

**EMC ResourcePak
Command Line Interface
for Windows**
Version 3.5.1

PRODUCT GUIDE
P/N 300-999-373
REV B09

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Copyright © 2000, 2001, 2002, 2003 EMC Corporation. All rights reserved.

Printed October, 2003

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Trademark Information

EMC², EMC, Symmetrix, AutoIS, Celerra, CLARiiON, CLARAlert, DG, E-Infostructure, HighRoad, Navisphere, PowerPath, ResourcePak, SnapView /IP, SRDF, VisualSAN, where information lives, WideSky, and The EMC Effect are registered trademarks and EMC Automated Networked Storage, EMC ControlCenter, EMC Developers Program, EMC Enterprise Storage, EMC Enterprise Storage Network, EMC OnCourse, EMC Proven, EMC Snap, Access Logix, AutoAdvice, Automated Resource Manager, AutoSwap, AVALONidm, C-Clip, CacheStorm, Celerra Replicator, Centera, CentraStar, CLARevent, Connectrix, CopyCross, CopyPoint, CrosStor, Direct Matrix, Direct Matrix Architecture, EDM, E-Lab, Enginuity, FarPoint, FLARE, GeoSpan, InfoMover, MirrorView, NetWin, OnAlert, OpenScale, Powerlink, PowerVolume, RepliCare, SafeLine, SAN Architect, SAN Copy, SAN Manager, SDMS, SnapSure, SnapView, StorageScope, SupportMate, SymmAPI, SymmEnabler, Symmetrix DMX, TimeFinder, Universal Data Tone, and VisualSRM, are trademarks of EMC Corporation. All other trademarks used herein are the property of their respective owners.

Preface	xiii
 Chapter 1 Product Overview	
WideSky SYMCLI and ResourcePak	1-2
Enterprise Storage for Windows	1-2
EMC ResourcePak	1-3
Requirements and Dependencies	1-5
 Chapter 2 Installation	
Before You Begin	2-2
Upgrade Methods	2-2
ResourcePak Installation.....	2-3
Starting the Installation.....	2-3
Installing the DRU	2-5
Installing the TEIM	2-7
 Chapter 3 Disk Management With Symmetrix Integration Utilities	
Introduction	3-2
Requirements.....	3-3
Volume Management Software	3-3
VxVM Dynamic Disk Groups With TimeFinder	3-4
SIU Features.....	3-4
Command Summary	3-6
Making Disks Visible to the System	3-7
Viewing Detailed Information About Disks	3-8
Defining Volume Sets and Disk Groups	3-9
Deporting VDGs	3-9

Importing VDGs	3-10
Manipulating Disk Signatures	3-11
Flushing Cache Buffers to Disk	3-13
Disk Mount Operations	3-14
Disk Unmount Operations	3-14
Open Handles on Drives	3-15
Exclusive Locks on Drives.....	3-16
Device Masking Operations.....	3-16
Creating a Backup for Dynamic Disks.....	3-19
Typical Storage Operations	3-20
Synchronizing the BCV.....	3-20
Restoring Dynamic Disks With TimeFinder	3-22

Chapter 4 TEIM Overview and Setup

Overview	4-2
Business Continuance Storage Environment	4-4
Long Duration Locks	4-8
Setting Up an Exchange Business Continuance System	4-9
Setting Up a Production Server for TEIM	4-10
Windows Installation Requirements	4-10
Configuring Volumes for the Server Database.....	4-10
Server Database Application Install Strategy.....	4-12
EMC WideSky Installation	4-14
Setting Up a Backup/Recovery Server Environment	4-15
Windows Operating System	4-15
Server Database Application Install Strategy.....	4-16
EMC WideSky Installation	4-17
Configuring TimeFinder Environment	4-17
Configuring Snap Environment	4-19
EMC ResourcePak Installation	4-20
Configuring Symmetrix Remote Data Facility	4-21
BCV Remote Mirroring.....	4-21
Standard Remote Mirroring.....	4-23
Setting Up a Production Exchange 5.5 Server	4-25
Configuring Disks for Exchange	4-25
Exchange Server Installation.....	4-26
WideSky Installation	4-29
Setting Up a Backup Exchange 5.5 Server.....	4-30
Creating SYMCLI TimeFinder Device Groups.....	4-30
Establishing BCVs	4-31
Exchange Server Installation.....	4-32
EMC ResourcePak Modules.....	4-33

Aligning Exchange I/O on Storage Track Boundaries	4-34
Dual-Boot for Single Mailbox Recoveries	4-38
Configuration Steps	4-38
Performing Daily Backups With TEIM	4-41
Single Mailbox Recovery Using BCVs	4-41

Chapter 5 Backup and Restore Operations With TEIM

Backup Execution Environments	5-2
Various Considerations for Device Configurations	5-3
Command Line Start Up	5-5
Backing Up Exchange 5.5 Servers	5-6
Backing Up Exchange 2000 Servers	5-8
Backing Up Exchange 2003 Servers	5-11
Backing Up Multiple Windows 2000/2003 Servers	5-14
Creating a Backup Command Initialization File	5-15
Creating a Services Initialization File	5-19
Restore Procedures	5-21
Exchange 5.5 Database Restore	5-21
Exchange 2000/2003 Database Restore of an Offline Split	5-21
Exchange 2000/2003 Single Mailbox Recovery From an Offline Split	5-21
Exchange 2000/2003 Hot Split Database Restore With Transaction Log Replay	5-21
Single Mailbox Recovery Using a Hot Split Database	5-29
Exchange 2000/2003 Database Restore From a Remote Site	5-31
Troubleshooting	5-34

Chapter 6 TSIM Overview and Setup

Overview	6-2
Requirements	6-3
Business Continuance Storage Environment	6-3
SQL Server Snapshots	6-5
Long Duration Locks	6-7
Concurrent BCVs	6-7
Setting Up an SQL Server Storage Environment	6-8
Setting Up the Production Server Storage With Local BCV	6-10
Setting Up the Production Server Storage With Concurrent BCV	6-12
Setting Up the Production Server Storage in SRDF	6-14

Setting Up the Standby Server Storage With Local BCV	6-15
Setting Up the Standby Server Storage (Remote BCV Side)....	6-17
Setting Up the Production Server Storage With Snap Devices	6-18
Configuring Windows Server Disks	6-20
Creating a Backup for Dynamic Disks With TimeFinder.	6-21

Chapter 7 SQL Server Backup and Restore Operations With TSIM

TSIM Execution Environments	7-2
Considerations and Guidelines	7-2
Event Logging and Error Files for Windows.....	7-3
TSIM Execution Sequence	7-4
Command Line Start Up	7-4
Backing Up a Database or Filegroup	7-5
Running TSIM Backup.....	7-5
Optional Selections.....	7-6
Restoring a Database or Filegroup	7-8
Running TSIM Restore.....	7-8
Optional Selections.....	7-9
Example	7-10
Backing Up Multiple Databases	7-12
Running TSIM Backup.....	7-13
Optional Selections.....	7-14
Restoring Multiple Databases	7-15
Running TSIM Restore.....	7-15
Optional Selections.....	7-16
Initializing Multiple Databases on Standby Host.....	7-16
Initializing Multiple Databases on BCV Host	7-16
Restoring a Database on a Production Clustered Host....	7-18
Disaster Recovery Strategy for Multiple Databases	7-19
SQL Backup and Restore Methods.....	7-22
Initializing and Updating the Standby Database	7-22
Initialize/Recovery of Backup Database on Local BCV ...	7-26
Initialize/Recovery of Backup Database on Virtual Snap	7-28
Database Filegroup Backup and Recovery	7-30

Appendix A ResourcePak Command Reference

SYMCLI Conventions	A-2
symntctl	A-3
ExBackup2	A-11
ExBackup2000	A-15
ExBackup2003	A-20
ExBackupCommander2	A-24

tsimsnap	A-28
tsimsnap2	A-33
Index	i-1

1-1	Windows Server Enterprise Storage System	1-2
4-1	Parallel Backups on Multiple Exchange Production Servers	4-3
4-2	Exchange Enterprise Storage Business Continuity System	4-5
4-3	SRDF and TEIM - BCV Mirroring	4-6
4-4	SRDF and TEIM - Standard Mirroring	4-7
4-5	Creating a Partition Without DiskPar	4-35
4-6	Creating a Partition With DiskPar	4-35
4-7	Creating a Partition With DiskPar on a Raw Device	4-37
4-8	An Example DNS Forest	4-40
5-1	TimeFinder Exchange Integration Module CLI Start Up	5-5
5-2	Sample Initialization File for Exchange 5.5	5-15
5-3	Sample Initialization File for Exchange 2000	5-16
5-4	Initialization File for a Clustered Exchange 5.5 Server	5-19
5-5	Initialization File for a Stand-Alone Exchange 5.5 Server	5-20
5-6	File Dump Sample for Log Required	5-26
5-7	Transaction Log Listing	5-27
5-8	Restoring Data From the R2	5-31
5-9	Restoring Data From the Remote BCV	5-33
6-1	SQL Enterprise Storage Business Continuity System	6-4
6-2	SQL Server Business Continuity Environment	6-8
7-1	Database Query: Logical and Physical Filename Pairs	7-11
7-2	Relocation File With Old Logical and New Physical Filenames	7-11
7-3	Updating Standby Database Using BCV Transaction Backup	7-24
7-4	Filegroup Backup Example Environment	7-32
7-5	Database Backup Schedule for Example Scenario 1	7-34
7-6	Database Backup Schedule for Example Scenario 2	7-37

1-1	Requirements for EMC ResourcePak Components	1-5
3-1	SIU Commands	3-6
5-1	TEIM Commands	5-2
5-2	TEIM Command Options	5-3
5-3	Local TimeFinder Operations Support	5-3
5-4	Standard Remote Mirroring Operations Support	5-3
5-5	BCV Remote Mirroring Operations Support	5-4
5-6	Troubleshooting an Exchange 2000 Server Operation	5-34
7-1	TSIM Commands	7-2
7-2	Filegroup Backup Example Environment	7-33

As part of its effort to continuously improve and enhance the performance and capabilities of the EMC product line, EMC periodically releases new versions of both the EMC Enginuity Operating Environment and EMC WideSky software. Therefore, some functions described in this guide may not be supported by all versions of Enginuity or WideSky software currently in use. For the most up-to-date information on product features, see your product release notes.

If an EMC WideSky feature does not function properly or does not function as described in this guide, please contact the EMC Customer Support Center for assistance. If you are an EMC Development Partner, refer to the EMC Powerlink web site.

Audience This manual provides both guide and reference information for command-line users and script programmers. The manual describes how to manage Symmetrix units that contain Microsoft Exchange databases and SQL Server databases using SYMCLI commands of the WideSky (formally Solutions Enabler) software. EMC disk management CLI commands integrate the Windows operating system (Disk Manager) with the SYMCLI features to collectively automate various storage enterprise management operations.

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

Chapter 1, *Product Overview*, provides an overview of the WideSky SYMCLI and the ResourcePak for Windows components.

Chapter 2, *Installation*, describes how to install the ResourcePak components.

Chapter 3, *Disk Management With Symmetrix Integration Utilities*, provides the disk management operations for your storage system that the Symmetrix Integration Utilities (SIU) can provide.

Chapter 4, *TEIM Overview and Setup*, provides an overview of the TimeFinder Exchange Integration Module (TEIM) and related software that manages Exchange production and backup servers. The chapter also describes the complete setup of an Exchange enterprise business continuance environment.

Chapter 5, *Backup and Restore Operations With TEIM*, describes how to perform backup and restore operations to a Windows Exchange server database using the TimeFinder Exchange Integration Module (TEIM) command line interface.

Chapter 6, *TSIM Overview and Setup*, provides a brief description of the EMC TimeFinder-SQL Server Integration Module (TSIM) and related software that manage the Microsoft SQL Server environment. The chapter also describes the complete setup of an SQL Server enterprise business continuance environment.

Chapter 7, *SQL Server Backup and Restore Operations With TSIM*, describes how to perform backup and restore operations to Microsoft SQL Server databases using the EMC TimeFinder-SQL Server Integration Module (TSIM) command line interface.

Appendix A, *ResourcePak Command Reference*, describes the syntax and parameters of the SYMCLI ResourcePak commands that support Windows disk management and backup operations in a TimeFinder or business continuance storage environment.

Related Documentation

Related documents include:

- ◆ *EMC ResourcePak Data Relocation Utility Product Guide*, P/N 300-000-081, EMC Corporation
- ◆ *WideSky Solutions Enabler Symmetrix Base Management CLI Product Guide*, P/N 300-000-874, EMC Corporation
- ◆ *WideSky Solutions Enabler Symmetrix TimeFinder CLI Product Guide*, P/N 300-000-876, EMC Corporation
- ◆ *WideSky Solutions Enabler Symmetrix SRDF CLI Product Guide*, P/N 300-000-877, EMC Corporation
- ◆ *Host Connectivity Guides*, EMC Corporation
- ◆ *EMC TimeFinder Integration for Microsoft Exchange 2000*, Engineering White Paper

- ◆ EMC TimeFinder Integration with Microsoft SQL Server 2000, Engineering White Paper
- ◆ Using Multiple BCVs with the TimeFinder Exchange Integration Module, Engineering White Paper, EMC Corporation

Conventions Used in this Manual

The following conventions are used in this manual:

In this manual, every use of the word Solutions Enabler or SYMCLI means WideSky Symmetrix CLI. The former Solutions Enabler product is now called WideSky Solutions Enabler.

In this manual, every occurrence of the words volume, disk, or drive, also means device.

Note: A note calls attention to any item of information that may be of special importance to the reader.



CAUTION

A caution contains information essential to avoid damage or degraded integrity to storage of your data. The caution might also apply to protection of your software or hardware.

Typographical Conventions

This manual uses the following type style conventions in this guide:

AVANT GARDE	Key-cap
bold text	Boldface text provides extra emphasis and emphasizes warnings, and specifies window names and menu items in text.
<i>italic text</i>	<i>Italic text and characters emphasizes new terms, identifies variables in a software syntax (non-literal notation), identifies unique word usage, and applies emphasis in examples and in references to book titles and sections.</i>
fixed space courier font	A fixed space font identifies files and path names, and is used in command line entries, displayed text, or program listings.

Syntax Conventions

The syntax conventions used in this guide are:

- ◆ [] = optional entry
- ◆ | = alternative parameter value

Where to Get Help

EMC software products are supported directly by the EMC Customer Support Center and the EMC Developers Program.

For WideSky Solutions Enabler products, you can contact technical support by calling the EMC Customer Support Center at one of the following numbers:

United States: (800) 782-4362 (SVC-4EMC)

Canada: (800) 543-4782 (543-4SVC)

Worldwide: (508) 497-7901

Follow the voice menu prompts to open a service call and select the applicable product support.

If you are a partner in the EMC Developers Program, refer to the EMC Powerlink Web site at:

<http://powerlink.emc.com>

Sales and Customer Service Contacts

For the list of EMC sales locations, please access the EMC home page at:

<http://www.emc.com/contact/>

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink Web site at:

<http://powerlink.emc.com>

Your Comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please e-mail us at **techpub_comments@emc.com** to let us know about your opinion or any errors concerning this manual.

Product Overview

This chapter provides an overview of the WideSky SYMCLI and the ResourcePak for Windows components.

- ◆ WideSky SYMCLI and ResourcePak 1-2
- ◆ Requirements and Dependencies 1-5

WideSky SYMCLI and ResourcePak

The WideSky™ Symmetrix® Command Line Interface (SYMCLI) is a specialized library or set of UNIX-formatted commands that can be invoked one at a time. The SYMCLI is used in single command line entries and scripts to map and perform control operations on devices and data objects toward the management of your storage complex. The ResourcePak® component extends the basic SYMCLI command set to include the commands that allow you to integrate the SYMCLI offerings with various Windows server database applications and streamline the management of their associated database objects.

Enterprise Storage for Windows

Figure 1-1 illustrates the major elements of a Symmetrix enterprise storage system for Windows Server applications. Symmetrix is an integrated cached disk array (ICDA) designed for online data storage. Host servers and Symmetrix communicate via SCSI or Fibre Channel interfaces.

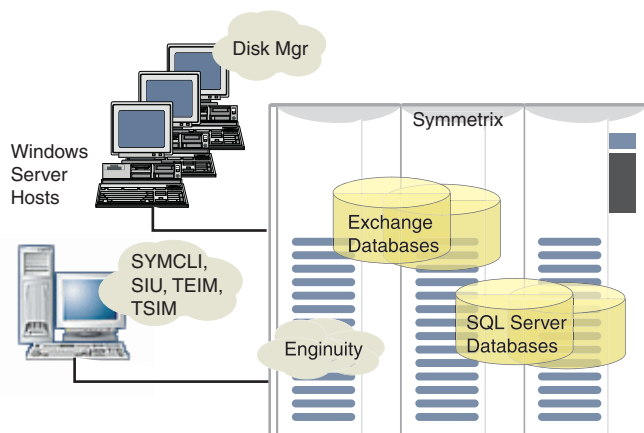


Figure 1-1 Windows Server Enterprise Storage System

For more detail information about the Symmetrix major components, see Chapter 1 of the *WideSky Solutions Enabler Symmetrix Base Management CLI Product Guide*.

EMC ResourcePak

EMC ResourcePak provides the following components:

- ◆ Data Relocation Utility (DRU)
- ◆ Symmetrix Integration Utilities (SIU)
- ◆ TimeFinder™ Exchange Integration Module (TEIM)
- ◆ TimeFinder SQL Server Integration Module (TSIM)

DRU The Data Relocation Utility (DRU) provides online data migration for high availability data centers. The DRU operates at the filter-driver level to manage and move Windows data from a source to a target volume with minimal disruption to the server or applications.

For more information on the DRU, refer to the *EMC ResourcePak Data Relocation Utility Product Guide*.

SIU The Symmetrix Integration Utilities (SIU) are disk management utilities for setting up and controlling a TimeFinder or SRDF business continuance configuration involving a Windows 2000 or Windows 2003 host. The SIU provides the disk management functions missing from the Windows operating system when working with TimeFinder and SRDF®.

For more information on the SIU, refer to *Disk Management With Symmetrix Integration Utilities* on page 3-1.

TEIM The TimeFinder Exchange Integration Module (TEIM) streamlines the collective TimeFinder actions required in backup operations of the storage enterprise for Exchange servers. The TEIM leverages EMC WideSky software (SYMCLI) and the Microsoft Win32 and Exchange backup application program interface (API) to coordinate the integration of EMC TimeFinder software and Microsoft Exchange Server.

Using the TimeFinder software, the TEIM produces exact copies of the production volumes that hold the Exchange Server information stores and logs. This enables Exchange administrators to perform both full and single-mailbox restores in a fraction of the usual time.

For more information on the TEIM, refer to *TEIM Overview and Setup* on page 4-1.

TSIM The TimeFinder-SQL Server Integration Module (TSIM) integrates and automates the features of EMC TimeFinder, the EMC WideSky (SYMCLI), and tools supplied with Microsoft SQL Server products.

