information

Figure 37  CE Manager CLARiiON site information
Table 8 lists the heading information that displays for Symmetrix and CLARiiON sites.

### Table 8  Site component displayed information

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the Site name.</td>
</tr>
<tr>
<td>Number of Storage Units</td>
<td>Displays the number of storage units for this site.</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>Displays the number of nodes for this site.</td>
</tr>
<tr>
<td>Storage Unit Name &amp; ID</td>
<td>The Symmetrix or CLARiiON array ID (such as, Symmetrix+00187900830 or CLARiiON+AMP00070902744).</td>
</tr>
<tr>
<td>Version Information</td>
<td>For Symmetrix arrays, displays the Symmetrix Enginuity version. For CLARiiON arrays, displays the FLARE version.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Displays the node name.</td>
</tr>
<tr>
<td>OS Name</td>
<td>Displays the Windows operating system (such as, 2003 SP2).</td>
</tr>
<tr>
<td>OS Version</td>
<td>Displays the Windows operating system version (such as, 5.2.3790).</td>
</tr>
<tr>
<td>System Type</td>
<td>Displays the Windows system type (such as, X86).</td>
</tr>
<tr>
<td>Cluster Group Name</td>
<td>Indicates the CE Group name to which the device belongs.</td>
</tr>
<tr>
<td>Device Group Name</td>
<td>Indicates the SYMAPI device group name to which the device belongs; derived from Cluster Group name.</td>
</tr>
<tr>
<td>Consistency Group Name</td>
<td>Indicates the consistency group name to which the remote CLARiiON mirror belongs; derived from Cluster Group name.</td>
</tr>
<tr>
<td>Owning Node</td>
<td>Shows the failover cluster node name that owns the particular group. This information is obtained directly from MS Failover Cluster (MSCS). Only groups that are part of MS Failover Cluster (MSCS) will display.</td>
</tr>
<tr>
<td>Sync State</td>
<td>For Symmetrix arrays, indicates the RDF state for the group. The <em>EMC Solutions Enabler SRDF Family CLI Product Guide</em> provides a listing of all possible RDF states. For CLARiiON arrays, indicates the CLARiiON consistency group state. Navisphere Manager Help or the <em>EMC MirrorView/Synchronous Command Line Interface (CLI) Reference</em> provides a listing of all possible states.</td>
</tr>
<tr>
<td>Devices</td>
<td>Listed by cluster resource name.</td>
</tr>
</tbody>
</table>
Cluster Enabler logging

Cluster Enabler incorporates various logging capabilities to create application detail logs. The amount of detail that these logs contain is controlled by the logging level. The user can adjust the logging level. Refer to “Changing the logging level” on page 118 for instructions. Under normal operating conditions error, warning, and information entries will be written to the application detail log. When verbose logging is enabled, these logs contain enough information to help developers diagnose various application failures.

By default, logs are stored in

C:\Program Files\EMC\Cluster-Enabler in a file called ce_event_trace.etl

This is a binary file. To create a readable version, you have to run the extraction program called CE_EventTraceDump.exe. “Extracting logs” on page 116 provides more detail and some extraction examples.

To help manage logging disk space the binary file is closed each night at midnight and renamed to ce_event_trace_yyyymmddhhmmss.etl where yyyymmddhhmmss is the current date and time. By default, 7 days worth of logs will be saved. The user can control how many days of logs are saved. Refer to “Changing logging retention period” on page 118 for instructions. Each days logs will grow as needed.

Disk space requirements

There is no limit to the log file size. The amount of disk space needed depends on the logging level and the amount of cluster activity taking place. As a general guide, you might expect 50 KB per day for a logging level of normal. If the logging level is set to verbose, and cluster activity is greater than normal, it might not be uncommon to expect 200 MB or more per day.
Extracting logs

There are some options available from the CE_EventTraceDump.exe application for extracting logs. Table 9 presents a full list of the available options and a brief explanation.

### Table 9 Options for log extraction

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-outdir &lt;outdir&gt;</td>
<td>Path to the output directory.</td>
</tr>
<tr>
<td>-outfile &lt;file&gt;</td>
<td>Path to the output file. Cannot be used with -split option.</td>
</tr>
<tr>
<td>-split</td>
<td>If specified, the text output file will be split into multiple files.</td>
</tr>
<tr>
<td>-from &lt;time&gt;</td>
<td>Specifies the start time. Format yyyy/mm/dd-hh:mm:ss.</td>
</tr>
<tr>
<td>-to &lt;time&gt;</td>
<td>Specifies the start time. Format yyyy/mm/dd-hh:mm:ss.</td>
</tr>
<tr>
<td>-sincelast</td>
<td>Only report log entries since the last time this program was run.</td>
</tr>
<tr>
<td>-xml</td>
<td>Output log entries in XML format.</td>
</tr>
<tr>
<td>-localtime</td>
<td>Output log entries in local time format not GMT format.</td>
</tr>
<tr>
<td>-offline</td>
<td>If specified the EventTraceService will not be stopped or started.</td>
</tr>
<tr>
<td>-help or -h or -?</td>
<td>Display usage information.</td>
</tr>
</tbody>
</table>

### Examples

Each of the following examples assume that the current working directory is `C:\Program Files\EMC\Cluster-Enabler` and that the default output is `C:\Program Files\EMC\Cluster-Enabler\Logs`.

From here on the `C:\Program Files\EMC\Cluster-Enabler\Logs` directory will be called the log directory.

#### Example 1

To extract the dump file to the log directory and name it `ce_event_trace_yyyyMMddhhmmss.txt`, enter:

`CE_EventTraceDump.exe`

To create the output file in XML format you can specify the `-xml` option. In this case the output file will be in XML format instead of text format and the file naming will be `ce_event_trace_yyyyMMddhhmmss.xml`.

`CE_EventTraceDump.exe -xml`
Example 2
To create a dump file in a particular location using local time format, enter:

```
CE_EventTraceDump.exe -localtime -outfile C:\foo.txt
```

Example 3
To extract the dump file to a particular location, enter:

```
CE_EventTraceDump.exe -outfile C:\foo.txt
```

Example 4
To extract the dump file of multiple .etl files. The files will be merged and sorted before creating the dump file. The -offline option is useful for processing log files that have already been archived. The -offline option will not start and stop the CE Event Log Service.

```
CE_EventTraceDump.exe ce_event_trace_20080305000005.etl ce_event_trace_20080306000004.etl -offline
```

Example 5
To extract the dump file to a specified directory, enter:

```
CE_EventTraceDump.exe -outdir C:\logs
```

Example 6
This command will extract the dump file to the log directory, but allows specifying a from and to time to limit the logs file extraction. In this example only log entries between 1:00 and 2:00 on Mar 10, 2008 will be extracted.

```
CE_EventTraceDump.exe -from 2008/03/10-01:30:00 -from 2008/03/10-02:00:00
```

Example 7
This command will create a dump file in a particular location using local time format, but only show you the logs since the last time the CE_EventTraceDump.exe program was run.

```
CE_EventTraceDump.exe -sincelast -localtime -outfile C:\foo.txt
```

Example 8
This command will split the dump file into multiple parts. Each file will be named ce_event_trace_yyyyymmddhhmmss_999.txt. Where 999 is a number between 1 and 999.

```
CE_EventTraceDump.exe -split
```
Using Cluster Enabler Manager

Changing the logging level

The logging level is controlled by a registry key. To change the logging level follow these steps from the command line:

1. Type `regedit`
2. Edit `HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CE\Configuration\EventTraceLevel`. By default the level is set to 4. At this level error, warning, and informational messages will appear in the log file. To create verbose logs, you can change the value to a 5. At this level error, warning, informational, and verbose messages will be sent to the log file. Be aware that changing this level to a 5 will dramatically increase the amount of data that is sent to the log file. The `ce_eventrace` service does not need to be restarted. The new value will take effect in about 30 seconds.

Changing the logging directory

The logging directory is controlled by a registry key. To change the logging directory, follow these steps from the command line:

1. Type `net stop ce_eventrace`
2. Type `regedit`
3. Edit `HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CE\Configuration\EventTraceDirectory`. Your edited path must have a trailing backslash and must exist before you make this change.
4. Type `net start ce_eventtrace`

Changing logging retention period

The log retention period is controlled by a registry key. To change the log retention period, follow these steps from the command line:

1. Type `regedit`
2. Edit `HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CE\Configuration\EventTraceLogRetention`. The DWORD value represents the number of day’s worth of logs to keep. The `ce_eventtrace` service does not need to be restarted. The new value will take effect in about 30 seconds.
**Restore and recovery operations**

This section details some of the restore and recovery operations that should be performed for different types of failures.

The following SRDF/CE restore and recovery operations are provided in Section “SRDF/CE recovery procedures” on page 119:

- Section “Restoring a failed SRDF site” on page 119
- Section “Recover SRDF backup site in case of primary site failures” on page 121
- Section “Recovery from SRDF link failure” on page 121
- Section “Restrict group movement and recovery” on page 122
- Section “Recovery from a corrupt quorum log” on page 123
- Section “Symmetrix array replacement”
- Section “Recover CE Cluster Wizard” on page 124

The following MirrorView/CE restore and recovery operations are provided in Section “MirrorView/CE recovery procedures” on page 127:

- Section “Restoring a failed MirrorView/S site” on page 127
- Section “Recovering a MirrorView/S backup site in case of primary site failures” on page 128
- Section “Recovering from a MirrorView link failure” on page 129
- Section “CLARiiON array replacement” on page 130

**SRDF/CE recovery procedures**

This section details SRDF/CE restore and recovery operations that should be performed for different types of failures.

**Restoring a failed SRDF site**

The following procedure describes how to restore your storage system after a site failure occurs with all links lost:

1. Restore SRDF and IP links.
2. Restart all nodes.
3. Open CE Manager and connect to the cluster.
4. Perform Storage Discover from CE Manager.

Any groups that are failed over to a secondary site are in a split state. Groups that are not failed over are in suspended state. You can safely bring the groups that did not failover to a secondary site online at this point.

5. To restore groups that failed over to a secondary site, follow these steps:

**WARNING**

Choosing the wrong option for restore could cause data loss. Contact EMC support if you have any question about the commands that should be issued.

Assuming that the secondary site has good data and you want to copy this data to primary site, follow these steps:

a. Open the command line prompt.

b. Change the directory to `<CE Install Directory>`.

c. Set the `SYMCLI_DB_FILE` environment variable to `SRDFCESymapi.db`.

d. Run the following command for every failed-over group.

   ```bash
   symrdf -g <failed over group name> restore -incr
   ```

   e. Monitor the group state by running the following command:

   ```bash
   symrdf -g <groupname> query
   ```

Assuming that the primary site has good data and you want to copy this data to secondary site:

a. Open the command line prompt.

b. Change the directory to `<CE Install Directory>`.

c. Set the `SYMCLI_DB_FILE` environment variable to `SRDFCESymapi.db`.

d. Run the following command for every failed over group:

   ```bash
   symrdf -g <failed over group name> establish -incr
   ```

   e. Monitor the group state by running the following command:

   ```bash
   symrdf -g <groupname> query
   ```
Recover SRDF backup site in case of primary site failures

The following procedure describes how to recover a backup site when the primary site fails. Cluster Enabler V3.0 lets you set the failover option on a group basis.

For MNS clusters
You can restart the backup site using the /forcequorum option that is described in Microsoft clusters manual.

For Shared Quorum models
1. If the Cluster Group (the group in which the quorum disk is a member) does not have the failover option set to “Automatic Failover”, then the group will not failover to secondary node and therefore the cluster cannot be started. On one of the secondary nodes, use the Recover CE Wizard to start the cluster in “Safe Mode”. This starts the cluster service on this node with just the Cluster Group.

Once you have cluster service running on the secondary site:
2. Open CE Manager and connect to the cluster.
3. For each group that you want to failover, change the failover policy to “Automatic Failover”.
4. From MS Cluster Administrator/Failover Cluster Manager, bring all of these groups online.

At this point the cluster is running with required services at the backup site.

Recovery from SRDF link failure
This following two procedures describe how to recover from an SRDF link failure:

WARNING
Choosing the wrong option for restore could cause data loss. Contact EMC support if you have any question about the commands that should be issued.

- For groups that failed-over on the RDF link, when the link was in a failed state:
  a. Choose the remote mirror that has valid user/application data.
  b. Move the group to a node that has a valid mirror mapped.
c. Restore the SRDF link.
d. Open CE Manager and perform Storage Discover.
e. Open the command line prompt.
f. Set the `SYMCLI_DB_FILE=<CE InstallDir>\SRDFCESymapi.db`
g. If the R1 has valid data, enter the following command:
   `symrdf -g <groupname> establish -incr`

   If the R2 has valid data, enter the following command:
   `symrdf -g <groupname> restore -incr`

   • For groups that remained online on the same side as before the link failure:
     a. Restore SRDF link.
     b. Open CE Manager and run Storage Discover.

**Restrict group movement and recovery**

If a CE group has the "Restrict Group Movement" policy set and the RFD link is down, it may take a long time for the resource to come online if the user manually tries to move the group to a node that is connected to a different storage array. For example, if the user tries to move group G1 from the R1 side to the R2 side when the RDF link is down, then Microsoft’s preferred owner logic will attempt to bring the group online on the R2 side as expected.

But since the restrict group movement policy is set for the CE group, Microsoft will fail the resource on the R2 side nodes. This is correct behavior and is expected, but it may take a long time for the resource to fail on all the R2 nodes before coming back online on one of the R1 side nodes. This is because by default Microsoft will try to bring the group online 3 times on each node. The more nodes you have in the cluster the longer it will take for Microsoft to complete the preferred owner logic. To minimize this undesirable effect you can change the property of the resources to "Do not Restart". This will minimize number of retries and reduce the time required to bring the group online.
Recovery from a corrupt quorum log

The complete Microsoft article can be found on Microsoft Knowledge Base Article 172951 at the following site:

http://support.microsoft.com/kb/q172952

Symmetrix array replacement

The following process can be used to replace a Symmetrix array. This process assumes that all RDF groups are Dynamic and that all failover cluster (or MSCS) groups are configured for Swapping RDF personalities (SwapEnabled) during failover:

1. Change the Microsoft Failover Cluster (or MSCS) service start up to Manual on all cluster nodes.
2. Failover all groups to the Symmetrix array that you are NOT replacing. Now the groups are online on R1 side of RDF device.
3. Shutdown all nodes that are attached to the Symmetrix array that is being replaced.
4. Replace the R2 Symmetrix array and establish new R1/R2 relations.
5. Bring the SRDF link up and synchronize R2 with R1 data.
6. Wait for the synchronization to complete.
7. Adjust device masks on all nodes connected to new Symmetrix array, so that the devices are correctly mapped to these hosts.
8. Reboot the nodes attached to new Symmetrix array.
9. Open CE Manager on one of the nodes connected to R1 side.
10. Choose UpdateMirrorPair and step through the wizard processes.
11. Once UpdateMirrorPair wizard completes successfully, CE updates its internal configuration database to reflect new R1/R2 relations. At this point you should be able to failover groups between these Symmetrix array.
12. Reset the Cluster Service Startup type to Automatic.
Cluster Enabler provides a wizard to help you recover a failed shared quorum cluster by bringing the cluster online on a single node. The shared quorum cluster will fail to come online in a site failover scenario where the failover option for a quorum group is set to "Restrict Group Movement". The Recover CE Cluster Wizard changes the failover policy on quorum group to "Automatic Failover" and then brings the cluster online on the node. You can then use the Create Group Wizard to change other groups failover policies and bring them online appropriately.