The TSIM with SYMCLI provides a user interface that you can use to back up and restore databases, using both the Microsoft *Virtual Device Interface* (VDI) and the database *snapshot* functionality. The TSIM provides an integrated method for quickly creating point-in-time database copies that can be used for decision-support systems or database maintenance. The TSIM also provides a database backup that can be quickly restored in disaster scenarios.

The TSIM further enhances the availability of the database to mission-critical applications. It can greatly reduce backup and restore times and, in conjunction with typical database administration tasks, provide a more stable and available production platform.

For more information on the TSIM, refer to *TSIM Overview and Setup* on page 6-1.

Requirements and Dependencies

Table 1-1 lists the EMC software dependencies, their minimum requirements, and the license keys needed to run each of the ResourcePak components.

Table 1-1 Requirements for EMC ResourcePak Components

Component	WideSky Solutions Enabler Version	EMC License Keys	Requires the SIU Component	Execution Host	Comments
DRU	V5.2 minimum	1, 4	No	Any	
SIU	V5.2 minimum	1, 4	-	Production or BCV	
TEIM	V5.2 minimum	1, 2, 3, 4, 5	No ^a	BCV	WideSky Solutions Enabler must be installed on the production host and the BCV host. The SRDF key (2) is only required for SRDF configurations. The Snap key (5) is only required for Snap configurations.
TSIM	V5.2 minimum	1, 2, 3, 4, 5	No ^a	Production	WideSky Solutions Enabler must be installed on the production host. The SRDF key (2) is only required for SRDF configurations. The Snap key (5) is only required for Snap configurations.

a. However, for certain mount and dismount actions, during recovery procedures, the SIU is recommended.

License Keys

The EMC WideSky (or Solutions Enabler) license key numbers enable certain SYMCLI component areas as follows:

- 1 Base
- 2 SRDF
- 3 TimeFinder
- 4 ResourcePak
- 5 Snap

Windows Environment

The SIU, TEIM, and TSIM integration utilities only support Windows 2000 Server and Windows 2003 Server environments.

VxVM VERITAS Volume Manager (VxVM) version 2.7 (5.27) or higher is required when you have dynamic disks in a Windows 2000 or Windows 2003 environment.

Meta Volumes Noncontiguous meta volumes (including striped) require a Symmetrix Enginuity 5x66 or higher operating environment.

This chapter describes how to install the ResourcePak components.

- ◆ Before You Begin2-2
- ◆ ResourcePak Installation.....2-3

Before You Begin

Before you run the installation program, be sure to do the following:

- ❑ Choose an upgrade method (if applicable).
- ❑ Stop the SIU service and any running ResourcePak components.
- ❑ Review the requirements listed in Chapter 1 and in each of the component overview chapters of this guide.

For the DRU requirements, refer to the *EMC ResourcePak Data Relocation Utility Product Guide*.

Upgrade Methods

When upgrading ResourcePak for Windows, you have the following options:

- ◆ Uninstall the previous version of ResourcePak for Windows, then install the new version. This is the preferred method.
- ◆ Keep the previous version of ResourcePak for Windows and install the new version in a different path.

ResourcePak Installation

EMC ResourcePak for Windows is packaged on a single CD-ROM that contains executable files for the following ResourcePak components:

- ◆ Data Relocation Utility (DRU)
- ◆ Symmetrix Integration Utilities (SIU)
- ◆ TimeFinder Exchange Integration Module (TEIM)
- ◆ TimeFinder SQL Server Integration Module (TSIM)

You can install each component separately or choose to install any or all of the components in a multiple install session.

You must perform the installation as a Windows administrator so that the folders and files created by the installation have the correct permissions.

Starting the Installation

Perform the following steps to install ResourcePak for Windows:

1. Log on as host system administrator.
2. Insert the ResourcePak for Windows CD in the CD-ROM drive.

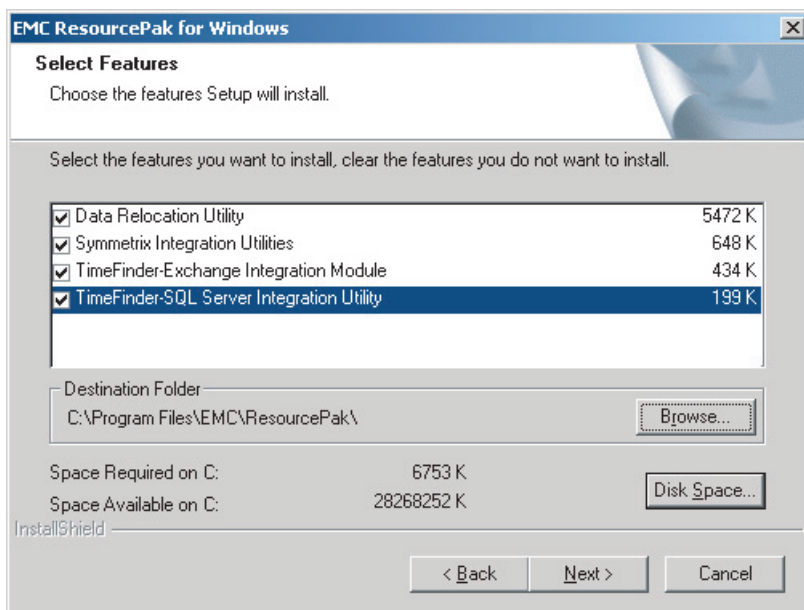
If autorun is enabled, the installation script starts automatically.

If autorun is not enabled, run <CD-ROM drive>:\setup.exe.

The **Welcome** dialog box opens.

3. Click **Next**.

The **Select Features** dialog box opens, allowing you to select the components to install.



4. Select the components to install and an installation directory.

Tip: The **Disk Space...** button allows you to check the available disk space.

5. Click **Next**.

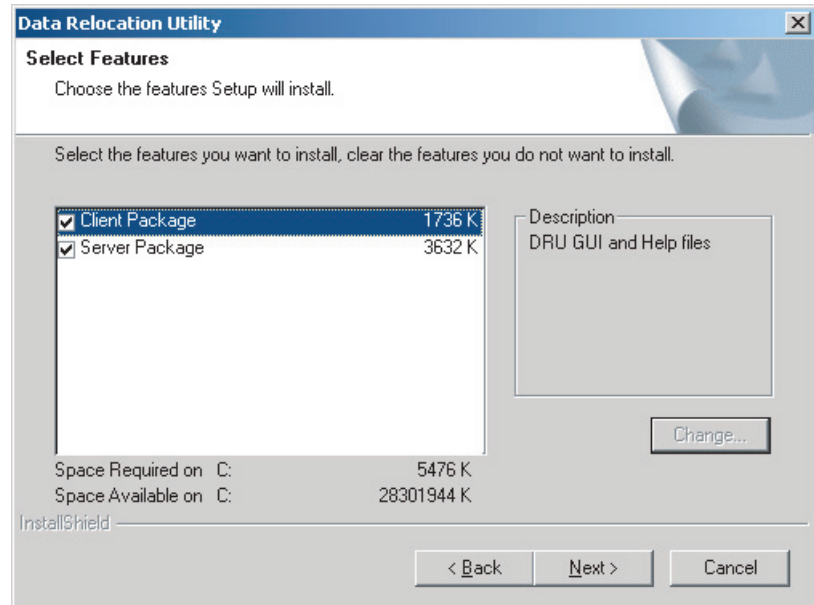
The setup programs for each selected component launch one at a time. Complete the following procedures according to the components you are installing:

- If you are installing the DRU, complete *Installing the DRU* on page 2-5.
- If you are installing the TEIM, complete *Installing the TEIM* on page 2-7.

The installation program for the SIU and the TSIM components do not require user input.

Installing the DRU

If you are installing the DRU, the **Select Features** dialog box opens, allowing you to select the software package(s) to install.



1. Select the software package(s), based on the following:
 - **Client Package** — installs the user interface elements and allows you to access a remote system to launch, monitor, and manage migrations on that system.
 - **Server Package** — installs the DRU Service, the filter driver, the volume expand utility, and associated DLLs. This package allows you to launch, monitor, and manage migrations on the local server and on remote servers, which have the DRU server software installed.

Installing both the client and server packages allows you to perform migrations on the local system and on a remote system, which has the DRU server software installed.

2. Click **Next**.

The **Set a password for the DRU MMC Snap-In** dialog box opens, prompting for a password to access the Microsoft Management Console (MMC). Once the installation is complete, you will need this password to access the console file and the DRU Snap-In from `mmc.exe`.

3. Type a password, and then click **Next**.

The **Select a log file path** dialog box opens, prompting for a directory to place the debug and migration log files.

You will NOT be able to change the directory path once the installation is complete.

4. Specify a directory, and then click **Next**.

If you are installing DRU in a Windows 2003 environment, a **Security Alert - Driver Installation** pop-up will appear, explaining that the DRU driver software has not been properly signed with Authenticode technology. Click **Yes** to continue installing the driver.

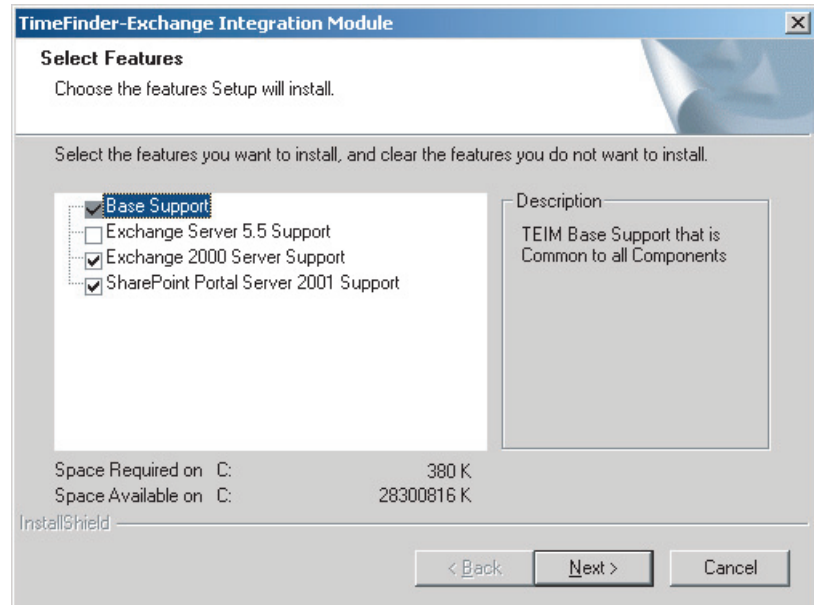
The DRU installation is complete.

5. Click **Finish**.
 - If you are only installing the DRU at this time, you may be asked to restart the computer. In which case, you should select **Yes, I want to restart my computer now**, and then click **Finish**.
 - If you are installing additional components, the setup program for the next component will launch. If this is the case, the installation program may prompt you to restart the computer once the entire installation is complete.

For more information on the DRU, refer to the *EMC ResourcePak Data Relocation Utility Product Guide*.

Installing the TEIM

If you are installing the TEIM, the **Select Features** dialog box opens, allowing you to select the level(s) of server support.



1. Select the appropriate support level(s).

Tip: Clicking on an option will display option specific information in the Description portion of the dialog box.

2. Click **Next**.

The TEIM installation is complete.

3. Click **Finish**.

Disk Management With Symmetrix Integration Utilities

This chapter describes the disk management operations for your storage system that the Symmetrix Integration Utilities (SIU) can provide for your Windows 2000 Server.

◆ Introduction	3-2
◆ Making Disks Visible to the System	3-7
◆ Viewing Detailed Information About Disks	3-8
◆ Defining Volume Sets and Disk Groups	3-9
◆ Manipulating Disk Signatures	3-11
◆ Flushing Cache Buffers to Disk	3-13
◆ Disk Mount Operations	3-14
◆ Creating a Backup for Dynamic Disks	3-19
◆ Typical Storage Operations	3-20

Introduction

The Symmetrix Integration Utilities (SIU) integrates and extends the, otherwise limited Windows 2000 and Windows 2003 disk management functionality to better operate with and on the EMC Symmetrix Business Continuity storage devices. TimeFinder and Symmetrix Remote Data Facilities (SRDF) are two main management components of the EMC Business Continuity offering. The SIU operations integrate with the management functionality of TimeFinder and SRDF with support specifically for:

- ◆ Windows 2000 Server, Advanced Server, and Datacenter Server
- ◆ Windows 2003 Server Standard Edition, Enterprise Edition, and Datacenter Edition

by extending their ability to:

- ◆ Mount and unmount hard disks and their associated file systems.
- ◆ Flush file system cache buffers to disk.
- ◆ Provide an automated method for importing and deporting volume set definitions.
- ◆ Write or erase signatures to a disk or group of disks.

The SIU is not a replacement for the Windows Logical Disk Manager (LDM), but bridges these lacking functionalities necessary for Windows users to optimally work with EMC business continuity storage devices.

For more information about the syntax of the SIU command, see Appendix A.

Note: In the text of this chapter, every occurrence of the word volume also means device or disk.

Requirements

The SIU software is based on the functionality and features of associated hardware and software in an EMC Enterprise Storage environment managed and used on Windows 2000 and Windows 2003 platforms.

Requirements for the SIU are:

- ◆ Symmetrix Enginuity environments of 5x66 and higher.

The Windows 2000/Windows 2003 host connection to the Symmetrix can be direct or through EMC Enterprise Storage Network™ (ESN), operating over a SCSI or Fibre Channel interface.

The SIU stand-alone software is designed to enhance and work with a Symmetrix system. However, a Symmetrix type storage array is not a specific prerequisite target for the operation of this software.

- ◆ A Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 Datacenter Server with SP2 or later, Windows 2003 Server Standard Edition, Windows 2003 Server Enterprise Edition, or Windows 2003 Server Datacenter Edition operating system.
- ◆ VERITAS Volume Manager (VxVM) version 2.7 (5.27) or greater when using dynamic disks. (Specifically to support the import and deport actions.)
- ◆ Most command actions require you to have administrative privileges.

Volume Management Software

VERITAS Volume Manager (VxVM) for Windows

Windows 2000/Windows 2003 Server have two types of disks: basic and dynamic. Basic disks support primary partitions only. Dynamic disks support FT-Volumes only. The Windows Logical Disk Manager (LDM) provides basic volume management and enables you to logically group disks under disk groups.

To manage dynamic disks, full SIU functionality requires you upgrade to VERITAS Volume Manager (VxVM) (formerly referred to as LDM-Pro). Most of the advanced capabilities of dynamic disks are only available with VxVM. VxVM is a storage management subsystem that enables you to manage physical disks as logical devices or *volumes*. A volume is a logical device that appears to data management systems as a physical disk partition device.

VxVM operates as a subsystem between Windows and data management systems, such as file systems and database management systems, such as Exchange and SQL Server.

VxVM Dynamic Disk Groups With TimeFinder

For Windows advanced server systems with dynamic disks, SIU functionality requires the support of VERITAS Volume Manager (VxVM). Specifically, the deport and import operations are dependent on the underlying support of VxVM.

If you are going to set up and use VxVM dynamic disk groups (VDGs) on a production server, you must comply with the following requirements when configuring VDGs for use with WideSky TimeFinder software:

- ◆ Create a TimeFinder device group for every dynamic disk group, maintaining the one-to-one basis. To keep this relationship clear, name the dynamic disk groups the same as the TimeFinder device groups.
- ◆ It is not necessary to create the disk group on the backup server, since the Logical Disk Manager (LDM) database is resident on every dynamic disk, as it is copied over to the backup server on each of the BCVs. All disk group definitions are stored in this database and will immediately appear on the backup server (in an offline state). You can create the TimeFinder device groups on either the production server or the backup server.
 - Do not mix STD and BCV devices in the same VDG.
 - Do not have Symmetrix and non-Symmetrix storage type devices in the same VDG.
 - Do not mix R1 and R2 devices in the same VDG.
 - Do not add gatekeeper devices to any VDG.

SIU Features

The SIU enables you to perform the following actions:

- ◆ Mount and unmount hard disks and their associated file systems.
- ◆ Manipulate drive letter assignments.
- ◆ View the actual physical configuration and the volume configuration data in the Windows operating system.
- ◆ Erase or write signatures (labels) to a disk or group of disks.
- ◆ Restore a disk signature changed by a TimeFinder or SRDF establish or restore operation.

- ◆ Import and deport VxVM type disk groups across Windows platforms.
- ◆ Flush any pending cached file system data to disk.
- ◆ Show any applications using a specified volume.
- ◆ Rescan and discover the disk configuration in view by the Windows host.
- ◆ Mask and unmask devices from and to the Window host.

Command Summary

The SIU CLI commands are a syntactical set and form of one command (`symmctl`), which has various arguments to support each of the main functional operations or actions. A summary of the SIU command set that operate in a Windows operating system environment is listed in Table 3-1.

These commands can be used in scripts when working with TimeFinder or SRDF operations on Windows 2000 platforms.

Table 3-1 SIU Commands

Command	Argument	Action
symmctl		Performs disk management operations for Windows platforms to properly work with business continuance devices. Possible operations are:
	mount	Mounts the specified disk to the specified mount point or drive letter.
	umount	Unmounts the specified disk from the specified mount point or drive letter.
	list	Views the actual physical disk configuration and the volume configuration data in the Windows operating system.
	openhandle	Displays any open sessions (applications/processes) working with a specified disk.
	Import	Imports dynamic disk groups to the Windows system.
	deport	Deports dynamic disk groups to the Windows system.
	signature	Manipulates the disk signature.
	flush	Flushes all pending unwritten file system cache entries to disk.
	rescan	Rescans and discover the disk configuration in view by the Windows host.
	locks	Controls the file system locks held on devices.
	mask	Uses device masking to remove the device from the host.
	unmask	Uses device masking to present the device to the host.

For detail information about the command syntax, refer to Appendix A and the remainder of this chapter.

Making Disks Visible to the System

After any dynamic disks are added to the Windows system, the new disks are initially not accessible. The SIU rescan action scans the drive connections and discovers any new disks available to the system, using the following form:

```
symmtctl rescan
```

The rescan command is useful after you perform a TimeFinder establish or split operation because when you do an establish or split, your devices become inaccessible. So, after you perform the establish or split operations, you can rescan the buses to discover all the devices to make them visible to the system again.

After you perform the rescan action, you can examine the results of the discovered disks, to ensure these disks are available to the system:

```
symmtctl list -physical
```

Viewing Detailed Information About Disks

In the Windows operating system, the SIU list action provides a consolidated view for displaying and managing the actual physical disk configuration and the volume configuration data.

To view disk numbers in your storage configuration, enter:

```
symntctl list -physical [-brief]
```

To view the volume configuration, enter:

```
symntctl list -volume [-brief]
```

In situations when you want a collapsed or an abbreviated output display for quick overall viewing, use the `-brief` option.

Also, you can target a specific disk:

```
symntctl list -pd diskN
```

where *N* is the disk number.

Or, you can target a specific volume:

```
symntctl list -vol VolName [-dg DgName] [-brief]
```

and optionally confine the volume list within a device group (*DgName*).

Defining Volume Sets and Disk Groups

The term *volume set* is used to describe multidisk volumes on a Windows 2000/2003 systems. In the context of SIU, a volume set is referred to as a VxVM disk group (VDG) when using dynamic disks. A VDG is made up of disk space that is linked together from multiple disks. You can dynamically extend the size of a spanned volume.

You can extend a simple or spanned volume only if the volume was created on a dynamic disk. You cannot extend a simple or spanned volume that was upgraded from basic to dynamic.

When you import any Windows NT volume set to Windows 2000/2003, you can upgrade the underlying disk to a dynamic disk or you can leave the disk in the basic disk format.

When using dynamic disks in the Windows system, all the information about the volumes is stored on the disk, including the system ID, device group ID, and so on. After the split, the BCVs have all the information from the standard Symmetrix volume (STD). It is therefore necessary to make the IDs local to the system to make them accessible.

Deporting VDGs

Using the SIU deport action, you can deport VxVM dynamic disk groups (VDGs). A *disk group* consists of volumes and disks that are logically grouped together in the VERITAS database.

To deport a certain disk group, use the following form:

```
symntctl deport -dg DgName
```

Deporting a disk group disables access to a disk group that is currently enabled (imported) by the system. You should deport a disk group if you want to move the disk members of a disk group to another system or if you want to use all of the disks remaining in a disk group for a new purpose.

The `deport` action removes information about the disk group you want to deport from the database, thereby making the disk group no longer accessible from VxVM until the `symntctl import` command is executed.

Importing VDGs

When using dynamic disks in Windows systems, you can import disks of a dynamic disk group from a remote system to the local host system. Importing a disk group enables host system access to members of a disk group. If you want to move a disk group from one system to another, first disable (deport) the disk group on the original system, and then move the disk members between systems and enable (import) the disk group.

To import a certain disk group, use the following form:

```
symmtctl import -dg DgName [-c]
```

This command will *not* function when the VxVM disk group is part of a cluster.

The option to clear the host ID (-c) should be used with VxVM V3.0 or later, when the disk group originated on a host other than where it is being imported. This is a common occurrence with TimeFinder when the standard volumes and BCVs are presented to two different hosts. The `import` command will fail in this scenario if the clear host ID is not used.

Manipulating Disk Signatures

In the Windows operating system, basic disks are identified by disk signatures (also known as labels).

Using a signature action, you can save a disk's signature, restore a disk's signature, erase a signature from disk, write or edit a signature to disk, or initialize a signature. All current disk signature assignments are saved in the EMC_TEMP_SIGNATURES registry key.

You specify the physical disk for a signature operation using the `-pd` option:

```
symntctl signature -pd diskN ...
```

where *N* is the physical disk number.

To view disk numbers in your storage configuration, enter:

```
symntctl list -physical
```

Note that you can set an environment variable to allow your Windows applications to get signatures, as opposed to SYMCLI getting the signatures from the Symmetrix. To have your Windows applications get the disk signatures, set SYMCLI_GET_SIGNATURE to a value of 1. The default is 0 for SYMCLI to get the signatures.

Saving

Using the `-save` option, the current disk signature is saved to the EMC_TEMP_SIGNATURE registry key so that it can later be restored through the `-restore` action. These companion actions enable you to restore a disk signature that may be changed by a TimeFinder (or SRDF) establish or restore operation.

Restoring

Using the `-restore` option, the previous disk signature that was saved in the EMC_TEMP_SIGNATURE key is restored (re-assigned to the disk).

Assigning Signatures

Using the `-sig` option, the signature of a disk is assigned/changed to any desired label specified in this command option.

Initialize Action

Using the `-initialize` option, the SIU service assigns signatures to any disks discovered without signatures.

Erase Action Using the `-erase` option, the signature of the specified disk is erased. This option is only used when setting up shared disks and TimeFinder configurations.

With Windows 2003, this option will erase the signature, only to have Windows immediately re-generate a new signature. Therefore, the volume will appear with a different signature, instead of an empty signature.

Flushing Cache Buffers to Disk

TimeFinder operations such as an on-the-fly BCV split require that the Windows file system cache buffers be flushed to disk. For this case, all pending unwritten file system data must be flushed to disk for a clean and complete split. The SIU flush action does this without removing the drive letter or volume association. This flush action is needed where the standard/BCV or SRDF R1/R2 pair is split without taking down an application.

You can target the standard or R1 device to flush with a drive letter or mount point:

```
symmtctl flush -drive DriveLetter  
symmtctl flush -path MountPnt
```

Or you can target the standard device to flush with a volume name or global ID (GUID):

```
symmtctl flush -vol VolName [-dg DgName]  
symmtctl flush -guid VolGuid
```

Because this command only flushes the Windows file system, applications that handle their own cache management (such as SQL Server or Exchange) are not affected. Flush or checkpoint mechanisms embedded in the application must flush its own application data. The application data must be flushed first, followed by a file system flush.

For example, to flush a volume with the volume GUID of Volume{ecba40b5-d522-11d5-98cb-00b0d0b03303}, enter:

```
symmtctl flush -guid Volume{ecba40b5-d522-11d5-98cb-00b0d0b03303}
```

Disk Mount Operations

After splitting BCV or SRDF volumes, you can reassign the drive letters for those volumes using the SIU mount action. The SIU mount action lets you mount hard disks and their associated file systems (a feature missing from Windows) in your storage environment.

The mount action mounts the specified volume name, GUID, or Symmetrix device to the specified drive letter or mount point:

```
symntctl mount -drive DriveLetter | -path MountPnt
               <-vol VolName [-dg DgName]> | -guid VolGuid |
               -sid SymId | -symdev SymDev | -part PartNum
```

The SIU provides a Windows service that performs the mount, unmount, and flush operations. This is done so that an exclusive *lock* can be acquired and set on a volume when it is dismounted. This lock is cached so that no other applications can access the volume while it is being unmounted, thus ensuring data integrity during TimeFinder establish and split operations.

When a `symntctl mount` command is performed, the SIU service performs the following tasks:

1. Locates the cached handle and lock to the volume being mounted.
2. Adds the drive letter or mount point assignment to that volume.
3. Releases the cached operating system lock if one is currently held.
4. Closes the handle to the volume.

Disk Unmount Operations

On the BCV or SRDF target (R2) side, establishing a BCV with its standard volume makes the BCV unavailable to the Windows system. The Windows system generates error messages if a mounted volume is referenced while unavailable.

The SIU unmount action provides the ability to unmount hard disks and their associated file systems (a feature missing from Window). The SIU unmount action also removes the drive letter from the specified disk volume.

You can target a drive letter or mount point:

```
symntctl umount -drive DriveLetter [-nolock]
symntctl umount -path MountPnt [-nolock]
```

Or you can target a volume or global ID:

```
symmtctl umount -vol VolName
symmtctl umount -guid VolGuid
```

This affects the current drive letter mapping. The command performs a file system flush as part of the dismount process, and the drive is latched with an exclusive lock until a subsequent mount (or forced release). This lock is set so that no other applications can access the volume while it is being unmounted, thus ensuring data integrity during TimeFinder establish and split operations.

If you wish to leave the drive unlocked after the dismount (umount) action, you can specify the `-nolock` option.

When an unmount operation is performed, the service performs the following tasks:

1. Gets a handle to the volume being unmounted from the operating system.
2. Obtains an exclusive lock on that volume from the operating system.
3. Flushes all pending file system cached data to disk for that volume.
4. Dismounts the volume by calling `DeviceIoControl()` with the `FSCTL_DISMOUNT_VOLUME` control code.
5. Deletes the specified drive letter or mount point. If the `umount` command was executed with the volume name or GUID, then all drive letter and mount point assignments are deleted.

Open Handles on Drives

Before performing an unmount or split action, you should determine if any other applications or processes are using, or have, an open handle on the target drive. The SIU open handle action enables you to determine whether there are processes accessing a volume you intend to unmount. This command should only be used for diagnostic and informational purposes to list processes using a drive.

You can target a drive letter or mount point:

```
symmtctl openhandle -drive DriveLetter
symmtctl openhandle -path MountPnt
```

Or you can target a volume or volume GUID:

```
symmtctl openhandle -vol VolName [-dg DgName]
symmtctl openhandle -guid VolGuid
```

Exclusive Locks on Drives

The SIU service caches exclusive locks on specified devices typically during an unmount operation.

In troubleshooting situations, or when a third-party application fails, you can release these locks using the following command:

```
symmtctl locks -releaseall
```

This command releases all locks currently being cached by the SIU service.

Note: When the SIU service is stopped or the system is rebooted, all SIU exclusive locks are released.

To release only a single exclusive lock being held for a particular volume, specify the volume's GUID in the following command:

```
symmtctl locks -release VolGuid
```

To view all of the exclusive locks currently held by the SIU, use the following command:

```
symmtctl locks -listall
```

For details about the SIU command syntax, see Appendix A.

Device Masking Operations

It is often necessary to add and remove access to a given Symmetrix device for the current host. This is known as device masking. Device masking typically requires several steps in order to make the device visible or hidden to the host, especially if multiple HBAs and PowerPath are being used. The SIU provides the ability to perform device masking operations with a single command by leveraging some of its internal functionality, like system rescan. When using the SIU to mask or unmask a device, the SIU does the following:

1. Obtains a list of all of the HBAs connected to the specified Symmetrix on the current host.
2. Determines the current state of the specified device on each of the HBAs (whether it is currently masked or unmasked).
3. Either adds or removes access to the specified device (depends on whether it is a mask or unmask operation) for each of the HBAs.

4. Performs a system rescan of the host so that the newly masked devices will be removed from the host, and the newly unmasked devices will appear on the host.

There is currently no way to control which HBAs should be involved in the mask/unmask operation. Currently, the SIU will perform the mask/unmask on all HBAs where the specified device is accessible. This is required in order to support PowerPath.

In order for SIU device masking to work correctly, Volume Logix must be configured on the Symmetrix where the device masking is going to take place. The following requirements exist:

- ◆ There must be a valid VCMDDB created on the Symmetrix unit.
- ◆ The VCMDDB must be mapped to all of the Fiber Adapters (FA) where the device masking is to take place.
- ◆ The VCM flag must be set on all of the FAs where the device masking is to take place.
- ◆ The Symmetrix device that is to be masked or unmasked must be mapped to all of the FAs where the device masking is to take place.
- ◆ The VCMDDB must be initialized and readable by the SIU.

SIU device masking does not perform any checking to determine if the Symmetrix device is currently accessible to other hosts on the SAN. It is the user's responsibility to prevent multiple hosts from using the same device (and potentially corrupting each other's data).

Device masking is very useful when attempting to break openhandles to a current volume. Currently, the SIU `umount` command will remove a drive letter from a volume even if there are processes with open handles to that volume, but these open handles will not be broken. In order to ensure the integrity of the data on the volume, these open handles need to be removed. By masking the device from the host, Windows will be forced to completely unload the IO stack for that device, thus removing all open handles. The device can then be unmasked and it will appear on the host without any open handles.

Using device masking to break the open handles to a volume may be necessary when using TimeFinder in particular environments. Currently, it is recommended that the BCV be unmounted, and subsequently locked, by the SIU before establishing it. In most cases,

this is sufficient to prevent the volume's cache from getting corrupted during the TimeFinder establish. However, if the host is running monitoring agents or anti-virus software that maintains open handles to the BCV, then the unmount and lock will not be enough. Instead, you must mask the BCV prior to the TimeFinder establish in order to remove the open handles. After the split operation, the BCV can be unmasked so that it is accessible to the host. This procedure is explained in *For Basic Disks With Open Handles*: on page 3-21.

Creating a Backup for Dynamic Disks

The following procedure describes the process for using both the SIU and TimeFinder to create a BCV of a dynamic disk. If the disk group on the backup server containing the BCVs is not online, skip steps 1 and 2.

1. Unmount any drive letters or reparse points currently assigned to the BCVs in the dynamic disk group on the backup server.

Do not use `mountvol` to perform this dismount.

2. Deport the dynamic disk group on the backup server. This step is only for precaution. In test, the dynamic disk groups are deported automatically once the TimeFinder establish is performed and the BCVs become Not Ready to the server.
3. Establish the TimeFinder device group.
4. Rescan the storage bus on the backup server. The dynamic disk group and all of its dynamic disks are listed as unreadable, and are therefore, offline.
5. Split the TimeFinder device group.
6. Rescan the storage bus on the backup server. The dynamic disk group and all of its dynamic disks are readable, but are still offline and foreign.
7. Import the dynamic disk group. Accept the default to keep the dynamic disk group name the same. The final result is that the dynamic disk group and all of its dynamic disks are online and usable.

This backup procedure is the same for all types of dynamic volumes.

Typical Storage Operations

The following are typical storage operations that use both SIU and TimeFinder commands to manage the storage environment.

Synchronizing the BCV

Using the `symmtctl` and the `symmir` commands, the following procedures for basic and dynamic disks work with `devgroup1` to synchronize the BCV device (drive *x*) with the standard on primary and secondary servers. For more information about the `symmir` command, refer to *EMC WideSky Solutions Enabler Symmetrix TimeFinder CLI Product Guide*.

For Basic Disks:

1. Unmount the volume on the secondary system:
`symmtctl umount -drive x:`
2. Establish the standard and BCV pair on the primary system:
`symmir -g devgroup1 est`
3. Verify that the device is synchronized on the primary system:
`symmir -g devgroup1 verify -synched`
4. Split the device on the primary system:
`symmir -g devgroup1 split`
5. Mount the volume on the secondary system:
`symmtctl mount -drive x: -vol volumex`

For Dynamic Disks:

1. Unmount the volume on the secondary system:
`symmtctl umount -drive x:`
2. Deport the dynamic disk group on the secondary system:
`symmtctl deport -dg devgroup1`
3. Perform an establish on the primary system:
`symmir -g devgroup1 est`

4. Rescan the storage bus on the backup server to assure that the disk has been dropped and will not be accessed by Windows Plug and Play:

```
symmtctl rescan
```

5. Perform a flush on the primary system:

```
symmtctl flush -drive x:
```

6. Verify that the device is synchronized on the primary system:

```
symmir -g devgroup1 verify -syncd
```

7. Split the device on the primary system:

```
symmir -g devgroup1 split
```

8. Perform a rescan on the secondary system:

```
symmtctl rescan
```

9. Perform an import of the disk group on the secondary system:

```
symmtctl import -dg devgroup1 -C
```

10. Mount the volume on the secondary system:

```
symmtctl mount -drive x: -vol volumex
```

For Basic Disks With Open Handles:

To ensure that cache corruption does not occur when a BCV has open handles, use the following procedure:

This procedure should be used for all TimeFinder operations if the BCV volume has openhandles (usually due to a monitoring agent or anti-virus software). To determine if a BCV has open handles, use the `symmtctl openhandle` command.

1. Unmount the volume on the secondary system:

```
Symmtctl umount -drive x:
```

2. Mask the volume on the secondary system:

```
Symmtctl mask -sid SymmId -symdev SymDev
```

3. Establish the standard and BCV pair on the primary system:

```
symmir -g devgroup1 est
```

4. Verify that the device is synchronized on the primary system:

```
symmir -g devgroup1 verify -synched
```

5. Split the device on the primary system:

```
symmir -g devgroup1 split
```

6. Unmask the volume on the secondary system:

```
Symntctl unmask -sid SymmId -symdev SymDev
```

7. Mount the volume on the secondary system:

```
Symntctl mount -drive x: -vol volumex
```

The above SIU mask and unmask commands (steps 2 and 6) can also be applied to the Dynamic disk procedure (*For Dynamic Disks*: on page 3-20) in order to perform TimeFinder operations on Dynamic Disks with openhandles.

Restoring Dynamic Disks With TimeFinder

The following procedure restores a BCV of a dynamic disk that uses both SIU and TimeFinder commands.

1. Unmount any drive letters or repare points currently assigned to the BCVs in the dynamic disk group on the backup server.

```
symntctl umount -drive x:
```

2. Deport the dynamic disk group on the backup server.

```
symntctl deport -dg DgName
```

3. Unmount any drive letters or repare points currently assigned to the standard devices in the dynamic disk group on the production server. This step is necessary to ensure that the standard device is not written to during the restore (since all writes are committed to the BCV). Do not use `mountvol` to perform this dismount.

```
symntctl umount -drive x:
```

4. Deport the dynamic disk group on the production server. Failure to perform this step may leave the dynamic disk group in an unrecoverable state on the production server.

```
symntctl deport -dg DgName
```

5. Restore the TimeFinder device group.

```
symmir -g DgName restore
```

6. Rescan the storage bus on the backup server. The dynamic disk group and all of its dynamic disks are listed as unreadable, and are therefore, offline.

```
symntctl rescan
```

7. Split the TimeFinder device group.

```
symmir -g DgName verify -synched  
symmir -g DgName split
```

8. Rescan the storage bus on the backup server. The dynamic disk group and all of its dynamic disks are readable, but are still offline and foreign.

```
symntctl rescan
```

9. Rescan the storage bus on the production server. The dynamic disk group and all of its dynamic disks are present, but offline and foreign on the production server.

```
symntctl rescan
```

10. Import the dynamic disk group on the backup server.

```
symntctl import -dg DgName
```

11. Import the dynamic disk group on the production server. The dynamic disk group and all of its dynamic disks are online and healthy.

```
symntctl import -dg DgName -C
```

12. Remount each of the volumes in the disk group on the production server. Use the LDM snap-in, SIU CLI, for this mount.

```
symntctl mount -drive x: -vol volumex
```


TEIM Overview and Setup

This chapter provides an overview of the TimeFinder Exchange Integration Module (TEIM) and related software that manage Exchange production and backup servers. The chapter also describes the complete setup of an Exchange enterprise business continuance environment.

- ◆ Overview 4-2
- ◆ Setting Up an Exchange Business Continuance System..... 4-9
- ◆ Setting Up a Production Server for TEIM 4-10
- ◆ Setting Up a Backup/Recovery Server Environment..... 4-15
- ◆ Configuring Symmetrix Remote Data Facility 4-21
- ◆ Setting Up a Production Exchange 5.5 Server 4-25
- ◆ Setting Up a Backup Exchange 5.5 Server 4-30
- ◆ Aligning Exchange I/O on Storage Track Boundaries 4-34
- ◆ Dual-Boot for Single Mailbox Recoveries..... 4-38

Overview

The TimeFinder Exchange Integration Module (TEIM) provides a comprehensive backup management interface specifically for Windows servers that support Microsoft Exchange databases residing in Symmetrix storage.

Using EMC storage technologies, the TEIM leverages EMC WideSky software and Microsoft Win32 and Exchange backup application program interfaces (APIs) to coordinate the integration of EMC Business Continuity and Microsoft's Exchange Server software.

Using the Business Continuity software, the TEIM produces exact copies of the production volumes that hold the Exchange server information stores and logs. This enables Exchange administrators to perform both full- and single-mailbox restores in a fraction of the usual time. EMC's TimeFinder and the Symmetrix Remote Data Facility (SRDF) are actually the two basic interface elements of the Business Continuity technology. In an SRDF configuration, the TEIM can create remote copies of the Exchange data to be used in case of site disasters. The term TimeFinder is sometimes used to mean the full scope of what the business continuity umbrella provides.