**Note:** The Recover CE Cluster Wizard is useful for shared quorum clusters. To force a Majority Node Set (MNS) cluster node to form a cluster use the /forcequorum option as documented in your Microsoft Clusters documentation.

Follow these steps to automatically recover and restore a shared quorum cluster using the Recover CE Cluster Wizard:

1. Select the **EMC Cluster Enabler Manager** icon from the navigation tree and select **Action** and **Recover CE Cluster** from the menu bar. This opens the first page of the Recover CE Cluster Wizard. The wizard can also be launched by using the right-click or Action menus.

   **Note:** When running the Recover CE Wizard to recover a CE cluster, you should only run the wizard on a failed node when the entire cluster is down.

2. The Enter Node Name page appears. Type the **Cluster Name** and **Node Name**, click **Validate**. The Recover CE Wizard should only be run on a single node. **Figure 38 on page 125** shows the Enter Node Name page.
3. The Choose Tasks page appears. To restart a cluster in safe mode and bring the cluster online using previous CE cluster settings, select **Start Cluster in Safe Mode**. To resolve a cluster number for a Shared Quorum model cluster and recover the cluster, select **Resolve Cluster Number**. Click **Next**. Figure 39 on page 126 shows the Choose Tasks page.
4. If you selected **Resolve Cluster Number** in step 3 and are recovering a shared quorum model cluster, the following screen appears.

![Figure 39 Recover CE Cluster Choose Tasks](image)

![Figure 40 Recover CE Cluster Change Cluster Number](image)
The wizard will automatically generate a list all of the available cluster numbers. From the Select a Cluster Number scroll box, select the Cluster Number that you want to use for the cluster, click **Next**. Figure 40 on page 126 shows the Change Cluster Number page.

**Note:** Check the Show All Cluster Numbers box to view all of the cluster numbers both used and unused for the system. Do not select a number that is already used.

5. The Summary page appears and Cluster Enabler begins to restart the cluster service for the CE cluster. Upon "Started cluster service successfully", click **Finish**.

---

**MirrorView/CE recovery procedures**

This section details MirrorView/CE restore and recovery operations that should be performed for different types of failures.

**Restoring a failed MirrorView/S site**

The following procedure describes how to restore your CLARiiON storage array after a site failure:

1. Power on the storage at the failed state.
2. Restore the MirrorView and IP links.
3. All consistency groups that are not locally promoted are marked as “Waiting on Admin” in Navisphere. For each consistency group that is marked “Waiting on Admin”, do the following:
   a. From Navisphere, right-click on each consistency group and choose Synchronize from drop down-menu.
   b. Wait for consistency groups to synchronize.
4. Restoring consistency groups that are locally promoted at the secondary site is more detailed. For each consistency group that is locally promoted, perform the following sequence of steps:
   a. From Navisphere, destroy the consistency group on both CLARiiON arrays. Open **CG Properties** and click the **Force Destroy** button.
   b. Destroy the remote mirrors on the CLARiiON array at the failed site. Open **Mirror Properties**, select the **Primary Image** tab and click the **Force Destroy** button.
c. Remove the corresponding LUNs from the storage group on the CLARiiON array at the failed site.

d. Right-click each remote mirror on the CLARiiON array at the surviving site, and choose **Add Secondary Storage**.

e. Choose the LUN from the CLARiiON array at the failed site.

f. Create a new consistency group using the same name.

g. Add all remote mirrors that were part of the original consistency group.

h. Add the corresponding LUNs to the storage group on the CLARiiON array at the failed site.

5. Restart all nodes at the failed site.

6. Open the CE Manager and connect to the cluster.

7. Perform a Storage Discover from CE Manager.

8. Ensure that the groups can failover back and forth between the sites successfully.

---

**Recovering a MirrorView/S backup site in case of primary site failures**

The following procedure describes how to recover a backup site when the primary site fails. When a cluster loses majority, the Majority Node Set based cluster shuts itself down. In this scenario, you can restart the backup site using the `/forcequorum` option as described in your Microsoft Clusters documentation.

Once you have the cluster service running on the secondary site, do the following:

1. Open CE Manager and connect to the cluster.

2. For each group that you want to failover and bring online at the secondary site, change the group's failover policy to “Automatic Failover” by using the Create Group Wizard.

3. From the Microsoft Cluster Administrator/Failover Cluster Manager, bring all of these groups online.

At this point, the cluster is running with required services online at the back up site.
Recovering from a MirrorView link failure

The following two procedures describe how to recover from a MirrorView link failure:

- For groups that failed-over to the remote storage when the link was in a failed state:

  Any applications that failed over to the remote site during link failure will be locally promoted on the remote storage. These consistency groups will have their remote mirror relationship broken with the primary site. To restore the remote mirror relationship do the following:

  a. From Navisphere, destroy the consistency group on both CLARiiON arrays. Open CG Properties and click the Force Destroy button.

  b. Destroy the remote mirrors on the CLARiiON array at primary site. Open Mirror Properties, select the Primary Image tab and click the Force Destroy button.

  c. Remove the corresponding LUNs from the storage group on the CLARiiON array at the primary site.

  d. Right-click on each remote mirror on the CLARiiON array at the backup site and choose Add Secondary Storage.

  e. Choose the corresponding LUN from the CLARiiON array at the primary site.

  f. Create a new consistency group using the same name.

  g. Add all remote mirrors that were part of the original consistency group.

  h. Add the corresponding LUNs from the storage group on the CLARiiON array at primary site.

- For groups that remained online on the same side as before the link failure:

  a. From Navisphere, right-click on each consistency group and choose Synchronize from drop-down menu.

  b. Wait for the consistency groups to synchronize.
**CLARiiON array replacement**

The following procedure can be used to replace a CLARiiON array:

1. Change the Microsoft Failover Clusters (or MSCS) service start up to **Manual** on all cluster nodes.

2. Failover all groups to the CLARiiON array that you are not replacing. Now the groups are online on the primary side of the remote mirrors.

3. Shutdown all nodes that are attached to the CLARiiON array that is being replaced. If you are running a Majority Node Set cluster with an equal number of nodes at each site, this may result in shutting down the entire cluster. You may have to restart the cluster using the `/forcequorum` option as described in your Microsoft Clusters documentation.

4. Make a list of all consistency groups that are part of the cluster and their remote mirrors.

5. Delete consistency groups that are part of the cluster.

6. Replace the CLARiiON array and establish new remote mirror relationships.

7. Add secondary LUNs to the appropriate storage groups.

8. Wait for all remote mirrors to synchronize.

9. Create consistency groups and their respective remote mirrors.

10. Reboot the nodes attached to the new CLARiiON array.

11. Open CE Manager on one of the nodes connected to the primary site.

12. Choose Update Mirror Pairs and step through the wizard processes.

13. Once the Update Mirror Pairs Wizard completes successfully, CE updates its internal configuration database to reflect the new remote mirror pair relationships. At this point, you should be able to failover groups between the CLARiiON arrays.

14. Reset the Cluster Service Startup type to **Automatic** on all nodes.
Configuring a custom resource

This section provides examples of creating and modifying a custom resource using the CE Manager. A custom resource could be a Veritas volume or other third-party resource. Once a CE Group is created and the custom resource volumes are added, the storage resource will be comprised of either Symmetrix or CLARiiON disks.

Before you can configure a custom resource using the CE Manager, you must set up the custom resource using the vendor’s resource software (for example, Veritas Volume Manager). Then you must manually add the custom resource to Microsoft Failover Clusters (or MSCS). For example, a custom resource is of the Resource Type “Generic Application”. Figure 41 shows a custom resource named “test” in “Group 4” as displayed from the Microsoft Cluster Administrator application.