The TEIM can be used in an enterprise environment where there are multiple production Exchange servers for one backup server (Figure 4-1). In this type of environment, the TEIM is able to perform backups of all production servers in parallel. This greatly reduces the nightly backup window.

The TEIM backup interface targets different combinations and versions of Windows and Exchange Server releases. The TEIM interface supports the following environments:

- ◆ Windows 2000 Server with Exchange 2000
- ◆ Windows 2000 Server with Exchange 5.5
- ◆ Windows 2000 Server with Exchange 2003
- ◆ Windows 2003 Server with Exchange 2003

The TEIM supports the following Windows server types:

- ◆ Windows 2000 Server, Advanced Server, and Datacenter Server
- ◆ Windows Server 2003, Standard Edition, Enterprise Edition, and Datacenter Edition

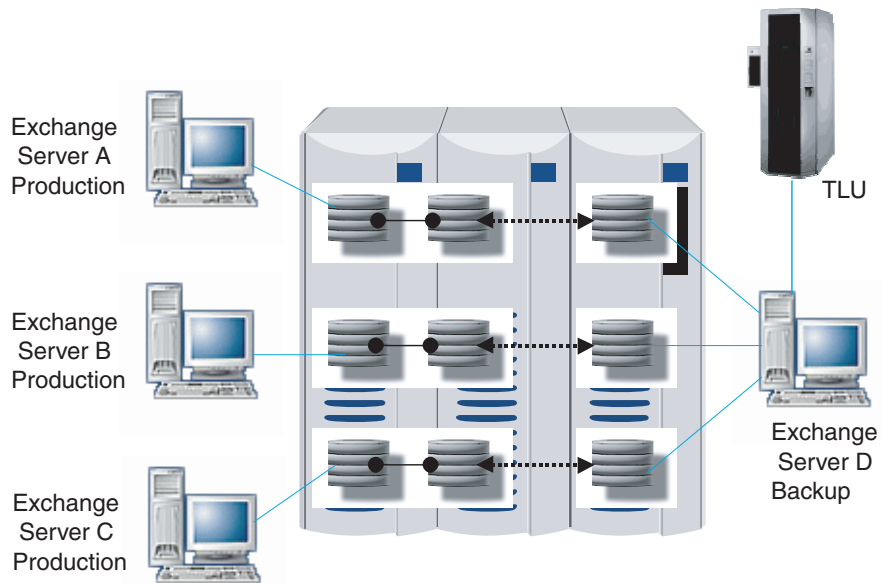


Figure 4-1 Parallel Backups on Multiple Exchange Production Servers

The TEIM requires the Symmetrix Engenuity version to be 5x65 or greater. To use the instant or hot split features, the Symmetrix Engenuity versions must be at least 5x66 or 5x67. Note that for 5x68 versions and greater, the instant split behavior is the default mode. EMC Snap requires Symmetrix Engenuity 5x69 or later.

Note: A user must have both local administrative rights for the server as well as Exchange administrative rights for the domain.

For more information about the syntax of the TEIM commands, see Appendix A.

Note: In the text of this chapter, every occurrence of the word volume also means device or disk.

Business Continuity Storage Environment

The Symmetrix business continuity storage environment for the Exchange database is based on the integration of the TEIM with TimeFinder and SRDF technologies.

EMC TimeFinder

EMC TimeFinder works by creating multiple, independently addressable online Business Continuity Volumes (BCVs) for information storage (Figure 4-2 on page 4-5). Each BCV is a Symmetrix device and is configured as a single mirror, which independently supports host applications.

BCVs, created as mirror images of active production volumes, give you another source of data with which to work. This is ideal for backup and recovery, as well as off-line operations such as defragmentation. The principal device, known as the *standard* device, remains online for regular Symmetrix operation so there is no interruption of service with the original production server.

Each BCV contains a unique host address making it accessible to a separate backup/recovery server.

A business continuity sequence first involves setting, or *establishing*, the BCV device as a mirror of a standard Symmetrix device, making the BCV device available for backup. The BCV device may later be separated, or *split*, from the standard Symmetrix device with which it was previously established. The split BCV device still has valid data, and is available for backup or other host processes through its original device address.

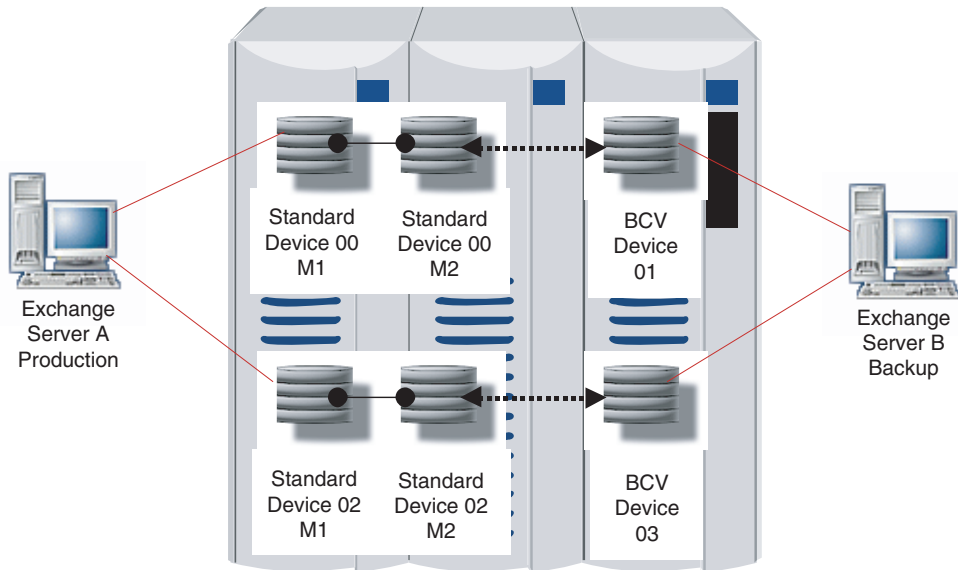


Figure 4-2 Exchange Enterprise Storage Business Continuance System

SRDF

Symmetrix Remote Data Facility (SRDF) provides a disaster tolerant business continuance environment. SRDF with TEIM allows for the recovery from local database corruption and local site disasters as well as restart capabilities from the remote site.

With the TEIM integrating your Exchange server with both TimeFinder and SRDF, you can recover from any disaster. You can also restart Exchange at the remote location in the event something happened to the production site.

The TEIM supports two configurations of SRDF: BCV mirroring and standard mirroring.

SRDF BCV Mirroring

The BCV mirroring configuration shown in Figure 4-3 consists of a standard volume and a local BCV-R1 volume. The remote R2 mirror mirrors the local BCV, and it also has a remote BCV (BRBCV) mirror. This configuration allows for local database recovery as well as remote disaster recovery. When the BCV-R1 and R2 are synchronized, the remote BCV exists to ensure that a valid, remote copy of your Exchange data is always available.

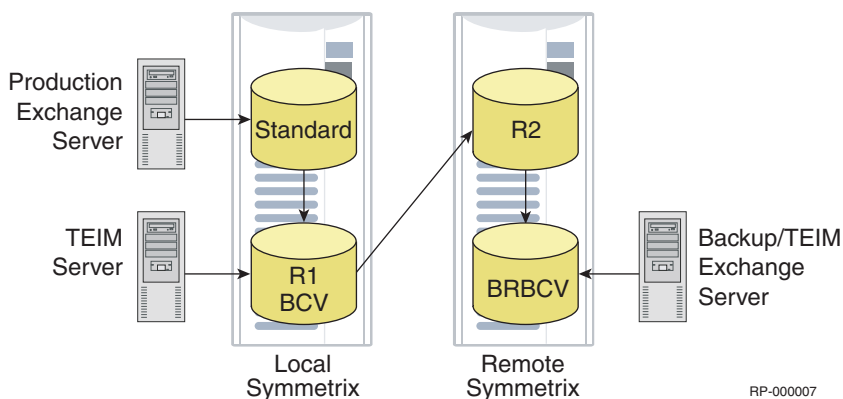


Figure 4-3 SRDF and TEIM - BCV Mirroring

With this BCV mirroring configuration, each mirror is incrementally established independently in sequence:

1. The BCV-R1 is established and split from the standard volume.
2. The R2 is established and split from the BCV-R1.
3. The remote BCV (BRBCV) is established and split from the primary R2 device.

SRDF Standard Mirroring

The standard mirroring configuration, shown in Figure 4-4, consists of a production R1 standard device that is mirrored by a remote R2 device. Also, the remote R2 device has a remote BCV (RBCV). This configuration provides remote database and site disaster recoverability, but does not provide any local recoverability. This configuration is ideal for environments that require the remote site disaster recoverability, but do not have enough storage available to implement the previous example. The obvious disadvantage to this configuration is that database restores, necessitated by corruption or other failures, must be performed over the SRDF link, which will be slower than the local database restores using EMC TimeFinder.

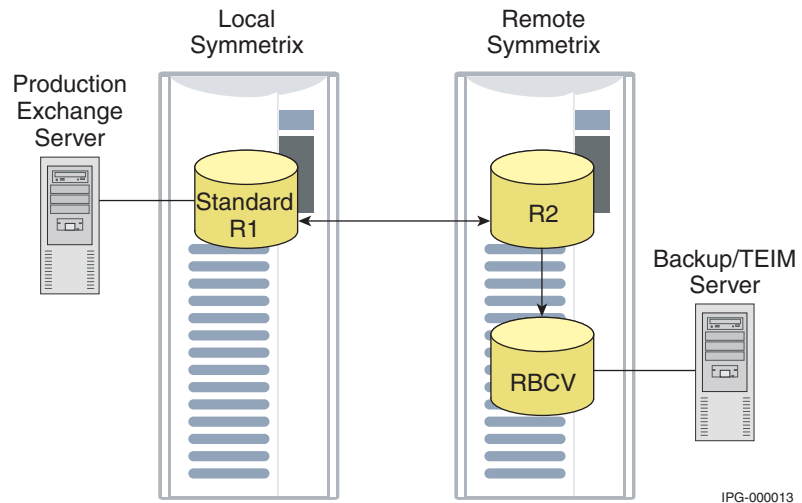


Figure 4-4 SRDF and TEIM - Standard Mirroring

With this standard mirroring configuration, there are two possible modes of operation:

- ◆ Keep the SRDF link synchronously established R2 with R1. In this case, the TEIM will establish and split the RBCV.
- ◆ Keep the SRDF link split. In this case, the TEIM will first establish and split the SRDF link, transferring data from R1 to R2. The TEIM will establish and split the RBCV.

EMC Snap

EMC Snap allows you to create virtual copy sessions between a source device and multiple *virtual* (VDEV) target devices. The source device can be either a standard device or a BCV device. The target device(s) must be virtual device(s).

EMC Snap is useful in situations where multiple copies of production data are needed for testing, backups or report generation. It can also be used to reduce disk contention and improve data access speed, by assigning users to copies of data rather than accessing the one production copy.

EMC Snap functionality is controlled via copy sessions, which pair the source and target devices. Sessions are maintained on the Symmetrix unit and can be queried to verify the current state of the devices. A copy session must first be created and then activated for the target virtual devices to become accessible to its host. When the information is no longer needed, the session can be terminated.

Long Duration Locks

To protect TEIM target devices from being used by other applications, the TEIM has the ability to use WideSky long duration locks. Once a device is locked, it is not available to other applications, unless they get the lock ID from the TEIM. The TEIM will lock the BCVs or VDEVs, but not standard volumes.

To use the long duration locks, use the `-lock` option. To list the locks held by the TEIM, use `-lock list`. To release a lock, use `-lock release` or `-lock releaseall`.

Once the TEIM locks a device, any manual operation to establish/split/restore TimeFinder or virtual snap devices should use `-preservetgtlock -lockid LockID`.

If the devices are already locked, and the user wants the TEIM to use a specific lock holder ID for a specific Symmetrix, use `-lock -lockid LockID -sid SymID`.

When using long duration locks with SRDF, the TEIM will always lock only the last BCV in the process. For example, if the configuration is `R1>R2>RBCV`, then the TEIM will lock the RBCV. If the configuration is `STD>R1>BCV>R2>BRBCV`, then the TEIM will lock the BRBCV. If the `-srdf` option is not used here, then the TEIM will lock the R1-BCV.

Setting Up an Exchange Business Continuance System

The following sections describe how to setup an Exchange enterprise storage business continuance system, involving the various production and backup servers. The environment setup includes certain setup requirements for the volume configurations, plus the Windows operating systems, Exchange Server software, and the EMC WideSky software in the server system. The proper operation of the WideSky TEIM backup interface is dependent on the resulting configuration.

The setup process is presented in the following sections:

- ◆ Setting Up a Production Server for TEIM 4-10
- ◆ Setting Up a Backup/Recovery Server Environment 4-15
- ◆ Setting Up a Production Exchange 5.5 Server 4-25
- ◆ Setting Up a Backup Exchange 5.5 Server..... 4-30

Setting Up a Production Server for TEIM

This section outlines the setup procedure for the production server environment to properly integrate with the TEIM and the Solutions Enabler. The production server environment for the TEIM is for Exchange 2000 and SharePoint Portal Servers that require Windows 2000 software and the EMC WideSky Solutions Enabler.

For Exchange 5.5 environments, see *Setting Up a Production Exchange 5.5 Server* on page 4-25.

Windows Installation Requirements

For a proper Windows 2000 setup, the network environment must be in place on the network prior to the installation of the operating system on this server. Specifically, a forest, domain, and DNS server must exist (it can be on the same host as the domain controller). Additional information about creating a Windows forest and active directory can be found on the Microsoft web site.

For clustered systems, the Microsoft Cluster Service (MSCS) must be installed as an additional Windows component.

Configuring Volumes for the Server Database

If the Windows environment is correct, the host should be able to see Symmetrix devices. At this point, the logical volume layout should be considered. When creating the partitions on these volumes, it is recommended to assign appropriate volume labels to ease your future management tasks. Primarily, this will help to distinguish log volumes from Information Store volumes.

Dynamic Disks

The initial setup of the dynamic disks on a server determines the outcome of using EMC TimeFinder for backup and recovery of dynamic disks. It is important to keep dynamic disk groups and TimeFinder device groups on a one-to-one basis. For every dynamic disk group, create a TimeFinder device group, and vice versa. It may also be helpful to name the dynamic disk groups the same as the TimeFinder device groups. This helps keep the one-to-one relationship clear.

It is not necessary to create the disk group on the backup server. Because the LDM database is resident on every dynamic disk, it is copied to the backup server on each of the BCVs. All disk group definitions are stored in this database and immediately appear on the backup server (in an offline state). You can create the TimeFinder device groups on either the production server or the backup server.

Before you begin volume configuration, you should establish a plan for the layout of the database volumes. It is recommended to refer to the EMC white paper, *Exchange 2000 Best Practices on EMC Symmetrix*, when designing this plan. The white paper can be downloaded from <http://powerlink.emc.com>.

Follow these requirements for the layout of volumes when using the TEIM:

1. All Exchange 2000 and SharePoint Portal data must be located on Symmetrix disks. This includes all mailbox and public databases, as well as their respective transaction logs. In the case of TEIM Hot Splits, the checkpoint files must be located on Symmetrix disks as well.
2. No two volumes, being used for Exchange or SharePoint data, can be located on the same physical disk. Failure to follow this rule will result in TEIM failures.
3. Exchange or SharePoint Information Store databases and transaction logs should be located on separate physical disks. This way, no single disk failure will result in a loss of both the databases and transaction logs.
4. No two Information Store databases from different storage groups can be located on the same physical disk. This step is necessary to insure that all databases get copied at the same time as their transaction logs.

It is recommended that all Information Store databases be located on separate physical disks. This allows for flexible restore and recovery of single Information Store databases.

All volumes should be formatted with NTFS file system. FAT and FAT32 are not supported.

Disk Alignment

You should always create your volumes with partitions that are aligned along the track boundaries of the underlying Symmetrix disk. This improves the performance for any application using those volumes, refer to *Aligning Exchange I/O on Storage Track Boundaries* on page 4-34.

Hot Split

When using the Hot Split feature of the TEIM, all Exchange or SharePoint volumes must have partitions that are aligned with the underlying disk's track boundaries. This insures that the Hot Split does not cause a torn page on the BCV.

Server Database Application Install Strategy

Exchange 2000

This section highlights the installation strategies for Exchange 2000 and SharePoint Portal Server software.

The Exchange 2000 installation program is very different from that of Exchange 5.5. Upon initial start of the install program, the default items (*Microsoft Exchange Messaging and Collaboration Services* and *Microsoft Exchange System Management Tools*) are already selected. This guide assumes a basic Exchange 2000 installation. Other technologies, such as Conference Server and instant messaging, are out-of-scope.

Continue with the default selections and choose where to place the Exchange 2000 binaries (a local disk is acceptable). If this server is the first Exchange 2000 server in the forest, then the administrator is asked to specify an organization name.

For additional information about the Exchange 2000 installation process, refer to *How to Set Up Exchange 2000* at:

<http://support.microsoft.com/support/kb/articles/q262/0/68.asp>

Exchange 2000 starts with a single storage group containing both a private and public Information Store. At this point, the administrator must implement the Exchange 2000 framework that has already been designed. When creating the storage groups and Information Stores, be sure to locate the necessary files (*edb.log*, *priv1.edb*, *priv1.stm*, and so on) on the appropriate volumes. This is where the volume labels help. All private and public Information Stores, as well as transaction logs, must be located in Symmetrix storage.

When using the Exchange 2000 Hot Split feature of the TEIM, it is required that the checkpoint file (*E00.chk*, *E01.chk*, and so on.) for each storage group be located on the same volume as one of the databases in that storage group.

TEIM support (with the hot split feature) requires Exchange 2000 Service Pack 2 or higher to be installed at this point.

Exchange 2003

The same rules apply to an Exchange 2003 production server that apply to an Exchange 2000 production server. All Exchange 2003 data files (including the *.chk* files) must be located on the Symmetrix.

SharePoint Portal Server

SharePoint Portal Server can be installed by accepting all of the defaults during the setup program. The SharePoint Portal Server setup program installs its own version of Exchange 2000 Server, so there is no need to manually install Exchange 2000 Server prior to SharePoint Portal Server install.

Once the SharePoint Portal Server setup program is complete, the underlying Exchange 2000 Server configuration is locked in place. The user cannot configure the number of storage groups or databases used by SharePoint Portal Server. In all cases, the SharePoint Portal Server will run with a single storage group, named the SharePoint Portal Server Group, and a single public information store, named the SharePoint Portal Server Store. The Exchange System Manager will not be available when the SharePoint Portal Server is installed.

Run the SharePoint Portal Server Administrator MMC available at **Start, Settings, Control Panel, Administrative Tools**.

Right-click on the SharePoint Portal Server entry, which is shown in the tree on the left, and select **Properties**. Click the **Data** tab on the dialog box and to show where all of the database and transaction logs to the appropriate Symmetrix devices are listed.