![Cluster Administrator - [CLUS9493 (clus9493.APIAD.COM)]](image.png)

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Owner</th>
<th>Resource Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>test</td>
<td>Offline</td>
<td>API1194</td>
<td>Generic Application</td>
</tr>
</tbody>
</table>

**Figure 41**  Microsoft Cluster Administrator, Generic Application Resource Type

Configuring a custom resource
For Cluster Enabler to recognize a third-party resource, it must be added to cluster properties. Figure 42 displays the “CustomResourceTypes” as listed in the EMC Cluster Enabler cluster properties, which is viewable from the command line.

Figure 42  Cluster properties

If you would like to use another third-party resource (for example, Generic Application), you need to run the following command string from the command line:

```
cluster /priv
CustomResourceTypes="<?xml version="1.0"?>,"<CustomResTypeList>,
"<CustomResType>Volume Manager Disk Group</CustomResType>,
"<CustomResType>Generic Application</CustomResType>,
"</CustomResTypeList>:MULTISTR
```

Figure 43 displays the changed cluster properties with Generic Application added to CustomResourceTypes.
After you have configured your custom resource for MS failover clusters, you can use the CE manager Create Group Wizard to create a custom resource CE Group. “Using CE Manager to create a custom resource CE Group” on page 134 explains the process.
Using CE Manager to create a custom resource CE Group

Follow these steps to create a CE Group using custom resources for management with Cluster Enabler. The example uses Symmetrix devices but the procedure is the same for CLARiiON devices:

1. Open the CE Manager and select the Groups icon from the Navigation tree and select Action and Create Group from the menu bar. This begins the process of reading the storage configuration. After the storage has been read, the first page of the Create Group Wizard opens. The Create Group Wizard can also be launched using the Right-click or Action menu.

   **Note:** A mirror needs to be present on the array before attempting to create a group. Run the Storage Discover Wizard to detect a newly created mirror.

2. The Enter Group Name dialog box appears. Enter the exact same Group Name as displayed in the MS Cluster Administrator in the space provided and click Create. For this example, the Group Name is “Group 4”. Click Cancel to abort the operation and close the wizard.

3. The next wizard screen prompts you to select devices for inclusion in the new group. The wizard recognizes that this is a custom resource group and displays a warning that a custom resource is being configured.

   **Note:** A SYMAPI device group for Symmetrix or a consistency group for CLARiiON will be created by Cluster Enabler. The corresponding CE resource will also be created and the custom resource will be made dependent on the CE resource. Physical disk resources will not be created in the failover cluster by Cluster Enabler.

Select the appropriate devices from the list shown by clicking in the select boxes. For this example, select the device (device with mount point H) that should be included in the group with the custom resource (Group 4). Selected devices are identified by the checked box. Click Next. Figure 44 on page 135 shows the select devices page for adding devices.
Note: Selecting the RA Group will automatically select Async Group to show SRDF/Asynchronous devices.

4. The Select Group Policy screen appears. From the pull-down menu, select your desired policy for the group. You can select either the **Restrict Group Movement** or **Automatic Failover**. Once selected, click **Next**. Figure 45 on page 136 shows the select group policy for the devices in mount point H.

The **Restrict Group Movement** selection restricts the group from failing over to a peer node. In an SRDF or MirrorView link failure, this setting will only attempt to move disk laterally. If the link is up, this setting has no impact.

The **Automatic Failover** policy sets the group to automatically failover to another node in the event of a node or network failure.
5. The Summary page appears. Upon Group Created Successfully, click Finish to exit the wizard.

6. Cluster Enabler automatically begins refreshing the CE cluster. Upon completion of the refresh, you should see the group that you created listed under Groups. If you do not see the newly created group, select Action and Refresh from the menu bar. The Refresh action can also be accessed from the right-click or Action menus.

7. Open the Microsoft Cluster Administrator application and select Group 4. A resource named “EMC_Group 4” of resource type “EMC Cluster Enabler” is now visible in Group 4. Figure 46 on page 137 displays the new group in the Microsoft Cluster Administrator application.
Using CE Manager to edit a custom resource CE Group

If the composition of an underlying custom resource changes, you should make the same changes to the CE Group custom resource by adding or deleting devices from the group. Changes to a custom resource group can be made by using the CE Manager Modify Group Wizard. The following example adds devices to the custom resource CE Group in a Symmetrix array.

Follow these steps to add or remove devices from a custom resource CE Group using the Modify Group Wizard. This example uses Symmetrix devices but the procedure is the same for CLARiiON devices:

1. Select the Group icon in the navigation tree and select Action and Modify Group from the menu bar. This begins the process of reading the storage configuration. After the storage configuration has been read, the first page of the Modify Group Wizard opens. The Modify Group Wizard can also be launched using the Right-click or Action menus. In this example, Group 4 is selected.
2. From the Select Devices page, select the Action from the pull-down menu for either Add Devices or Delete Devices. Depending on your selection, a list of available devices that can be added or removed will display. Select the desired devices from the list shown by clicking in the select boxes. Selected devices are identified by the checked box. Click Next. Figure 47 shows the Select Devices page for adding devices to Group 4.

![Modify Group Wizard](image)

**Figure 47** Select devices, custom resource

3. The Validate Selection page appears, click Next to validate your selection or click Cancel to abort the action. The wizard recognizes that this is a custom resource group and displays a warning that a custom resource is being modified. Figure 48 on page 139 displays the Validate Selection page for Group 4.

---

**Note:** Only the storage group and the corresponding CE resource will be modified. No physical disk resources will be added to the failover cluster.
4. The Summary page appears. Upon Group Modified Successfully, click **Finish** to exit the wizard.

5. Cluster Enabler automatically begins refreshing the CE cluster. Upon completion of the refresh, you should see the updated group information reflecting the devices added or deleted. If you do not see the updated group information, select **Action** and **Refresh** from the menu bar. The Refresh action can also be accessed from the right-click or Action menus. **Figure 49 on page 140** displays a summary of the modified Group 4 from this example.
Figure 49  Summary of Group 4, custom resource

Note: The Deconfigure CE Group option removes the storage group definition and CE resource but does not change the Microsoft failover cluster physical disk resources.
This appendix describes how to manually install the Cluster Enabler Manager using the command line interface:

- Manual Installation upgrade using CLI .................................................. 142
Manual Installation upgrade using CLI

In certain scenarios, where scripting is employed for complex configurations, the install tasks may be performed using the command line interface (CLI). This method should only be performed by experienced system administrators who are familiar with the Windows Installer.

In most cases, installations and upgrades should be performed using the InstallShield Wizard as described in Chapter 3. Read the “Before you begin” section for installation requirements and considerations.

Command line notes

The following install command line notes are for installation, repair, upgrade, and un-install.

Run misexec.exe /? to see all available options. Logging is optional, but in general use this parameter:

/l*v "%TEMP%\CE_operation.txt".

Install
To install using the command line, enter:

msiexec.exe /i "<path_to_media>\EMC Cluster Enabler.msi" /l*v "%TEMP%\CE_install.txt"

Note: The installation requires a reboot.

Repair
To repair using the command line, enter:

msiexec.exe /fomus "<path_to_media>\EMC Cluster Enabler.msi" /l*v "%TEMP%\CE_repair.txt"

or

msiexec.exe /fomus <product_code_guid> /l*v "%TEMP%\CE_repair.txt"

Note: Use the later option if the media is not available and no files are missing or corrupted.
**Note:** Both options will stop all CE services, the cluster service, and require a reboot.

---

**Uninstall**

To uninstall using the command line, enter:

```shell
msiexec.exe /x <product_code_guid> /l*v "%TEMP%\CE_uninstall.txt"
```

or

```shell
msiexec.exe /x "<path_to_media>\EMC Cluster Enabler.msi" /l*v "%TEMP%\CE_uninstall.txt"
```

**Note:** Both options will stop all CE services, the cluster service, and require a reboot.

---

**Product code GUIDs**

The product code GUIDs are provided in case the original media is unavailable. The product code GUID as specified in the commands above different for each architecture that CE supports.

**Note:** Each configuration and platform that CE supports has a different product code GUID.

*Table 10* presents the current product code GUIDs for SRDF/CE v3.0.

<table>
<thead>
<tr>
<th>Architecture</th>
<th>GUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>x86</td>
<td>583985F9-6D23-463D-B114-DB7DB3007152</td>
</tr>
<tr>
<td>x64</td>
<td>7EB43387-84C6-4F75-AE71-8169C8A452BB</td>
</tr>
<tr>
<td>IA64</td>
<td>B5AFCE8B-6B40-49C8-AB71-E01E97CDF9BA</td>
</tr>
</tbody>
</table>
This glossary contains terms related to the EMC Cluster Enabler software.

**A**

**active state** The state in which a MirrorView/S remote mirror is running normally. See also remote mirror states.

**agent** An installed program designed to control a particular resource type. Each type of resource supported in a cluster is associated with an agent.

**Application Program Interface (API)** A language and message format used by an application program to communicate with another program that provides services for it. APIs are usually implemented by writing function calls. Examples of APIs are the calls made by an application program to such programs as an operating system, messaging system, or database management system.

See also SYMAPI, CLARAPI

**asynchronous mode** See “SRDF Asynchronous (SRDF/A)”.

**attention state** The MirrorView/S mirror’s secondary image is fractured, and the mirror is configured to generate an alert in this case. The mirror continues to accept server I/O in this state.
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auto recovery</strong></td>
<td>A MirrorView/S option to have synchronization start as soon as a system-fractured secondary image is determined to be reachable.</td>
</tr>
<tr>
<td><strong>availability</strong></td>
<td>The ability to continue to provide a service even during hardware or software failure.</td>
</tr>
<tr>
<td><strong>BCV device</strong></td>
<td>A Symmetrix business continuance volume (BCV) that functions as a mirrored media to a standard device for a protected storage environment.</td>
</tr>
<tr>
<td><strong>BCV mirror</strong></td>
<td>A Symmetrix BCV device upon establishing or reestablishing a BCV pair.</td>
</tr>
<tr>
<td><strong>BCV pair</strong></td>
<td>A standard Symmetrix device and a BCV device that provide a protected storage environment.</td>
</tr>
<tr>
<td><strong>business continuance</strong></td>
<td>An SRDF function that ensures business applications continue running despite possible disk failures.</td>
</tr>
<tr>
<td><strong>cache</strong></td>
<td>Random access electronic storage used to retain frequently used data between the CPU and either a hard disk or slower RAM. It speeds up general data flow because a cache can be accessed quickly.</td>
</tr>
<tr>
<td><strong>channel director</strong></td>
<td>The component in the Symmetrix array that interfaces between the host channels and data storage. It transfers data between the channel and cache.</td>
</tr>
<tr>
<td><strong>CLARAPI</strong></td>
<td>CLARiiON Application Program Interface. See Application Program Interface (API).</td>
</tr>
<tr>
<td><strong>client</strong></td>
<td>A computer using services or resources provided by a remote machine, called a server. Often, communications software will have a separate version for the client or guest, and the server or host.</td>
</tr>
<tr>
<td></td>
<td>Clients create a TCP/IP session with a service in the cluster using a known IP address. This address appears to the cluster software as a resource in the same group as the application providing the service.</td>
</tr>
<tr>
<td></td>
<td>In a failure, the Cluster Service will move the entire group to another system.</td>
</tr>
</tbody>
</table>
client failover The response of a client machine after resource failure on the server for the client caused a resource failover. A client will detect a failure in the session and reconnect in exactly the same manner as the original connection. The IP address is now available on another machine and the connection is quickly reestablished. In this simple case, all information related to the original session not committed to disk is lost. This provides higher availability, but no fault tolerance for the service. Applications can use transactions to guarantee the client request is committed to the server database to gain fault-tolerant semantics.

class A group of two or more independent computers addressed and used as a single system.

cluster aware software Software that provides a restart mechanism invoked whenever the application resource is moved to another node in the cluster.

cluster Service The collection of software on each node that manages all cluster-specific activity.

consistency group A set of MirrorView/S logical units that are synchronously mirrored in a way that allows a recoverable copy in the event of a disaster.

consistency group condition Displays more detailed information about the MirrorView/S consistency group, including whether the group is active, inactive, admin fractured, system fractured, waiting on admin, or invalid.

consistency group state Indicates the current state of the MirrorView/S consistency group: synchronized, consistent, synchronizing, out-of-sync, scrambled, empty, incomplete, or local only.

consistent state (of image) State in which a MirrorView/S secondary image is identical to either the current primary image or to some previous instance of the primary image.

create mirror To establish a remote mirror, that is, use the remote mirror software to create data structures on one or more LUNs on specific storage systems, such that one is the primary image and the other is a secondary image.
D

data center migrations
An SRDF or MirrorView function that reduces application outage to minutes instead of hours.

dependency
The requirement of one resource needing another resource to function properly. The Cluster Enabler resource becomes a dependency for physical disk resources in the cluster. Therefore, any operations performed on the disk resource cannot be completed until the Cluster Enabler resource has been invoked.

device
A uniquely addressable part of the Symmetrix array consisting of a set of access arms, the associated disk surfaces, and the electronic circuitry required to locate, read and write data.

device group
A grouping of several devices established to provide configuration, status, and performance data on the collective devices within the group.

director
The component in the Symmetrix array that allows the Symmetrix array to transfer data between the host channels and disk devices.

See also channel director and disk director.

disaster recovery
An SRDF or MirrorView function that recovers data at the disaster recovery site in minutes rather than days.

discover
A discover action performed in the Cluster Enabler Configuration Wizard scans the storage array connected to the current node and gathers device information.

disk director
The component in the Symmetrix array that interfaces between cache and the disk devices.

E

establish
A BCV process that assigns a BCV device as the next available mirror of a standard device.

established
The BCV pair condition where the BCV device and standard device are synchronized and functioning as a Symmetrix mirror. A BCV pair is established by the BCV commands establish, reestablish, restore, or incremental restore.
failback  The action of moving a resource back to the cluster member designated to be the resource’s preferred owner. By default, resources are owned by their preferred owners, so a failback would only occur if the resource moved from its preferred owner. This is likely the result of a failover.

failover  The process of taking one or more resources offline on one cluster member and bringing them online on another cluster member.

fault-tolerant  Continuous operation in case of failure. A fault-tolerant system can be created using two or more computers that duplicate all processing, or having one system stand by if the other fails. It can also be built with redundant processors, control units, and peripherals. Fault-tolerant operation requires backup power in a power failure. It may also imply duplication of systems in disparate locations in the event of natural catastrophe or vandalism.