The checkpoint file must now be re-located to a Symmetrix device. This option is not available in the SharePoint Portal Server Administrator MMC, so the change must be made in the registry.

Run the registry editor and navigate to:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl  
Set\Services\MSExchangeIS\CfgData\Objects
```

In the Objects folder are additional folders that are named with GUIDs. These GUIDs vary for each installation, making it difficult to identify the folder you need. Search each folder (try the second one in the tree, first) looking for the Circular Logging registry key. Change the value of the Circular Logging registry key to 0, so that circular logging is disabled. Also change the Working Directory registry key to match the DB Log Path registry key, causing the checkpoint file to be located on the transaction log volume. These changes will not take effect until you restart the Microsoft Exchange Information Store service and the SharePoint Portal Server service.

For additional setup details, refer to the Microsoft KnowledgeBase article, Q323584—Hot Split Snapshot Backups of SharePoint Portal Servers at:

<http://support.microsoft.com/default.aspx?scid=kb;en-us:323584>

EMC WideSky Installation

In addition, this article outlines the support agreement that is in place between Microsoft and EMC for this product.

After the Microsoft software is properly installed and configured, EMC WideSky Solutions Enabler must be installed.

EMC WideSky Solutions Enabler, which can provide the TimeFinder and SRDF components is also required. Refer to the *WideSky Solutions Enabler Installation Guide*, and verify that the software with the Base, TimeFinder, and SYMAPI server licenses are enabled. If not, enable the Base, TimeFinder, and SYMAPI server licenses using `symlmf`.

When prompted by the WideSky install program, select **Yes** to install the SYMAPI server and run `symapisrv start`. This service is necessary for the TEIM to connect and interface to the SYMAPI server from the backup recovery server.

If you have an SRDF environment, the SRDF license is also required. These licenses should be purchased from EMC prior to beginning this setup.

After WideSky is installed, run `symcfg discover` to populate the host's SYMAPI database with the appropriate disk information.

Setting Up a Backup/Recovery Server Environment

This section describes the setup of a TEIM backup/recovery server environment to support either the Exchange 2000, Exchange 2003, or SharePoint Portal Server databases. This setup involves certain install strategies and requirements for the following software: Windows operating system; Exchange 2000 Server, Exchange 2003, or SharePoint Portal Server; and the EMC WideSky Solutions Enabler.

For Exchange 5.5 environments, see *Setting Up a Backup Exchange 5.5 Server* on page 4-30.

It is acceptable to install the standard edition of Exchange 2000 on the backup server rather than the Enterprise edition.

If you are using the Exchange 2000/2003 backup server and BCVs for Exchange 2000/2003 single mailbox recoveries, a special dual-boot configuration must be implemented. Follow the steps outlined below to implement this configuration. Single item recoveries are not possible with SharePoint Portal Server.

Windows Operating System

The Windows operating system installation on the backup/recovery server is similar to that of the production server with one difference. The disks presented to the backup/recovery server are BCVs, and do not need to be configured. The disks will copy their data from the standard disks attached to the production server. Note that the backup/recovery server does not need the MSCS installed, even if the production server is clustered.

To perform single-mailbox recoveries from this backup/recovery server, it is necessary to set up a separate Windows forest and domain tree. The simplest way to accomplish this is to make the backup/recovery server the domain controller for its own forest and domain. Refer to the *Windows 2000 Step-by-Step Guides* deployment Web site at the following URL to help set up the forest and its active directory:

<http://www.microsoft.com/windows2000/library/planning/walkthroughs/default.asp>

It is important to realize that single mailbox recoveries will not be as prevalent in Exchange 2000/2003 due to the default 30 day, mailbox retention feature. With this feature enabled, any mailbox that is deleted will actually stay resident in the Information Store for another 30 days. Typically, the need to recover these deleted

mailboxes is realized within the first few days. Therefore 30 days is ample time to eliminate the need for configuring your backup/recovery server for single-mailbox recoveries.

If dynamic disks are used, the VERITAS Volume Manager for Windows 2000/2003 needs to be installed.

Server Database Application Install Strategy

Exchange 2000

This section highlights the installation strategies for Exchange 2000 and SharePoint Portal Server software.

The Exchange 2000 installation is almost identical to that of the production server. You should create the same storage groups and databases that exist on the production server, and locate them on the appropriate BCVs.

At this point, stop all Exchange 2000 services and set them to manual. The Exchange 2000 services do not need to run on the backup/recovery server until a single mailbox recovery is necessary.

TEIM support (with the hot split feature) requires Exchange 2000 Service Pack 2 or higher to be installed at this point.

Exchange 2003

When installing an Exchange 2003 backup server, follow the same guidelines as stated above for Exchange 2000.

SharePoint Portal Server

SharePoint Portal Server must be installed on the backup/recovery server in order to gain access to necessary utilities and COM objects. A single point-in-time recovery is not possible with SharePoint Portal Server, so it is necessary to configure SharePoint Portal Server on the backup/recovery server. Once SharePoint Portal is installed, stop both the SharePoint Portal service and the Microsoft Exchange Information Store service, and set them both to start manually.

Note: A single backup/recovery server cannot be used to backup both Exchange 2000 Servers and SharePoint Portal Servers. Both applications are required for their respective backups, and Microsoft has a restriction that the two cannot be installed on the same host.

EMC WideSky Installation

The EMC WideSky installation on the backup/recovery server is similar to that of the production server, except it is not necessary to install and run the `symapisrv` service on the backup/recovery server.

The Base and TimeFinder licenses must be installed. If you have an SRDF environment, the SRDF license is also required. These licenses should be purchased from EMC prior to beginning this setup.

After WideSky is installed and the licenses have been established, run a `symcfg discover` SYMCLI command to populate the host's SYMAPI database with the appropriate disk information.

Configuring TimeFinder Environment

When using the Symmetrix Remote Data Facility, refer to *Configuring Symmetrix Remote Data Facility* on page 4-21 for set up instructions.

With the proper Symmetrix configuration in place for your TimeFinder Exchange environment, you should now have a BCV on the backup/recovery server for every standard device that is being used for Exchange 2000 or SharePoint Portal storage. If this is not the case, then revise the Symmetrix configuration.

To provide the initial BCV to standard device association, you must create device groups on the backup/recovery server. The actual device group arrangement is completely up to you, as long as each standard device and BCV that is being used by Exchange or SharePoint Portal is included. Although the TEIM does not use these device groups directly, they can be very helpful to you during restore scenarios. For this reason, please use care when designing the device groups.

1. Create a device group using the following:

```
symdbg create DgName
```

2. After all of the device groups have been created, add the standard devices to the appropriate device groups with the following:

```
symld -g DgName add dev SymDevName
```

3. Associate all of the BCVs to the device groups with the following:

```
symbcv -g DgName associate dev SymDevName
```

4. To verify that the device group contains all of the devices that it should, run:

```
symdbg show DgName
```

5. All of the standard devices and BCVs should be listed in the order that they were added. To establish the devices in this order, the first standard device with the first BCV, use the following:

```
symmir -g DgName establish -full -exact
```

This performs a full establish on the devices, which can take a very long time depending on the size of the devices. Make sure you remove any mount points from the BCVs on the backup/recovery server before attempting the establish. To determine the current state of the establish command, enter:

```
symmir -g DgName query
```

6. Once this command shows that all of the device pairs are synchronized, run the following command to split all of the devices in the device group:

```
symmir -g DgName split
```

At this point, the BCVs connected to the backup/recovery server should have the identical volume label as its paired standard device.

Any BCVs that are dynamic disks are most likely offline after the split. Use the VxVM to bring these disks back online.

Multiple BCVs

The TEIM supports the use of multiple BCVs in a rotating fashion (using the `-multi` option). To configure this, associate and establish each BCV with its particular standard volume by repeating steps 3 through 6, as described above. The TEIM will only use multiple BCVs if each BCV has been fully established with the standard volume.

Because of a restriction imposed by the Windows operating system, you cannot use multiple BCVs with dynamic disks.

Furthermore, verify that all BCVs which are currently paired to a given standard device are visible on the backup server. If this is not the case, and `-multi` is used, the TEIM will fail at some point because it will try to use that BCV, but it will not find it on the backup server.

To remove an unused BCV pairing, use the following:

```
symmir -g DgName cancel LdevName dev SymDevName
```

Configuring Snap Environment

To use the TEIM and EMC Snap to snapshot your Exchange data, it is necessary to have a separate VDEV for every standard device that is currently storing Exchange data. This data includes all databases and logs.

The configuration of EMC Snap for the TEIM is very similar to that for EMC TimeFinder. The biggest difference is that device groups are required in order to make the TEIM work with EMC Snap. The reason for this is because EMC Snap does not maintain a constant pairing of standard to VDEV, the way that EMC TimeFinder does for standard to BCV. Because of this, the TEIM relies on the device group to understand which VDEVs should be used for the backup.

The only requirement with regard to device groups is that every standard that is being snapshotted must be in a device group with an available VDEV. All standards and VDEVs do not need to be in the same device group. It is acceptable to have several device groups, as long as each standard device has an available VDEV in its device group. A VDEV is considered available when:

- ◆ It is the same size as the standard device.
- ◆ The VDEV is not currently involved in a Snap session. This means that the VDEV can not be in the Created or Activated states.

During the backup with EMC Snap, the TEIM will use the next available VDEV in the device group. It will not always use the same VDEV. Furthermore, the TEIM will allow multiple Snap sessions per standard device if a multitude of VDEVs exist in the device group. This means that it is possible to run the TEIM with EMC Snap and then run it again without terminating the first Snap sessions. This is the default behavior for the TEIM with EMC Snap, so the `-multi` option is not needed in this case.

1. Create a device group with the following:

```
symdg create DgName
```

2. Add the standard devices to the device group with the following:

```
symld -g DgName add dev SymDevName
```

3. Add the VDEVs to the device group with the following:

```
symld -g DgName add dev SymDevName
```

Notice that you do not associate VDEVs to the device group, you add them. This means that a device group can contain both BCVs and VDEVs, and can be used for both TimeFinder and Snap.

4. Verify that the device group contains all of the devices that it should with the following:

```
symdg show DgName
```

5. View the current Snap sessions that are active for this device group with the following:

```
symsnap -g DgName query
```

To see multiple Snap sessions for a given standard device, use the following:

```
symsnap -g DgName query -multi
```

EMC ResourcePak Installation

The EMC ResourcePak for Windows CD contains the installation programs for all the ResourcePak integration utility modules. The TEIM module does not have any dependencies on other integration modules/commands, so it can be installed alone. However, the Symmetrix Integration Utility command (`symintctl`) can often be very useful when diagnosing disk/volume issues on a host.

Configuring Symmetrix Remote Data Facility

The following procedures describe how to configure the TEIM SRDF environment on the backup Exchange 2000/2003 server. There are two possible configurations:

- ◆ BCV remote mirroring
- ◆ Standard remote mirroring

The procedures in this section are only for Exchange 2000 and Exchange 2003.

BCV Remote Mirroring

The BCV remote mirroring configuration (see Figure 4-3 on page 4-6) involves a standard device and its local BCV (R1). The local BCV-R1 is remotely-mirrored by a remote R2 device which also has a remote BCV (BRBCV).

To provide this initial BCV remote mirroring association, you must create a device group on the backup server.

To create a device group, enter:

```
symdg create DgName
```

To configure the TEIM SRDF environment:

1. Add the standard devices to the appropriate device groups:

```
symld -g DgName add dev SymDevName
```

2. Associate all of the local BCVs (R1BCV) to the device groups:

```
symbcv -g DgName associate dev SymDevName
```

Make sure to add the devices in the order in which they are paired with their standard devices.

3. Associate all of the remote BCVs (BRBCV) to the device groups:

```
symbcv -g DgName associate dev SymDevName -rdf -bcv
```

Make sure to add the remote BCV devices in the order in which they are to be paired with their R2 devices.

4. Verify that the device group contains all of the devices that it needs:

```
symdbg show DgName
```

5. All of the standard devices, local BCVs and remote BCVs should now be listed in the order that they were added. To establish the standard and local BCV devices in this order, enter:

```
symmir -g DgName establish -full -exact
```

This performs a full establish on the devices. To determine the current state of the establish command, enter:

```
symmir -g DgName query
```

6. Once this command shows that standard and local BCV device pairs are synchronized, split all of the devices in the device group:

```
symmir -g DgName split
```

7. Establish the R2 and remote BCV device pairs in the order in which they were added to the device group:

```
symmir -g DgName establish -rdf -bcv -full -exact
```

This performs a full establish of the R2 and remote BCV device pairs. To determine the current state of the establish command, enter:

```
symmir -g DgName query -rdf -bcv
```

8. Once this command shows that device pairs are synchronized, split all of the remote devices in the device group:

```
symmir -g DgName split -rdf -bcv
```

At this point the BCVs connected to the backup server should have the same volume labels as the paired R2 devices.

The SRDF environment is now configured and ready for the TEIM.

Prior to running ExBackup2000 or ExBackup2003 with the `-srdf` option, it is important to ensure that the R1BCV/R2 and the R2/BRBCV device pairs are in a split state. To verify that the R1BCV and R2 are split, enter:

```
symrdf -g DgName query -bcv
```

To verify that the R2 and BRBCV pair is split, enter:

```
symmir -g DgName query -rdf -bcv
```

In addition to verifying that the remote devices are in a split state, it is important to ensure that these devices are not mounted by any host. The TEIM will still operate with the remote devices mounted but there is a potential for corruption of data on those devices.

Standard Remote Mirroring

The standard remote mirroring configuration (see Figure 4-4 on page 4-7) involves a standard device (R1) which is remotely mirrored by a remote R2 device and the remote R2 device is mirrored by a BCV (RBCV). This configuration requires the device group to be of type RDF2.

To create a device group, enter:

```
symdg create DgName -type rdf2
```

1. After creating all of the device groups, add the R2 devices to the appropriate device group:

```
symld -g DgName add dev SymDevName
```

2. Associate all of the remote BCVs to the device group:

```
symbcv -g DgName associate dev SymDevName
```

To verify that the device group contains all of the devices, enter:

```
symdg show DgName
```

3. To establish the R2 devices and the remote BCVs (RBCVs) in the order that they were added to the group, enter:

```
symmir -g DgName establish -full -exact
```

This performs a full establish on the devices, which can take a long time depending on the size of the devices. Make sure you remove any mount points from the BCVs on the backup/Exchange server before attempting the establish.

To determine the current state of the establish command, enter:

```
symmir -g DgName query
```

4. Once this command shows that all of the device pairs are synchronized, run the following command to split all of the devices in the device group:

```
symmir -g DgName split
```

At this point, the BCVs connected to the Backup/TEIM server should have the same volume label as its paired R2 device. This environment is now ready for the TEIM.

Prior to running ExBackup2000 or ExBackup2003 with the `-srdf` option, it is important to ensure that the R2 and remote BCVs are in a split state.

Setting Up a Production Exchange 5.5 Server

The following sections describe the setup requirements and strategies for the production Exchange 5.5 server environment supported by the TEIM.

Although the TEIM software is installed only on the backup server, it is critical that the production server be properly configured. You must verify or complete the following tasks on the production server:

1. Verify that Windows 2000 with Service Pack 2 is installed.
2. If you are using dynamic disks on Windows 2000, verify that VERITAS Volume Manager is installed.
3. Configure disks for the Exchange environment.
4. Install Microsoft Exchange Server version 5.5.
5. Install the EMC WideSky software.

Configuring Disks for Exchange

Before you begin disk configuration, you must establish a plan for the Exchange Server devices. This is because the physical head and disk assembly (HDA) isolation is a critical performance consideration within Exchange.

Dedicated Channels and Devices for Logs

The Exchange Server transaction log volumes and data store volumes are typically I/O intensive volumes in large organizations. These volumes should have dedicated HDA on the Symmetrix system. Furthermore, dedicated Symmetrix channels (SCSI directors or Fibre Channel directors) and dedicated host bus adapters (SCSI or Fibre Channel) are recommended for the transaction log and the Information Store volumes.

Exchange Server transaction logs are written sequentially, while the raw data store is a random read/write I/O. Therefore, isolating the volumes improves performance and fault tolerance, while enhancing recoverability. For this reason, separating the transaction log volume from the data store volume is required.

Disk Alignment

You should always create your volumes with partitions that are aligned along the track boundaries of the underlying Symmetrix disk. This improves the performance for any application using those volumes, refer to *Aligning Exchange I/O on Storage Track Boundaries* on page 4-34.

Hot Split When using the Hot Split feature of the TEIM, all Exchange 5.5 volumes must have partitions that are aligned with the underlying disk's track boundaries. This insures that the Hot Split does not cause a torn page on the BCV.

Partition Cluster Size The NTFS partitions should be formatted with a cluster size of 4 KB or a larger multiple of 4 KB to avoid splitting I/Os across the Exchange Server page size of 4 KB. This also optimizes performance. Standard devices that store Exchange databases and transaction logs must have only one partition.

Data Storage Plan You should have a detailed plan of the Exchange data storage devices. This plan should include the number of volumes, the different HDAs for each volume, size and type of volumes (stripe set, volume set, and so on), and volume labels. Volume labels (disk signatures) are helpful because they allow identification of the volumes when they are copied to the BCVs.

On Windows 2000 servers, implement this plan using the Logical Disk Manager.

On Windows NT, use Disk Administrator to assign Windows NT disk signatures to each disk so you can identify them.

Exchange Server Installation

The last step in setting up the production Exchange server environment is to install Microsoft Exchange Server version 5.5. At the end of Exchange setup, you can use the Exchange Performance Optimizer to relocate all of the Exchange databases and logs to the appropriate volumes.

All Exchange databases and transaction logs must be located on Symmetrix storage with an associated BCV. This includes `priv.edb`, `pub.edb`, `dir.edb`, the data store, transaction logs, and the directory transaction logs.

Hot Split When using the Exchange Server 5.5 Hot Split feature of the TEIM, the `edb.chk` file should be located on the same volume as the data store databases.

Stand-alone Exchange 5.5 Server

To move the `edb.chk` file to this volume on a stand-alone Exchange 5.5 server, perform the following steps:

1. Start the Exchange Server Administrator program and retrieve the properties of the server object. To get to the server object in the Exchange Server Administrator program, click **Organization**, **Site**, **Configuration**, **Servers**, **Server**, and then on the **File** menu, click **Properties**.
2. Click the **Database Paths** tab.
3. To modify the location of the `edb.chk` file for the Information Store, select **Information Store Working Path**, and click **Modify**. Using the interface, select the drive letter and folder that the new `edb.chk` file is created in, and then click **OK**.
4. Click **Apply**. This will stop and start the relative services creating the new `edb.chk` on the appropriate drive.

Clustered Exchange 5.5 Server

For a clustered Exchange 5.5 server, perform the following steps:

1. Shut down node 2 of the cluster.
2. On node 1, stop the cluster service.
3. On node 1, start the cluster service with the `-fixquorum` option. The option can be supplied in the **startup parameters** text box when using the GUI or at the command line using the `net start` command.
4. Use the Cluster Administrator tool to verify that all the resources are online, if not, bring them online.
5. Delete the MSCS folder on the quorum disk.
6. Stop (bring offline) all the Exchange resources in the Cluster Administrator.
7. Move the `edb.chk` file from `Exchsrvr\Mdbdata` on the binaries drive to its desired location.
8. Run `regedt32.exe` to edit the registry.
9. Locate and click:
`HKey_Local_Machine\System\CurrentControlSet\Services\MSExchangeIS\Parameters\System\Working Directory`
10. Change the path to reflect the new location of Information Store `edb.chk` file.

11. Start (bring online) all the Exchange services in the Cluster Administrator.
12. Stop the cluster service on node 1.
13. For Windows 2000, start the cluster service on node 1 using the option `-debug -resetquorumlog` to regenerate the MSCS folder.
14. Start the cluster service normally without using any option.
15. Use the Cluster Administrator to verify that all the resources are online; if not, bring them online.
16. Restart node 2 of the cluster.

For more information on the previous procedures, refer to the following Microsoft Knowledge Base articles: Q196332 - *XADM: Edb.chk Does Not Move During Performance Optimization*, Q269014 - *XADM: How to Move the Edb.chk File on a Cluster*, and Q278464 - *How to Change the Exchange Server Database Paths on a Cluster*.

Installing Service Pack

After Performance Optimizer has finished moving files, and the setup program has completed, you must install the necessary Microsoft Exchange Server version 5.5 Service Packs. Service Pack 3 or higher is required.

Disabling Circular Logging

To take advantage of EMC TimeFinder in the Exchange environment, you need to disable circular logging in the Exchange server. Circular logging alleviates storage constraints on the transaction log volume by keeping just the latest five logs and deleting the rest. However, because the total history of logs is not maintained, you cannot perform incremental and differential backups. More importantly, without a full history of transaction logs, you lose the ability to replay transactions against a BCV copy of the Information Store.

Note that circular logging is enabled by default after an Exchange Server installation, and it can be disabled through the Exchange Advance File Properties menu: select **Server, File - Properties, Advanced** from the **Exchange Administrator** menu.

Disabling circular logging has the following ramifications:

- ◆ Requires extremely careful log management.
- ◆ Causes transaction logs to accrue and not be purged until a full online backup is performed, or they are manually archived.
- ◆ Requires larger disk volumes to accommodate the increased number of logs.

Microsoft Exchange Event Service

The Microsoft Exchange Event Service (msexchanges) is installed and set to `automatic` during the typical Microsoft Exchange Server 5.5 installation. This service is not commonly used, however, so it is not included in the default list of services for the TEIM. The administrator must decide to either not use the Event Service and set it to `manual`, or use a services initialization file to specify that the Event Service needs to be shut down. When using a services initialization file with the Event Service, be sure to recognize that it is dependent on the Information Store. This step is not necessary when performing Hot Splits.

Deleted Item Retention

Microsoft Exchange Server has built-in functionality to retain deleted items for a specified period. You have the option to restrict the purging of these deleted items after a full backup. If you select this option when using the TEIM, deleted items will never be purged because the TEIM does not perform an online backup using the API. Selecting this option causes your Exchange database to grow consistently but never shrink. Eventually, your database will run out of free disk space. For this reason, it is required that the default values be kept for this setting.

Testing the Exchange Installation

Test your Exchange Server installation by creating a user and attempt to log in to that user's mailbox using Microsoft Outlook. If you are able to do this, then the Exchange installation was a success.

WideSky Installation

EMC WideSky Solutions Enabler, which provides the TimeFinder and SRDF components is required. Refer to the *WideSky Solutions Enabler Installation Guide*, and verify that the software with the Base, TimeFinder, and SYMAPI server licenses are enabled.

If you have an SRDF environment, the SRDF license is also required. These licenses should be purchased from EMC prior to beginning this setup.

Make sure that the SYMAPI server service is started (`symapisrv start`).

Setting Up a Backup Exchange 5.5 Server

This section describes the setup of a backup environment for an Exchange 5.5 Server.

The backup/recovery server should ideally have the same Symmetrix connectivity hardware configuration as the production server. Using the same host bus adapters to the Symmetrix system allows for consistent SCSI or Fibre Channel settings at the host bus adapter level.

The following sections outline the proper installation procedure for the backup Exchange server that you are going to use with the TEIM.

The main installation tasks must be completed in the following order on the backup server:

1. Verify that Windows 2000 with Service Pack 2 is installed.
2. Install EMC WideSky with Base and TimeFinder license keys.
3. Create SYMCLI TimeFinder device groups.
4. Perform the initial TimeFinder full establish on the device groups.
5. Install Microsoft Exchange Server version 5.5.
6. Install TimeFinder Exchange Integration Module.

Creating SYMCLI TimeFinder Device Groups

In device groups, TimeFinder SYMCLI pairs Symmetrix standard volumes with their associated BCV mirrors for TimeFinder operations. The disks associated with a device group are used to create BCV copies of the Exchange Server databases and transaction logs for backup and recovery purposes.

Although TimeFinder device groups are not needed for the TEIM to run on Windows 2000, you must use device groups during the initial setup. These device groups can also be beneficial when restoring backups. It is recommended that you create two independent TimeFinder device groups, one for each of the following:

- ◆ Exchange Directory and Information Store databases
- ◆ Exchange Directory and Information Store transaction logs
- ◆ Exchange Directory and Information Store databases
- ◆ Exchange Directory and Information Store transaction logs

A user-defined name is used to specify a TimeFinder device group. The name must be unique for each device group on a single Symmetrix system.

The following sequence of commands are a good example of the process of creating the device groups:

```
symdbg create -type regular exlogs
symdbg create -type regular exdata
symdbg list                      (verifies device groups are present)
syminq                          (lists Symmetrix devices acquired)
symld add dev 02c -g exlogs      (adds physical drive to device group)
symld add dev 02d -g exlogs
symld add dev 02a -g exdata
symld add dev 022 -g exdata
symld add dev 023 -g exdata
symbcv -g exdata associate dev 052 (associates BCV to device group)
symbcv -g exdata associate dev 053
symbcv -g exdata associate dev 054
symbcv -g exlogs associate dev 055
symbcv -g exlogs associate dev 056
```

For more information about these commands, see the *WideSky Solutions Enabler Symmetrix Base Management CLI Product Guide*.

Establishing BCVs

For detailed information on using TimeFinder device group commands to control TimeFinder operations, see the *WideSky Solutions Enabler Symmetrix TimeFinder CLI Product Guide*.



CAUTION

Before you perform an establish operation, make sure the BCV devices are not mounted to a drive letter.

1. To perform an establish, enter the following form:

```
symmir est -full -g exdata -exact
symmir est -full -g exlogs -exact
```

The `exact` option is valid only for a full establish or full restore operations on a group. It causes SYMCLI to pair devices in the exact order that the Standard and BCV devices have been added to the device group.

Alternately, to individually establish the BCV pairs, use the follow form:

```
symmir -full est -g exdata DEV001 BCV dev 02C
```

2. To check establish operation status, run the following commands:

```
symmir query -g exdata
symmir query -g exlogs
```

3. Once the BCVs are synchronized with the standard devices, they must be split to make them available to the backup/recovery host. To split the BCVs run the following:

```
symmir split -g exdata
symmir split -g exlogs
symmir query -g exdata (verifies the split is complete)
symmir query -g exlogs
```

4. To verify that the establish was a success, open Disk Management to ensure that the volume labels were correctly copied to the BCVs.

Do not restart the backup server while BCV devices are synch-in-progress or synchronized.

Exchange Server Installation

The last step in preparing the backup Exchange Server is to install Microsoft Exchange Server version 5.5. The installation of Exchange Server version 5.5 for the backup server is similar to the process described for the production server with two differences. For the backup server, the Exchange Directory Service must be installed on a non-BCV disk or a BCV that is not being used for TimeFinder operations. This enables the backup Exchange server to be brought up for single mailbox recovery purposes. In addition, the backup Exchange server must create an identical, but separate, site and organization.

The Exchange Directory Service database, `dir.edb`, can only be used on the Exchange server that it was created for. So, it is impossible to use the `dir.edb` from `\\extest01` on `\\extest02`. For example, assume that `\\extest02` is the backup Exchange server and its `dir.edb` is located on the BCV that is used for backup of `\\extest01`.

After a backup, `\\extest02's dir.edb` is overwritten with `\\extest01's dir.edb`, making it impossible to start the Exchange Directory Service on `\\extest02`.

By locating `\\extest02's` Directory Service on a volume where it will not be overwritten, we are able to back up `\\extest01's` Directory Service and perform single mailbox recoveries on

\\extest02. This means that both the Directory database (`dir.edb`) and the Directory logs need to be located on a nonBCV volume.

One additional step is needed for single mailbox recoveries. Since \\extest02 is using its own `dir.edb`, it is missing all of the users on \\extest01. The consistency adjuster must be used on the backup server to populate the directory with all of the users from \\extest01. Once this is completed, a single mailbox recovery is possible.

To avoid replication between the production and backup servers, it is necessary to create two identical, but separate, Exchange organizations and sites. The site and organization names must be identical so that the databases can be interchanged between the backup and production Exchange servers. Install Service Pack 3 or higher.

To perform a single mailbox recovery on the backup server when using the Hot Split option, the Information Store's working path must be changed to the location of the checkpoint file (`edb.chk`) on the BCV. The procedure to change this path is identical to that on the production server, which is outlined in *Exchange Server Installation* on page 4-26. Changing this path causes the backup server to use the actual checkpoint file from the production server when starting the Exchange services. Failure to make this configuration change on the backup server when using the Hot Split option could result in the inability to perform a single mailbox recovery.

EMC ResourcePak Modules

Use the EMC ResourcePak for Windows Setup program to install the TimeFinder Exchange Integration Module.

Refer to Chapter 2, for complete instructions on installing the TEIM module for EMC ResourcePak for Windows.

If you plan to use the TEIM in a Microsoft Cluster Service environment, you will need to either install the Cluster Administrator or copy the `clusapi.dll` file to the backup server's `system32` directory.

Aligning Exchange I/O on Storage Track Boundaries

The Windows 2000 operating systems have an internal structure called the master boot record (MBR) that limits the maximum number of hidden sectors to 63. Specifically, the partition table inside of the MBR maintains StartingSector and EndingSector values which are six bits in length. Therefore, their maximum value is 63 due to the limited number of bits and the fact that sector enumeration begins at 1, not 0. This characteristic of the MBR causes the default starting sector for disks that report more than 63 sectors per track to be the 64th sector. As a result, when programs transfer data to or from these disks, misalignment can occur at the track level, with allocations beginning at a sector other than the starting sector. This misalignment can defeat system optimizations of I/O operations designed to avoid crossing track boundaries. Additional information regarding the MBR and its internal structures can be found in the *Disk Concepts and Troubleshooting* article at:

http://www.microsoft.com/WINDOWS2000/techinfo/reskit/en/ProRK/prcb_dis_qxql.htm

In the case of a physical disk that maintains 64 sectors per track, Windows operating system will always create the partition starting at the 64th sector, thus misaligning it with the underlying physical disk. To be certain of disk alignment, you can use DiskPar, which is a utility provided by Microsoft in the Windows 2000 Resource Kit. DiskPar is a command line utility that explicitly sets the starting offset in the MBR. Setting the starting offset can ensure track alignment and improve disk performance. Microsoft Exchange 2000 Server writes data in multiples of 4 KB I/O (4 KB for the databases and up to 32 KB for streaming files), so it is important that the starting offset be a multiple of 4 KB. Failure to do so may result in a single I/O spanning two tracks, causing performance degradation.

Figure 4-5 shows the case where a partition was created without using DiskPar resulting in a partition that is not aligned with the underlying physical disk.

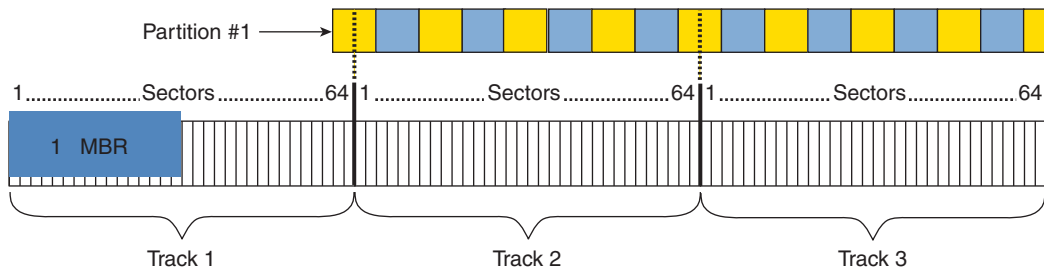


Figure 4-5 Creating a Partition Without DiskPar

By breaking out the partition into 4 KB blocks, as the colors do above, it is clear to see that one out of every eight blocks would be straddling a track boundary. This greatly reduces the performance of the physical disk, and thus the application.

Figure 4-6 shows the case where DiskPar was used to create the partition along a track boundary of the underlying physical disk.

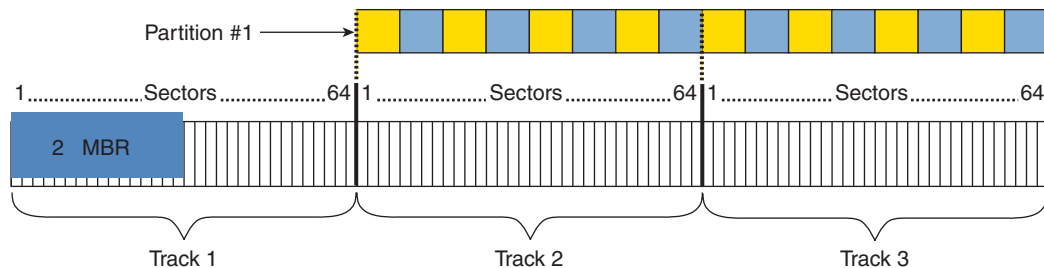


Figure 4-6 Creating a Partition With DiskPar

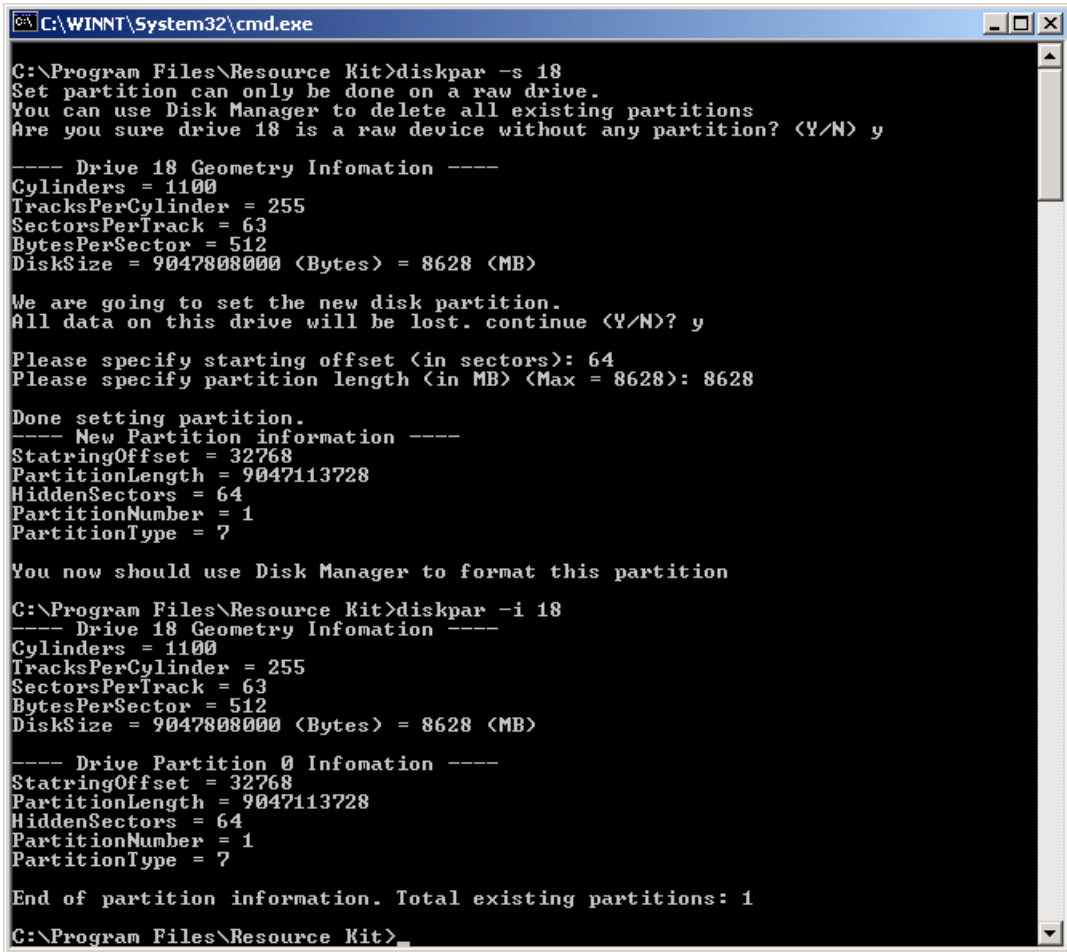
In this case, there are no 4 KB blocks straddling a track boundary.

To set the starting offset and create the first partition on disk X:

1. If disk X is a raw drive, skip to step 3. If disk X has data that you do not want to lose, backup that data.
2. Delete all partitions on disk X, making it a raw disk.
3. Issue `DiskPar -s X` (where X is the drive number) from the command line. You can obtain the drive number by using the SYMINQ command or by using Disk Manager.

4. Make sure that the device you are partitioning is a raw device and that all partitions have been deleted from the device. You can delete any existing partitions using Disk Manager.
5. Confirm that this is the drive you want to partition.
6. Enter the new starting offset (in sectors), and the partition length (in MB). This writes the new offset to the MBR for that drive and creates the partition. To determine the starting offset for an Exchange device, choose an offset that is some multiple of 4 KB. Exchange writes I/O in 4 KB blocks and no more than 32 KB per track.
7. After you enter the starting offset and partition size, the MBR is modified and the new partition information displays.
8. Issue `DiskPar -i X` (where *X* is the drive number) at the command prompt to review the information on the newly created partition. In the example shown in Figure 4-7, the starting offset is 32768, which is a multiple of 4 KB. We also see that the device is reporting 63 sectors per track.
9. Use Disk Manager to format the partition that was just created. When formatting this partition make sure that **NTFS** is selected as your chosen file system and the allocation unit size is 4096. Having the allocation unit size set to 4096 bytes and having the starting offset a multiple of 4096 (4 KB) ensures that this partition is always aligned on a 4 KB boundary.

Figure 4-7 shows the execution of these commands.