FDDI  An acronym for Fiber Distributed Data Interface.

fibre Channel  A high-speed serial interface capable of data transfer rates of up to 400 MB/s.

fibre Channel Director  The Fibre Channel adapter (FA) in the Symmetrix subsystem that interfaces between the host Fibre Channel interface and data storage. It transfers data between the channel and cache.

fracture  A condition in which I/O is not mirrored to the MirrorView/S secondary image and can be caused when you initiate the fracture (Admin Fracture) or when the system determines that the secondary image is unreachable (System Fracture). An admin fracture may also occur if the MirrorView/S software detects an error condition that requires administrative intervention to correct.

fracture log  A bitmap, maintained in SP memory, that indicates which portions of the MirrorView/S primary image might differ from the secondary images. The fracture log is used to shorten the synchronization process after fractures. The bitmap is maintained in SP memory, so if the mirror is not configured to use the optional write intent log (which stores the data on disk), and the SP that controls the primary fails while the secondary image is fractured, the fracture log is lost, and full synchronization of the secondary image is required.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>forced failover</strong></td>
<td>An SRDF/CE feature allowing you to automatically keep a cluster up on a particular Symmetrix array or arrays in a total site disaster.</td>
</tr>
<tr>
<td><strong>forced quorum</strong></td>
<td>Software functionality allowing the cluster to be forced up in the event that total communication is lost between nodes and Microsoft failover cluster (or MSCS) wants to shut down the cluster to avoid a split-brain condition.</td>
</tr>
<tr>
<td></td>
<td>See also <em>split-brain condition.</em></td>
</tr>
<tr>
<td><strong>G</strong></td>
<td></td>
</tr>
<tr>
<td><strong>graphical user interface (GUI)</strong></td>
<td>A method that allows users to interact with the computer and its special applications based on graphics instead of text. GUIs use icons, pictures, and menus and use a mouse as well as a keyboard to accept input.</td>
</tr>
<tr>
<td><strong>group</strong></td>
<td>A collection of resources to be managed as a single unit. Usually, a group contains all elements needed to run a specific application and for client systems to connect to the service provided by the application. Groups allow an administrator to combine resources into larger logical units and manage them as a unit. Operations performed on a group affect all resources contained within that group.</td>
</tr>
<tr>
<td><strong>H</strong></td>
<td></td>
</tr>
<tr>
<td><strong>HBA</strong></td>
<td>See also <em>host bus adapter (HBA).</em></td>
</tr>
<tr>
<td><strong>heartbeat</strong></td>
<td>A polling communication mechanism used by the cluster processes to determine whether the other members of the cluster are alive and working or have failed. If the heartbeat is not functioning, a failover is initiated, and another node in the cluster will take over the services.</td>
</tr>
<tr>
<td><strong>high availability</strong></td>
<td>The characteristic of a computer system/computing environment that allows it to continue to provide applications and access to data if a single component or resource fails. Service is interrupted for only a brief time, and may or may not be apparent to the end users.</td>
</tr>
<tr>
<td><strong>host bus adapter (HBA)</strong></td>
<td>A device circuit board that provides an interface between the SCSI bus and the computer I/O bus (for example, PCI, EISA, microchannel).</td>
</tr>
<tr>
<td><strong>Term</strong></td>
<td><strong>Definition</strong></td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td>hyper-volume</td>
<td>The term used by the Symmetrix array to make a physical disk appear as multiple physical disks. Each hypervolume has its own unique SCSI address.</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/output.</td>
</tr>
<tr>
<td>identifier (ID)</td>
<td>A sequence of bits or characters that identifies a program, device, controller, or system.</td>
</tr>
<tr>
<td>image condition</td>
<td>The condition of a MirrorView/S secondary image provides additional information about the status of updates for the image. Values include normal, administratively fractured, system fractured, queued to be synchronized, synchronizing, or waiting-on-admin.</td>
</tr>
<tr>
<td>image state</td>
<td>Indication of the relationship between a MirrorView/S secondary image and the primary image of a mirror. The image states are: synchronized, consistent, synchronizing, and out-of-sync.</td>
</tr>
<tr>
<td>incremental establish</td>
<td>A TimeFinder BCV or SRDF control operation. For BCV control operations, an incremental establish causes the BCV device to be incrementally synchronized and functioning as a Symmetrix mirrored device. (The devices must have been previously paired.) This is the same as an establish operation except an incremental establish is much faster: It copies only the differences or new storage data from the standard device to the BCV device. Any changed tracks on the BCV device are overwritten by the data on the corresponding tracks from the standard device. For SRDF control operations, an incremental establish causes the target (R2) device to be incrementally synchronized and established as a Symmetrix mirrored device. (The devices must have been previously paired.) This is the same as an establish operation except that an incremental establish is much faster: It copies only the differences or new storage data from the source (R1) device to the target (R2) device. Any changed tracks on the device are overwritten by the data on the corresponding tracks from the source (R1) device.</td>
</tr>
<tr>
<td>incremental restore</td>
<td>A TimeFinder BCV or SRDF control operation. In BCV control operations, an incremental restore is a control operation that reassigns a BCV device as the next available mirror of the standard device in the pair. However, the standard devices are</td>
</tr>
</tbody>
</table>
updated with only the data written to the BCV device during the time of the original pair split. The data written to the standard device during the split is overwritten with data from the BCV mirror.

In SRDF control operations, an *incremental restore* is a control operation that reassigns a target (R2) device as the next available mirror of the source (R1) device in the pair. The source (R1) devices are updated with only the data written to the target (R2) device during the time of the original pair split. The data written to the source (R1) device during the split is overwritten with data from the target (R2) mirror.

**L**

**lateral node** Nodes connected to the same Symmetrix or CLARiiON array.

**M**

**Majority Node Set (MNS)** A quorum-capable resource based on replicating data to local disks associated with a majority of cluster nodes. MNS enables you to create a server cluster without shared disk for the quorum resource. Cluster Enabler allows you to configure an MNS cluster on Windows Server 2003 Enterprise and Datacenter Editions.

**Microsoft Management Console (MMC)** A Microsoft user interface (UI) framework for use in administrating different components of the Microsoft Windows operating platform. This framework is used to host specific UI/control extensions called *snap-ins*. Use snap-ins to administer both local and remote computers. Third-party snap-ins can be written for use with MMC.

**mirrored pair** A device comprising two hypervolumes with all data recorded twice—once on each disk drive.

**mirroring** Symmetrix mirroring — A device comprising two hypervolumes with all data recorded twice—once on each disk drive. The Symmetrix array maintains two or more identical copies of a set of data on separate disks. Each copy automatically updates during a write operation. If one disk device fails, the Symmetrix array automatically uses one of the other copies from another disk drive.

MirrorView/S mirroring — A feature that provides disaster recovery by maintaining one or more mirrors of LUNs on other storage systems. MirrorView/S can work in conjunction with, but is independent of, the other major CLARiiON software options such as PowerPath software and SnapView software. MirrorView/S works
with LUNs in SAN storage systems, and thus can be used to mirror one or more LUNs that may compose a SAN storage group.

<table>
<thead>
<tr>
<th><strong>Glossary</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MMC</strong></td>
<td>See “Microsoft Management Console (MMC)”</td>
</tr>
<tr>
<td><strong>network interface card (NIC)</strong></td>
<td>A device that provides network communication capabilities to and from a computer system.</td>
</tr>
<tr>
<td><strong>nodes</strong></td>
<td>Members of a cluster. Also referred to as systems. A node contains a CPU, disk, and network resource.</td>
</tr>
<tr>
<td><strong>offline</strong></td>
<td>The state of a resource or group that classifies it as unavailable. When used in context with a cluster member, offline implies the cluster member may not be booted, or the cluster service on the node in question may not be functioning properly.</td>
</tr>
<tr>
<td><strong>online</strong></td>
<td>The state of a resource or group that classifies it as available. When used in context with a cluster member, online implies the other cluster members are receiving heartbeats from the cluster member in question. See also resource.</td>
</tr>
<tr>
<td><strong>out-of-sync state</strong></td>
<td>In MirrorView, a remote mirror state in which the software does not know how the primary and secondary images differ; therefore, a full synchronization is required to make the secondary images usable for recovery. Also see image state.</td>
</tr>
<tr>
<td><strong>peer node</strong></td>
<td>Nodes connected to different Symmetrix or CLARiiON arrays located across the SRDF link from each other.</td>
</tr>
<tr>
<td><strong>primary image</strong></td>
<td>The LUN on the MirrorView/S production storage system that contains user data and is the source for data copied to the secondary image. For MirrorView/CE there is one primary image and one secondary image. A remote mirror is ineffective for recovery unless it</td>
</tr>
</tbody>
</table>
has at least one secondary image. This manual also refers to primary image as primary or primary mirror image.

**promote (to primary)** The operation by which the administrator changes a MirrorView/S image’s role from secondary to primary. As part of this operation, the previous primary image becomes a secondary image. If the previous primary image is unavailable when you promote the secondary image (perhaps because the primary site suffered a disaster), the software does not include it as a secondary image in the new mirror. A secondary image can be promoted if it is in either the synchronized state or the consistent state. An image cannot be promoted if it is out-of-sync or synchronizing.

**Q**

**query** A command reporting the state of all the BCV devices in the system, as well as the status of SRDF states.

**quiesce threshold** The time period after which, without I/O from the server, any MirrorView/S secondary image in the consistent state and not fractured is marked as being in the synchronized state (the default is 60 seconds).

**quorum disk** An ordinary disk volume used as a special communication mechanism between server systems. In a Microsoft failover cluster (or MSCS), a small amount of cluster system data (a few megabytes) is stored on this volume. The SCSI-3 Reserve and Reset commands are used to move quorum-disk ownership back and forth between nodes. If the heartbeat mechanism fails, the quorum disk is used for each node to verify whether the other node is still functioning. Because not all disk products implement these multihost SCSI-3 commands, not all disk products will work in a failover cluster environment. Thus, Microsoft is very rigorous in providing the Cluster/RAID category of tests to qualify disks (refer to Microsoft’s Hardware Compatibility List) capable of running with Microsoft failover cluster software.

**R**

**R1 device** See “source (R1) device”.

**R2 device** See “target (R2) device”.
| **RDF1/RDF2** | A type of SRDF device group. Only RDF devices can be assigned to an RDF group. An RDF1 group type contains source (R1) devices and an RDF2 group type contains target (R2) devices. |
| **RDF State** | The SRDF state information displayed in a column in the middle pane. The possible RDF states are the following: | |
| *Invalid* | — The device and link are in an unrecognized combination. | |
| *SyncInProg* | — Synchronizing in progress. | |
| *Synchronized* | — The source and target have identical data. | |
| *Split* | — The source is split from the target and the target is enabled. | |
| *Suspended* | — The link is suspended. | |
| *Failed Over* | — The target is write-enabled, the source is write-disabled and the link is suspended. | |
| *Partitioned* | — The communication link to the remote Symmetrix array is down and the device is write-enabled. | |
| *R1 Updated* | — The target is write-enabled, the source is write-disabled and the link is up. | |
| *R1 UpdInProg* | — The target is write-enabled, the source is write-disabled, the link is up, but there are invalid tracks between the target and the source. | |
| *Mixed* | — This state is only set for a SymDgShow() call when the RDF states of the devices in the group are different from each other, thereby making the RDF state of the group mixed. | |
| *N/A* | — Not applicable. | |
| *Consistent* | — R2 data is consistent. | |
| **RA** | Remote adapter. An RA provides the link connection and fiber optic protocol support between the local and remote Symmetrix arrays. The RA cable connection is ESCON fibre (ESCON protocol). | |
| **RAID** | Redundant array of independent disks. Data is stored on multiple magnetic or optical disk drives to increase output performance and storage capacities and to provide varying degrees of redundancy and fault tolerance. Instead of storing valuable data on a single hard disk that could fail at any time, RAID ensures a backup copy of all |
information always exists by spreading data among multiple hard disks.

**recovery policy**  
In MirrorView, the policy for recovering the secondary mirror image after a system fracture. If the recovery policy is set to Auto, then the secondary starts re-synchronizing as soon as the primary image determines that the secondary mirror image is once again accessible. If the policy is set to Manual, then an administrator must explicitly start a synchronization operation to recover the secondary mirror image.

**reestablish**  
A business continuance process that reassigns a BCV device as the next available mirror of the standard device with which it was previously paired. The BCV mirror is updated with the data written to the standard device during the period the BCV pair was split. The data written to the BCV device during the split is overwitten by data from the standard device.

**Remote Link Director (RLD)**  
RLDs create the data link paths between two data storage units. Each Symmetrix array requires a minimum of two, up to a maximum of eight RLDs, depending on the Symmetrix model in use. Each RLD manages two ESCON fibre link connections. Each RLD can perform a single I/O at a time to its paired RLD in the remote Symmetrix array.

RLDs have either an RA1 or RA2 designation. RA1s reside in the source Symmetrix array. RA2s reside in the target Symmetrix array. These RLDs can also be assigned to an RA group. Up to four RA groups can exist in an SRDF configuration.

See also RA.

**remote mirror**  
For Symmetrix, the remote mirror refers to a target (R2) device located in a remote Symmetrix array. When a source (R1) device is participating in SRDF operations with a target (R2) device, all writes to the R1 device are mirrored to a target (R2) device in a remote Symmetrix array.

For MirrorView, a remote mirror is the combination of a LUN on one storage system, called the primary image, and another LUN on a different storage system, called the secondary image. The software maintains the secondary image as an exact copy of the primary image at some (possibly previous) point in time. If the server and/or storage system at the primary site fails, you can promote the secondary image to take over the role of the primary, thus allowing continued access to your production data.
**remote mirroring**
A feature that provides the means for disaster recovery by maintaining one or more copies (images) of LUNs at separate locations.

**remote mirror states**
There are three types of MirrorView/S mirror states. The mirror states are active, inactive, and attention.

Active — The remote mirror is running normally.

Inactive — I/O is rejected. This can be a temporary state during some consistency group operations or a result of an error during a consistency group operation.

Attention — The state to alert you that the minimum number of images required is not currently met. A fracture or the removal of an image can cause this. The mirror will continue to accept I/O in this state.

**resource**
An object managed by the Cluster Service that sees all resources as identical opaque objects. Resources may include physical hardware devices such as disk drives and network cards, or logical items such as disk partitions, TCP/IP addresses, entire applications, and databases. A resource is said to be online on a node when it is providing its service on that specific node.

**resource failback**
The movement of resources back to their preferred location in the cluster. This is usually done under manual user control to avoid a situation where a resource is failed back, and then immediately fails over again because of an unresolved node problem. Microsoft failover cluster (or MSCS) also allows automatic failback and provides a timing window to try to avoid repeated failovers.

**resource failover**
The process where control of a resource moves to another node of a cluster. Failover can be initiated automatically or manually. When initiated automatically, the cluster management software detects a failure of server node hardware or an application. When manually initiated, the cluster administrator uses the Cluster Administrator software application.

**resource group**
A collection of resources to be managed as a single unit. Usually a group contains all elements needed to run a specific application, and for client systems to connect to the service provided by the application. Groups allow an administrator to combine resources into larger logical units and manage them together. Operations performed on a group affect all resources contained within that group.
**restore**

A TimeFinder BCV or SRDF control operation.

In BCV control operations, a restore copies a full BCV mirror back to the standard device in the pair and reassigns the BCV device as the next available mirror to the standard device.

In SRDF control operations, a restore copies the full target (R2) device back to the source (R1) device in the pair and reassigns the target (R2) device as the next available mirror to the source (R1) device.

See also *incremental restore*.

**RF**

A remote adapter that provides the link connection and fiber optic protocol support between the local and remote Symmetrix arrays. The RF cable connection is SCSI fibre (SCSI protocol). An RF differs from an RA only in the type of connection; an RA uses an ESCON fibre connection, and an RF uses a SCSI fibre connection.

See also RA.

**scalability**

The ability to add new components to a storage system as system load increases.

**SCSI**

Small Computer System Interface. SCSI is a high-speed parallel interface used to connect microcomputers to SCSI peripheral devices, such as disks, printers, and other computers and local area networks.

**secondary image**

For MirrorView, a LUN that contains a mirror of the primary image LUN.

**secondary image state**

The secondary image states are synchronized, consistent, synchronizing, and out-of-sync. They describe the data on the secondary storage system in relation to the data on the primary storage system.