```

C:\WINNT\System32\cmd.exe

C:\Program Files\Resource Kit>diskpart -s 18
Set partition can only be done on a raw drive.
You can use Disk Manager to delete all existing partitions
Are you sure drive 18 is a raw device without any partition? (Y/N) y

---- Drive 18 Geometry Information ----
Cylinders = 1100
TracksPerCylinder = 255
SectorsPerTrack = 63
BytesPerSector = 512
DiskSize = 9047808000 (Bytes) = 8628 (MB)

We are going to set the new disk partition.
All data on this drive will be lost. continue (Y/N)? y

Please specify starting offset (in sectors): 64
Please specify partition length (in MB) (Max = 8628): 8628

Done setting partition.
---- New Partition information ----
StartingOffset = 32768
PartitionLength = 9047113728
HiddenSectors = 64
PartitionNumber = 1
PartitionType = 7

You now should use Disk Manager to format this partition

C:\Program Files\Resource Kit>diskpart -i 18
---- Drive 18 Geometry Information ----
Cylinders = 1100
TracksPerCylinder = 255
SectorsPerTrack = 63
BytesPerSector = 512
DiskSize = 9047808000 (Bytes) = 8628 (MB)

---- Drive Partition 0 Information ----
StartingOffset = 32768
PartitionLength = 9047113728
HiddenSectors = 64
PartitionNumber = 1
PartitionType = 7

End of partition information. Total existing partitions: 1

C:\Program Files\Resource Kit>

```

Figure 4-7 Creating a Partition With DiskPar on a Raw Device

Using the DiskPar utility we have successfully created a partition on a raw device that is aligned on a 4 KB boundary.

Dual-Boot for Single Mailbox Recoveries

This section provides procedures necessary for TEIM users to perform recoveries specific to Exchange 2000 mailboxes. TEIM for both Exchange Server 5.5 and Exchange 2000 is a useful tool to expedite single mailbox recoveries due to the immediate availability of the Exchange data on the mirroring BCV devices. In tape backup environments, there is no need to restore the data from tape.

However in Exchange 2000 systems, a single mailbox recovery must be performed with the backup server processes that exist in a directory tree primary zone (forest) separate from that of the production Exchange 2000 server. The TEIM fails when the backup Exchange 2000 server is not in the same forest as the production Exchange 2000 server. In this situation, the Microsoft APIs, which the TEIM normally uses (CDOEXM), are not supported across forests.

To work around the Microsoft incompatibility, a dual-boot configuration for the EMC TEIM should be implemented. The basis of the dual-boot option is that one boot is an Exchange 2000 backup server in its own forest (for recovering mailboxes), while the other boot is an Exchange 2000 backup server in the production forest (for running the TEIM). With these configurations, the only difference between the TEIM and single mailbox recoveries is a special reboot of the backup Exchange 2000 server.

Configuration Steps

The following sections describe the steps needed to configure a dual-boot backup Exchange 2000 server that works around this single mailbox incompatibility. In this example, it is assumed that the production Exchange 2000 server is correctly installed and configured for proper TEIM operation. Also assume that an operational DNS server exists in the forest. In our example, the production forest (procedure) is named `TEIMPROD.COM` and the backup forest is `TEIMBACKUP.COM`.

Production Forest Configuration

The following steps configure the production DNS server to service all DNS requests for the backup server:

1. In the properties of TCP/IP, verify that the production Exchange 2000 server has the IP address of the DNS server entered as **Preferred DNS Server**.

2. On the production DNS server, open the DNS console by selecting:
Start, Programs, Administrative Tools, DNS
3. Verify that there is a `TEIMPROD.COM` primary standard DNS zone on the DNS server.
4. Add a primary standard DNS zone named `TEIMBACKUP.COM` by right-clicking the server in the console and select:
New, Primary DNS Zone
5. Right-click the new `TEIMBACKUP.COM` zone and select:
Properties
6. Change the **Allow dynamic updates** property to **Yes** (No is the default).

Backup Exchange Configuration

The following procedure sets up the backup Exchange 2000 server configuration. The backup Exchange 2000 server must be configured with two separate partitions to accommodate dual boots:

Boot #1

1. Install the Windows operating system on the first partition of the backup server.
2. In the properties of TCP/IP, add the IP address of the production DNS server as **Preferred DNS Server**.
3. Select **Start, Run**, and enter `dcpromo` in the box. Click **OK**. This starts the Active Directory installation wizard.
4. Choose to create a new forest and a new domain name and enter **TEIMBACKUP.COM**
(You should not get prompted to install DNS. If prompted, recheck the DNS server setup in `TEIMPROD.COM`.)
5. Allow the wizard to complete the installation (may take up to 5 minutes) and then reboot the server.
6. When the server comes up, verify that the DNS server on `TEIMPROD.COM` has been updated similar to the tree display of Figure 4-8 on page 4-40.
7. Install Exchange 2000. When prompted for an Exchange 2000 organization name, enter the same organization name that is used for the production Exchange 2000 server. Then configure the storage groups and databases to be identical to those on the production Exchange 2000 server (including volume drive letters and paths).

8. Stop all of the Exchange 2000 services and set their startup to **Manual**.

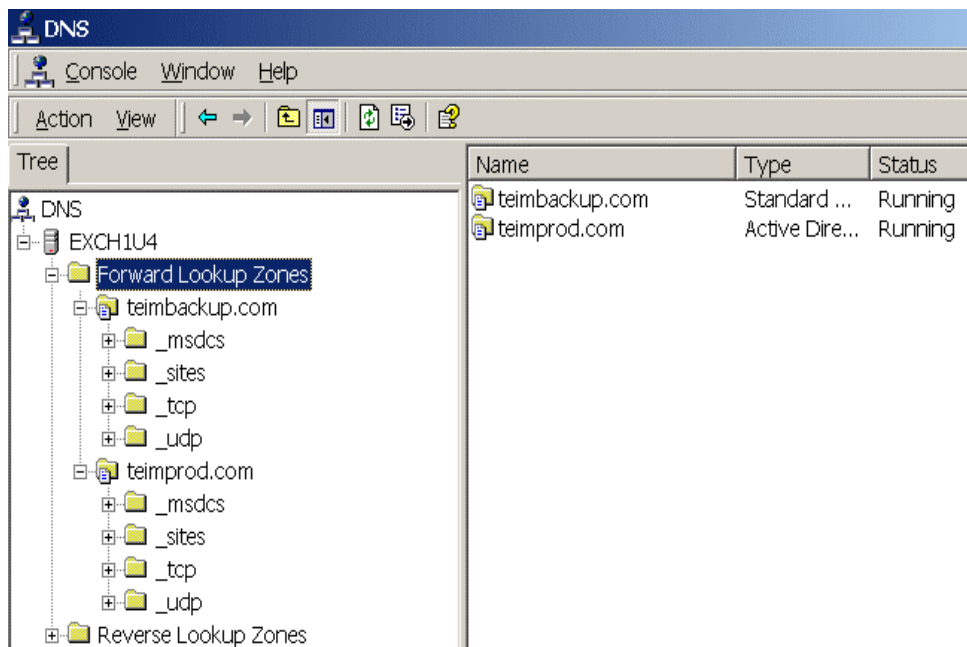


Figure 4-8 An Example DNS Forest

Boot #2 This second partition is configured to run the TEIM within the production forest.

1. Install the Windows operating system on the second partition of the backup server.
2. In the properties of TCP/IP, add the IP address of the DNS server as **Preferred DNS Server**.
3. Join the server into the `TEIMPROD.COM` domain.

4. Edit the `boot.ini` file (hidden file located at the root of the system partition) to give each boot a friendly name that indicates its role. For example:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(3)\WIN2K
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\
    WIN2K="EXCH1u5.TEIMBACKUP.COM(Active Directory) "
    /fastdetect
multi(0)disk(0)rdisk(0)partition(3)\
    WIN2K="EXCH1U5.TEIMPROD.COM(Backup Server) "
    /fastdetect
```

5. Install Exchange 2000 or Exchange 2003. The storage groups and databases do not need to be configured.
6. Stop all of the Exchange 2000/2003 services and set their startup to **Manual**.
7. Install the EMC WideSky Solutions Enabler from the Solutions Enabler kit and then the TEIM functionality from the ResourcePak kit.

Performing Daily Backups With TEIM

To perform daily backups of your production Exchange 2000 server with TEIM, boot to "Boot #2\" denoted as "EXCH1U5.TEIMPROD.COM (Backup Server)" in the boot menu. The operation of the TEIM in this configuration is no different than the standard TEIM setup.

Single Mailbox Recovery Using BCVs

When a recovery is required for an Exchange 2000/2003 mailbox, the backup Exchange 2000/2003 server must be rebooted. boot to "Boot #1" denoted as "EXCH1U5.TEIMBACK.COM (Active Directory)" so that the server is running in its own forest. From here, the standard Microsoft single mailbox recovery procedure can be followed according to the whitepaper, *Mailbox Recovery for Microsoft Exchange 2000 Server*, available on the Microsoft web site.

Note: You may find that it is not advisable to leave the server in this configuration. Once you have completed the recovery operation for an Exchange 2000/2003 mailbox, it is suggested that you reboot the backup server with boot #2 option, to bring the server back to the standard daily backup mode.

Backup and Restore Operations With TEIM

This chapter describes how to perform backup and restore operations to a Windows Exchange server database using the TimeFinder Exchange Integration Module (TEIM) command line interface.

◆ Backup Execution Environments.....	5-2
◆ Backing Up Exchange 5.5 Servers.....	5-6
◆ Backing Up Exchange 2000 Servers.....	5-8
◆ Backing Up Exchange 2003 Servers.....	5-11
◆ Backing Up Multiple Windows 2000/2003 Servers	5-14
◆ Creating a Backup Command Initialization File	5-15
◆ Creating a Services Initialization File.....	5-19
◆ Restore Procedures.....	5-21
◆ Troubleshooting.....	5-34

Backup Execution Environments

The various TEIM backup executable commands target different combinations and versions of Windows and Exchange Server releases. The TEIM backup commands intergrate with and support the following environments:

- ◆ Windows 2000 Server with Exchange Server 5.5 —
ExBackup2
- ◆ Windows 2000 multiple Exchange 5.5 Servers —
ExBackupCommander2
- ◆ Windows 2000 Server with Exchange 2000 Server and
Windows 2000 with SharePoint Portal Server 2001 —
ExBackup2000
- ◆ Windows 2000 Server with Exchange 2003 Server,
Windows 2003 Server with Exchange 2003 Server —
ExBackup2003
- ◆ EMC WideSky TimeFinder and SRDF environments

Table 5-1 briefly describes each of the TEIM commands.

Table 5-1 TEIM Commands

Command	Description
ExBackup2	For Windows 2000, backs up a single or a clustered Exchange 5.5 Server.
ExBackupCommander2	For Windows 2000, backs up multiple Exchange 5.5 Servers through a single backup server.
ExBackup2000	For Windows 2000 Server, backs up a single or a clustered Exchange 2000 Server or SharePoint Portal Server.
ExBackup2003	For Windows 2000 Server and Windows 2003 Server, backs up a single or a clustered Exchange 2003 Server.

Table 5-2 illustrates the options supported with each command.

Table 5-2 TEIM Command Options

Command	Supported Options								
	TimeFinder	Hot Splits	Instant Split	SRDF	EMC Snap	Multiple BCV	Full Establish	Multiple Server Backup	Long Duration Locks
ExBackup2	X	X	X						
ExBackupCommander2	X	X	X					X	
ExBackup2000	X	X	X	X	X	X	X	X	X
ExBackup2003	X	X	X	X	X	X	X	X	X

Various Considerations for Device Configurations

The following are various device configuration or environment setups, and the possible support options for each, when running TEIM operations.

Local TimeFinder Operations

The following table shows the possible options for Local TimeFinder (non-SRDF) operations of TEIM:

Table 5-3 Local TimeFinder Operations Support

Source	Mirror	-hot allowed	-srdf allowed	Comments
STD R1 R2	BCV BCV-R1 BCV-R2	Yes	No	All combinations of the listed source and mirror volumes are supported.

Standard Remote Mirroring

The following table shows the options for Standard Remote Mirroring SRDF operations of TEIM:

Table 5-4 Standard Remote Mirroring Operations Support

Source	Mirror 1	Mirror 2	SRDF Link State	-hot allowed	-srdf required	Comments
R1	R2	RBCV	Synchronized	Yes	Yes	Using the <code>-nobrbcv</code> option will result in nothing being backed up.
R1	R2	RBCV	Split	No	Yes	No <code>-hot</code> option, because you cannot instant split an SRDF link.

BCV Remote Mirroring

The following table shows the options for BCV Remote Mirroring SRDF operations of TEIM:

Table 5-5 BCV Remote Mirroring Operations Support

Source	Mirror 1	Mirror 2	Mirror 3	SRDF Link State	-hot allowed	-srdf required	Comments
STD	BCV-R1	R2	BRBCV	Split	Yes	No	The BRBCV will not be used if the <code>-nobrabcv</code> is specified.

Although the `-srdf` option is not required in this configuration, it is needed if you want the R2 and BRBCV to be established and split. Not passing the `-srdf` option will yield a local TimeFinder operation (between the STD and BCV-R1 only).

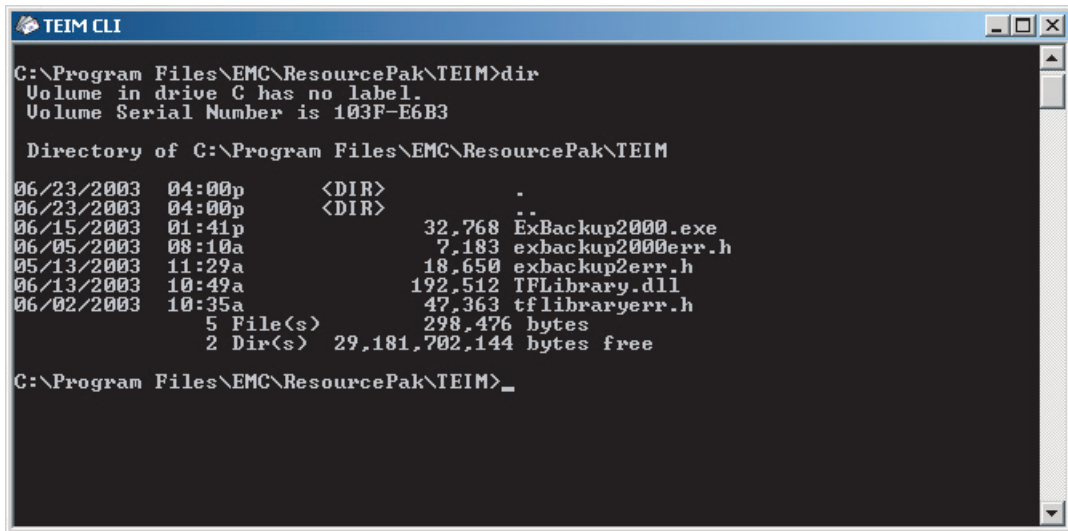
Command Line Start Up

To use TEIM CLI for command line entries:

1. From the **Start** menu, select **Programs, EMC, ResourcePak, TimeFinder Exchange Integration Module, TEIM CLI**.

TEIM CLI (MS-DOS command prompt window) opens to the \Program Files\EMC\ResourcePak\TEIM directory (see Figure 5-1).

2. Enter TEIM commands at the prompt.
3. Type **exit** to close the console window.



```

TEIM CLI
C:\Program Files\EMC\ResourcePak\TEIM>dir
Volume in drive C has no label.
Volume Serial Number is 103F-E6B3

Directory of C:\Program Files\EMC\ResourcePak\TEIM

06/23/2003  04:00p        <DIR>          -
06/23/2003  04:00p        <DIR>          ..
06/15/2003  01:41p           32,768  ExBackup2000.exe
06/05/2003  08:10a            7,183  exbackup2000err.h
05/13/2003  11:29a           18,650  exbackup2err.h
06/13/2003  10:49a          192,512  TFLibrary.dll
06/02/2003  10:35a          47,363  tflibraryerr.h
               5 File(s)           298,476 bytes
               2 Dir(s)  29,181,702,144 bytes free

C:\Program Files\EMC\ResourcePak\TEIM>_
  
```

Figure 5-1 TimeFinder Exchange Integration Module CLI Start Up

Backing Up Exchange 5.5 Servers

You can backup a stand-alone or clustered Windows 2000 server with Exchange 5.5 databases using a single TEIM command.

The TEIM command `ExBackup2` produces an exact copy of the production volumes that hold the Exchange Information Stores and Logs. This provides the capability for administrators to perform either a full or single-mailbox restore when needed.

The following action sequences summarize the TEIM tasks to backup a Windows 2000 server with an Exchange 5.5 database using `ExBackup2`:

- ◆ Parse and validate the input parameters.
- ◆ If MSCS is installed, determine which node is the active Exchange node.
- ◆ Initialize event logging on the backup server.
- ◆ Scan the production server for -1018 errors.
- ◆ Extract the Exchange database and log paths from the production server.
- ◆ Use SYMAPI mapping to determine which standard and BCV devices correspond to those Exchange database and log volumes.
- ◆ Establish these database and log devices (incremental establish if possible).
- ◆ Poll the BCV pairs until fully synchronized.
- ◆ Shut down Exchange services (or offline resources in the case of MSCS). Skip this for Hot Splits.
- ◆ Poll BCV pairs again to verify synchronization.
- ◆ Split BCVs from the standard devices.
- ◆ Restart online Exchange services or resources. Skip this for Hot Splits.
- ◆ Remount all previously mounted drives on the backup server.
- ◆ Run `ESEFILE` on all databases to verify consistency.

Use the Exchange backup API to perform log management on a production server.

Running ExBackup2

You can run ExBackup2 on a stand-alone Exchange server or an MSCS clustered Exchange server by specifying either the `-s` or `-c` option:

```
ExBackup2 -s ExchgServer
          -c ClustName
```

Optional Selections

The following syntax are optional selections to this server backup command:

```
[-f InitFile | -F InitPath] [-sd symapidb] [-v]
[-t TimeOut] [-o OutFile] [-p] [-nologdelete]
[-hot | -instant] [-norestart]
```

Backup Monitor

To verify or capture the backup process activity, you can pause the console window to keep it open long after the backup processes complete, using the `-p` option. Or you can specify an output file to capture the backup activity, using the `-o` option. To see more backup activity detail in the output, you can specify the verbose mode (`-v`).

Hot Splits

With the `-hot` option you can perform a hot split backup where the TEIM performs an online snapshot of the Exchange database (Exchange is not stopped before the split). The split is assisted with the instant TimeFinder split behavior. Note that this option overrides and ignores the StopServices request list in the initialization file.

TimeFinder Controls

You can control the TimeFinder split behavior by specifying `-hot` to cause an instant split on the BCV pairs or specify a timeout period to the full BCV sync (establish) operation, using the `-t` option. The default timeout is 10 minutes. With the `-sd` option, you can specify an alternate SYMAPI database file when not using the default file.

Returns

The backup command returns a zero upon success or a non-zero value for various warnings and failures. A list of return codes can be found in `ExBackup2Err.h` in the TEIM directory.

Stopping/Starting Services

You can stop the individual Microsoft services from running during the critical backup processes to minimize errors. Using the `-f` and `-F` option, you can specify your services initialization file that contains the services to stop and restart. If the file is just in the TEIM working directory, you simply specify a `.ini` file name with the `-f` option. If you have an alternate directory from the working default, then specify a full path name with the `-F` option.