**semisynchronous mode**

An SRDF mode of operation that provides an asynchronous mode of operation. Applications are notified an I/O (or I/O chain) is complete once the data is in the cache of the local RA1 Symmetrix array. Any new data is then written to cache in the remote RA2 Symmetrix array. The remote Symmetrix array acknowledges receipt of the data once it is secure in its cache. If source tracks are pending transfer to a target (R2) device, and a second write is attempted to the source (R1) device,
the Symmetrix array disconnects (non-immediate retry request), and waits for the pending track to transfer to the remote Symmetrix array.

**Snap-in**

See “Microsoft Management Console (MMC)”.

**Solutions Enabler**

Also known as SYMCLI, an application written using the Symmetrix Application Programming Interface (SYMAPI) that retrieves data from a Symmetrix array using special low-level SCSI commands. Solutions Enabler also uses the CLARiiON Application Programming Interface (CLARAPI) to retrieve data from a CLARiiON array.

Solutions Enabler allows you to run commands on the host to obtain configuration, status, and performance data from the Symmetrix or CLARiiON arrays attached to hosts that are running in an open systems environment.

SYMCLI SRDF and TimeFinder components allow you to perform control operations on RDF and BCV devices.

**Source (R1) Device**

A Symmetrix source (R1) device that is participating in SRDF operations with a target (R2) device. All writes to this device are mirrored to a target (R2) device in a remote Symmetrix array. An R1 device must be assigned to an RDF1 group type.

See also RDF1/RDF2.

**Source Unit**

In an SRDF configuration, it is the primary data storage subsystem. It initiates many of the SRDF synchronization activities. An SRDF configuration must have at least one source unit and one target unit.

See also target unit.

**Split**

A business continuance process that removes the BCV mirror from the existing BCV pair and assigns the BCV mirror back to its original device address. The BCV device then holds an instant copy of the data from the standard device.

**Split-brain Condition**

A total communication failure while both nodes remain operational. A split-brain condition is a potential cause of logical data corruption. For example, if both sides assume the other is dead and begin processing new transactions against their copy of the data, two separate and unreconcilable copies of the data can be created.

**SRDF**

Symmetrix Remote Data Facility. SRDF consists of the microcode and hardware required to support Symmetrix remote mirroring.
SRDF Asynchronous (SRDF/A)  A high-performance, extended-distance asynchronous replication using a delta set architecture for reduced bandwidth requirements and no host performance impact.

Asynchronous mode provides a point-in-time image on the target (R2) device only slightly behind the source (R1) device. SRDF/A session data is transferred to the remote Symmetrix system in delta sets, eliminating the redundancy of same-track changes being transferred over the link, reducing the required bandwidth. SRDF/A only needs enough bandwidth to support the average production workload versus peak workloads.

SRDF/A is intended for users who require no host application impact while maintaining a consistent, restartable image of their data on the R2 side at all times.

SRDF link  Fiber optic connections and channels between two Symmetrix arrays. A minimum of two to a maximum of eight links can exist between the two units.

SYMAPI  Symmetrix Application Program Interface. See "Application Program Interface (API)".

SYMCLI  See “establish”.

synchronize  For MirrorView, the process of updating each secondary image with changes from a primary image. There are several levels of synchronization: synchronization based on a fracture log, synchronization based on the optional write intent log, and full synchronization (a complete copy). Synchronization based on the fracture or write intent log requires copying only part of the primary image to the secondary images.

synchronized state  For SRDF, the state in which the data in the R1 device is identical to that of the R2 device.

For MirrorView, the state in which the data in the secondary image is identical to that in the primary. On the next write to the primary, the image state will change to consistent. Also see Secondary image states.

synchronizing state  For MirrorView, when a secondary image is in the process of synchronizing. The data in the secondary image is not usable for recovery until the synchronization operation completes. Thus, an
image in the synchronizing state cannot be promoted to the primary image. Also, see Secondary image states.

**synchronous mode**  
An SRDF mode of operation that ensures 100 percent synchronized mirroring between the two Symmetrix arrays. This is a synchronous mode of operation. Applications are notified that an I/O (or I/O chain) is complete when the RA2 Symmetrix array acknowledges that the data has been secured in cache.

**systems**  
See “nodes”.

**T**

**target (R2) device**  
A Symmetrix target (R2) device participating in SRDF operations with a source (R1) device. It resides in the remote, or target, Symmetrix array. It is paired with a source (R1) device in the local Symmetrix array and receives all write data from its mirrored pair. This device is not accessed by user applications during normal I/O operations. An R2 device must be assigned to an RDF2 group type. See also RDF1/RDF2.

**target unit**  
In an SRDF configuration, this subsystem maintains synchronization with the devices it is paired with in the source unit. It can serve as a source unit during disaster recovery. An SRDF configuration must have at least one source unit and one target unit. See also source unit.

**V**

**virtual servers**  
See “nodes”.

**W**

**write intent log (WIL)**  
For MirrorView, the WIL is a record of recent changes to the primary image. This record is stored in persistent memory on a private LUN reserved for the mirroring software. If the primary storage system fails (not catastrophically; that is, the WIL LUNs or the persistent mirror storage was lost), the optional write intent log can be used to quickly synchronize the secondary images when the primary storage system becomes available. This eliminates the need for full synchronization of the secondary images, which can be a lengthy process on very large LUNs.
workload migrations  In SRDF, similar to data center migrations; especially useful for minimizing outages during preventative maintenance of hardware or software.
A
Adding nodes 88
application
    software failure 53
asynchronous SRDF
    compatibility 33

B
behavior
    common with MSCS 52
    override 59
booting 42
Business continuance volumes (BCVs) 46

C
cabling 41
cluster
    architecture 46
    -aware software 48
    benefits 46
    concepts 45
    limitations 46
    modes of operation 46
    multiple SRDF/CE for MSCS 38
    pre-SRDF/CE considerations 41
Cluster Enabler installation 64
Cluster Enabler Manager GUI 82
clustering 41
Configuration Wizard 27
configurations
    basic SRDF 20
    custom resource 131

data protection 17
deconfigure a CE group 100
delay
    failback 28
delete a CE group 101
dynamic swap 34
failover
    due to application failure 45
    due to hardware failure 45
    manual 45
failure
    modes 57
    types 50
FastSwap 34
fault-tolerant system 46
hardware
    NIC 53
    SRDF/CE architecture 36
heartbeat
    link failure 52
host bus adapter
    failure 53
InstallShield Wizard 72
Index

L
LAN link failure 52
lateral node 28
link failure 54
local
    mirrors 38
logging capabilities 115

M
manual failover 45
mirroring 38
MirrorView/CE restore and recovery 127
MirrorView/Synchronous 22
modes of operation
    active/active 39
    active/passive 39
mount points 30
multiple
    remote adapters 35

O
offline
    data redundancy 46
override
    local 58
overview
    MSCS 43
    SRDF/CE and Cluster Behavior 49

P
peer node 28

Q
Quorum model support 28

R
R1/R2 swap 34
remote
    adapters 35
restore and recovery operations 119

S
site failure

modes 57
SRDF
    asynchronous
    compatibility 33
    coexistence 42
    swap 34
SRDF/A
    compatibility 33
SRDF/CE
    behavior 49
    behavior override 59
configuration with multiple RAs 35
Configuration Wizard 27
hardware architecture 36
response to complete site failure 57
SRDF swap 34
Symmetrix Remote Data Facility (SRDF) 20

U
uninstalling Cluster Enabler 79

V
Veritas volume 131

W
Windows Server 2008 26
Windows Server 2008 devices 70
Wizards 83
    Change Quorum Wizard 91
    Configuration Wizard 85
    Create Group Wizard 95
    Modify Group Wizard 99
    Recover CE Cluster Wizard 124
    Storage Discover Wizard 89
    Update Mirrored Pairs Wizard 90