For more information about building a services initialization file, see *Creating a Backup Command Initialization File* on page 5-15.

Backing Up Exchange 2000 Servers

You can backup a stand-alone or clustered Windows 2000 servers with multiple Exchange 2000 databases using a single TEIM command.

The TEIM command `ExBackup2000` produces an exact copy of the production volumes that hold the Exchange Information Stores and Logs. This provides the capability for administrators to perform either a full- or single-mailbox restore when needed.

The following summarizes the TEIM tasks to backup a Windows server with an Exchange 2000 database using `ExBackup2000`:

- ◆ Parse and validate the input parameters.
- ◆ If MSCS is installed, determine which node is the active Exchange node.
- ◆ Initialize event logging on the backup server.
- ◆ Query the active directory for information about the Exchange server, including number of storage groups, information stores, and so on.
- ◆ Scan the production server for -1018 errors.
- ◆ Use WideSky mapping to determine which standard and BCV devices correspond to those Exchange storage groups and information stores.
- ◆ Establish these database and log devices (full establish if specified).
- ◆ Poll the BCV pairs until fully synchronized.
- ◆ For each storage group whose devices have fully synchronized:
 - Dismount all of its information stores (except for hot splits).
 - Poll BCV pairs again to verify synchronization.
 - Split BCVs from the standard devices.
 - Remount all of the information stores (except for hot splits).
 - Mount each information store's BCV on the backup server and begin running `ESEUTIL*`.
 - Use the Exchange backup API to perform log management on the production server.

- If an SRDF remote backup is desired:
 - Establish the remote mirror (R2) with the local BCV (R1-BCV) for each database and log volume.
 - Split the remote mirror (R2) with the local BCV (R1-BCV) for each database and log volume.
- ◆ If a remote BCV (BRBCV) of the remote mirror (R2) is desired:
 - Establish the remote BCV (BRBCV) with the remote mirror (R2) for each database and log volume.
 - Split the remote BCV (BRBCV) with the remote mirror (R2) for each database and log volume.

ESEUTIL* is run against each information store BCV separately, and in sequence. But each storage group can be running ESEUTIL at the same time. So if there are four storage groups, there could be four instances of ESEUTIL* running at any given time.

Running ExBackup2000

You can run ExBackup2000 on a stand-alone Exchange or SharePoint Portal Server; or an MSCS clustered Exchange 2000 server by specifying either the `-s` for the specific server or the `-c` option for the clustered:

```
ExBackup2000 <-s ServerName> | -c ClustName
ExBackup2000 -f InitFile
```

For SharePoint Portal Servers, specify the `-sps` option.

Optional Selections

The following syntax are optional selections to this server backup command:

```
[ -sps ] [ -sg StorGroup ] [ -o OutFile ]
[ -srdf [ -nobrbcv ] ] [ -hot | -instant ] [ -test ]
[ -nologdelete ] [ -v ] [ -full ] [ -multi ] [ -snap ]
[ -lock [ list | releaseall | release -sid SymID ]
  [ -lockid LockID ] [ -sid SymID ] ]
```

For more information on these options, refer to *ExBackup2000* on page A-15.

Backup Monitor

To verify or capture the backup process activity, you can specify an output file to capture the backup activity, using the `-o` option. To see more backup activity detail in the output, you can specify the verbose mode (`-v`).

Multiple Servers

You can backup multiple production servers by specifying a list of the server names for backup in an initialization file, using the `-f` option that identifies the file name target.

SharePoint Portal Server	You can target a SharePoint Portal Server by specifying the <code>-sps</code> option along with specifying its name in the <code>-s</code> name-place.
Hot Splits	With the <code>-hot</code> option you can perform a hot split backup where the TEIM performs an online snapshot of the Exchange database (Exchange is not stopped before the split). The split is assisted with the instant TimeFinder split behavior.
Snapshot Technologies	The TEIM uses TimeFinder as its default snapshot technology. To force a full TimeFinder establish, specify the <code>-full</code> option. To use multiple BCVs, specify the <code>-multi</code> option. To use the EMC Snap technology, specify the <code>-snap</code> option.
SRDF Controls	You can back up to devices on the remote Symmetrix in the device group over the SRDF link with the <code>-srdf</code> option. When using the <code>-srdf</code> option, you can also reject backing up the remote BCV using the <code>-nobrbcv</code> option.
TimeFinder Controls	You can control the TimeFinder split behavior by specifying <code>-instant</code> to cause an instant split on the BCV pairs or specify a hot split with the <code>-hot</code> option. Use the <code>-full</code> option to force a full establish on all BCVs on the local Symmetrix unit that are being used in the Exchange backup.
Transaction Log Management	Normal TEIM functionality includes the management processing of transaction logs on the production server. If you need to allow another software product to manage the logs, you must use the <code>-nologdelete</code> option to force the TEIM to not manage these logs.
Test Mode	If you are tentative about running a backup command on a server (or particularly a command that involves multiple servers), you can specify the <code>-test</code> option that only validates and checks for proper command syntax, Enginuity and Exchange versions, etc. In test mode, the command will not execute any controls on devices or BCV devices in the database and not actually start the backup processes (such as establishing BCV pairs or dismounting devices). This option cannot be used with the <code>-c</code> (cluster) option.
Returns	The backup command returns a zero upon success or a non-zero value for various warnings and failures. A list of return codes can be found in <code>ExBackupErr2000.h</code> in the TEIM directory.

Backing Up Exchange 2003 Servers

You can backup a stand-alone or clustered Windows 2000/2003 servers with multiple Exchange 2003 databases using a single TEIM command.

The TEIM command `ExBackup2003` produces an exact copy of the production volumes that hold the Exchange Information Stores and Logs. This provides the capability for administrators to perform either a full- or single-mailbox restore when needed.

The following summarizes the TEIM tasks to backup a Windows server with an Exchange 2003 database using `ExBackup2003`:

- ◆ Parse and validate the input parameters.
- ◆ If MSCS is installed, determine which node is the active Exchange node.
- ◆ Initialize event logging on the backup server.
- ◆ Query the active directory for information about the Exchange server, including number of storage groups, information stores, and so on.
- ◆ Scan the production server for -1018 errors.
- ◆ Use WideSky mapping to determine which standard and BCV devices correspond to those Exchange storage groups and information stores.
- ◆ Establish these database and log devices (full establish if specified).
- ◆ Poll the BCV pairs until fully synchronized.
- ◆ For each storage group whose devices have fully synchronized:
 - Dismount all of its information stores (except for hot splits).
 - Poll BCV pairs again to verify synchronization.
 - Split BCVs from the standard devices.
 - Remount all of the information stores (except for hot splits).
 - Mount each information store's BCV on the backup server and begin running `ESEUTIL*`.
 - Use the Exchange backup API to perform log management on the production server.

- If an SRDF remote backup is desired:
 - Establish the remote mirror (R2) with the local BCV (R1-BCV) for each database and log volume.
 - Split the remote mirror (R2) with the local BCV (R1-BCV) for each database and log volume.
- ◆ If a remote BCV (BRBCV) of the remote mirror (R2) is desired:
 - Establish the remote BCV (BRBCV) with the remote mirror (R2) for each database and log volume.
 - Split the remote BCV (BRBCV) with the remote mirror (R2) for each database and log volume.

ESEUTIL* is run against each information store BCV separately, and in sequence. But each storage group can be running ESEUTIL at the same time. So if there are four storage groups, there could be four instances of ESEUTIL* running at any given time.

Running ExBackup2003

You can run *ExBackup2003* on a stand-alone Exchange server, or an MSCS clustered Exchange 2003 server by specifying either the *-s* for the specific server or the *-c* option for the clustered:

```
ExBackup2003 <-s ServerName> | -c ClustName
ExBackup2003 -f InitFile
```

Optional Selections

The following syntax are optional selections to this server backup command:

```
[ -sg StorGroup ] [ -o OutFile ]
[ -srdf [ -nobrcv ] ] [ -hot | -instant ] [ -test ]
[ -nologdelete ] [ -v ] [ -full ] [ -multi ] [ -snap ]
[ -lock [ list | releaseall | release -sid SymID ]
  [ -lockid LockID ] [ -sid SymID ] ]
```

For more information on these options, refer to *ExBackup2003* on page A-20.

Backup Monitor

To verify or capture the backup process activity, you can specify an output file to capture the backup activity, using the *-o* option. To see more backup activity detail in the output, you can specify the verbose mode (*-v*).

Multiple Servers

You can backup multiple production servers by specifying a list of the server names for backup in an initialization file, using the *-f* option that identifies the file name target.

Hot Splits	With the <code>-hot</code> option you can perform a hot split backup where the TEIM performs an online snapshot of the Exchange database (Exchange is not stopped before the split). The split is assisted with the instant TimeFinder split behavior.
Snapshot Technologies	The TEIM uses TimeFinder as its default snapshot technology. To force a full TimeFinder establish, specify the <code>-full</code> option. To use multiple BCVs, specify the <code>-multi</code> option. To use the EMC Snap technology, specify the <code>-snap</code> option.
SRDF Controls	You can back up to devices on the remote Symmetrix in the device group over the SRDF link with the <code>-srdf</code> option. When using the <code>-srdf</code> option, you can also reject backing up the remote BCV using the <code>-nobrabcv</code> option.
TimeFinder Controls	You can control the TimeFinder split behavior by specifying <code>-instant</code> to cause an instant split on the BCV pairs or specify a hot split with the <code>-hot</code> option. Use the <code>-full</code> option to force a full establish on all BCVs on the local Symmetrix unit that are being used in the Exchange backup.
Transaction Log Management	When used with Exchange 2003 Server, the TEIM will not properly truncate the production server's transaction logs. The TEIM will display output that indicates that the transaction logs were truncated, but this is incorrect. Due to changes in the Exchange 2003 Server backup API, the TEIM log management process completes successfully, but does not actually truncate the transaction logs. The user will need to monitor and truncate these transaction logs on their own.
Test Mode	If you are tentative about running a backup command on a server (or particularly a command that involves multiple servers), you can specify the <code>-test</code> option that only validates and checks for proper command syntax, Enginuity and Exchange versions, etc. In test mode, the command will not execute any controls on devices or BCV devices in the database and not actually start the backup processes (such as establishing BCV pairs or dismounting devices). This option cannot be used with the <code>-c</code> (cluster) option.
Returns	The backup command returns a zero upon success or a non-zero value for various warnings and failures. A list of return codes can be found in <code>ExBackupErr2003.h</code> in the TEIM directory.

Backing Up Multiple Windows 2000/2003 Servers

Across a common network, you can backup multiple Windows 2000/2003 Servers working with Exchange 5.5, Exchange 2000, or SharePoint Portal databases using a single TEIM command from the backup server. Depending on what version of the server type, the backup command varies:

For Exchange 2000 and SharePoint Portal, the following TEIM command is used:

```
ExBackup2000 -f InitFile
```

For Exchange 2003, the following TEIM command is used:

```
ExBackup2003 -f InitFile
```

The command executes an initialization file that is formatted with separate backup commands which can target each of the production server node names you select with different backup parameters. If the file is in the TEIM working directory, you can specify an *.ini* file name with the *-f* option.

If you have an alternate directory from the working default, then specify a full path name with the *-f* option.

Although each backup can have its own output file, another output file can be specified with the *-o* option. This output file will contain all the general output from the *ExBackup2000* command.

For Exchange 5.5, the following TEIM command is used:

```
ExBackupCommander2 -f InitFile | -F InitPath
```

For Exchange 5.5 only, if you have an alternate directory from the working default, then specify a full path name with the *-F* option.

Note: There are other options with these commands. For more information, see Appendix A.

For more information about the command initialization file, see *Creating a Backup Command Initialization File* on page 5-15.

Creating a Backup Command Initialization File

The backup command file contains sets of commands directed to various servers across the network. The `ExBackup2000`, `ExBackup2003`, and `ExBackupCommander2` commands on Windows platforms kick off these command entries organized in sections. As shown in Figure 5-2 below and Figure 5-3 on page 5-16, each command section is headed by the name in brackets ([]) of the server being targeted. Each server command section is one backup command, but with various required and optional parameter entries to modify the command action.

```
[EXCHGNODE03]
cluster=FALSE
verbose=TRUE
restart_services=FALSE
sync_timeout=48

[EXCHGNODE04]
cluster=FALSE
verbose=FALSE
pause=TRUE
restart_services=TRUE

[EXCHGCLUS]
cluster=TRUE
verbose=TRUE
pause=FALSE
sync_timeout=60
services=c:\program files\emc\exbackup\exchgclus.ini
```

Figure 5-2 Sample Initialization File for Exchange 5.5

```
[EXCHANGE1]
Split=Hot
storagegroup=SG1
verbose=true
output=c:\program files\emc\resourcepak\teim\Exchange1.log

[EXCHANGE2]
Split=instant
multi=true
verbose=true
output=c:\program files\emc\resourcepak\teim\Exchange2.log
log_delete=false

[EXCHANGE3]
srdf=true
Split=hot
verbose=true
output=c:\program files\emc\resourcepak\teim\Exchange3.log
```

Figure 5-3 Sample Initialization File for Exchange 2000

File Commands

The following are possible command parameter entries for each backup command or server section in the init file:

`log_delete`

When set to TRUE, truncates the transaction logs. This parameter is optional. Possible values are TRUE and FALSE. The default is TRUE.

`output`

Specifies a program output file to record backup activity. This parameter is optional.

`symapidb`

Specifies an alternate WideSky SYMAPI database file when not using the WideSky default file name. This parameter is optional.

`verbose`

When set to TRUE, provides a more detailed, verbose output display. This parameter is optional. Possible values are TRUE and FALSE. The default is FALSE.

**Exchange 2000/2003
and SharePoint Only**

The following file commands are applicable to Exchange 2000/2003 and SharePoint Portal Servers only:

`sharepoint`

When set to TRUE, specifies that the production server is a SharePoint Portal Server type. This parameter is optional. The default is FALSE.

`split`

Specifies the type of split action required. Possible values are:

HOT— a hot split will be performed

INSTANT— an instant split will be performed

The default is to perform a normal offline split.

`srdf`

When set to TRUE, specifies that an SRDF backup will be performed. This parameter is optional. The default is FALSE.

`brbcv`

When set to FALSE and `srdf` is set to TRUE, the SRDF backup will not use the remote BCVs. This parameter is optional. The default value is TRUE.

`storagegroup`

Specifies a storage group name to be backed up. This parameter is optional. When using this option, all other storage groups are masked out of the backup operation.

`multi`

When set to TRUE, specifies that the TEIM should use multiple BCVs in a rotating fashion. This parameter is optional. The default is FALSE. When using this option, you must set it to the same value for each server in the file.

`full`

When set to TRUE, specifies that the TEIM should perform a full establish on all BCVs. This parameter is optional. The default is FALSE. When using this option, you must set it to the same value for each server in the file.

snap

When set to TRUE, specifies that the TEIM should use EMC Snap as the snapshot technology. This parameter is optional. The default is FALSE, which means that TimeFinder will be used. When using this option, you must set it to the same value for each server in the file.

Exchange 5.5 Only

The following file commands are applicable to Exchange 5.5 Servers only:

cluster

Specifies whether the target server is clustered or stand-alone. Possible values are:

- TRUE — a clustered server
- FALSE — a stand-alone server

services

Specifies an initialization file (just file name or full path name) that contains the services to stop/start (freeze) the backup operation on that server. This parameter is optional.

hotsplit

When set to true, specifies that a hot split will be performed in the backup operation, where the TEIM performs an online snapshot of the Exchange database (Exchange is not stopped before the split). The split is assisted with the instant TimeFinder split behavior. This parameter is optional. Possible values are TRUE and FALSE. The default is FALSE.

restart_services

When set to TRUE, specifies that the backup services are restarted when this backup command fails. This parameter is optional. Possible values are TRUE and FALSE. The default is TRUE.

pause

When set to TRUE, specifies a pause action at the end of the backup operation that keeps the console window open. This parameter is optional. Possible values are TRUE and FALSE.

sync_timeout

Specifies a timeout period for backup operation if other than the default value of 100 minutes. This parameter is optional.

Creating a Services Initialization File

The services initialization file specifies various Microsoft services to freeze (stop and restart) during the critical backup processes. In the backup commands, the file is specified by a `-f` or `-F` option.

The services initialization file consists of two sections, **StopServices** and **StartServices**. These section headings are designated with surrounding brackets (`[]`) and built with a specific program format:

- ◆ The services must be listed in the exact order that you would like to stop and restart them.
- ◆ Each service entry is assigned a number according to its spot in the list. Assigned numbers must be in order without skipping or duplicating any of them.
- ◆ The two sections are completely independent from one another so that you can stop and start different services if necessary.

Any failure in the running of a service because of its own dependencies can cause the backup command to fail. Figure 5-4 below and Figure 5-5 on page 5-20 offer recommended examples of typical services to enter in the initialization files for the TEIM backup commands. File names should have a `.ini` file extension.

```
[StopServices]
1=MS Mail Connector Interchange
2=Microsoft Exchange Message Transfer Agent
3=Microsoft Exchange Event Service
4=Microsoft Exchange Information Store
5=Microsoft Exchange Directory Synchronization
6=Microsoft Exchange Directory
7=Microsoft Exchange System Attendant

[StartServices]
1=Microsoft Exchange System Attendant
2=Microsoft Exchange Directory
3=Microsoft Exchange Directory Synchronization
4=Microsoft Exchange Information Store
5=Microsoft Exchange Event Service
6=Microsoft Exchange Message Transfer Agent
7=MS Mail Connector Interchange
```

Figure 5-4 Initialization File for a Clustered Exchange 5.5 Server

```
[StopServices]
1=msexchangemta
2=NAVEExchange
3=msexchangeis
4=msexchangeds
5=msexchangesa

[StartServices]
1=msexchangesa
2=msexchangeds
3=msexchangeis
4=NAVEExchange
5=msexchangemta
```

Figure 5-5 Initialization File for a Stand-Alone Exchange 5.5 Server

If neither the `-f` or `-F` option is supplied, the following services and resources are assumed:

- ◆ Microsoft Exchange System Attendant (msexchangesa)
- ◆ Microsoft Exchange Directory Service (msexchangesa)
- ◆ Microsoft Exchange Information Store (msexchangesa)
- ◆ Microsoft Exchange Message Transfer Agent (msexchangesa)

Note: If the `-hot` option is also specified in backup command, the TEIM performs a hot split where an online snapshot is executed without stopping any services in the StopServices list.

Restore Procedures

Restore procedures vary depending on your Windows environment.

Exchange 5.5 Database Restore

The restore and recovery procedures for TimeFinder backups of a Microsoft Exchange Server 5.5 are explained in detail in the *EMC TimeFinder Integration for Microsoft Exchange Server 5.5* white paper.

Exchange 2000/2003 Database Restore of an Offline Split

The restore and recovery procedures for TimeFinder backups of a Microsoft Exchange 2000/2003 Server are explained in detail in the *EMC TimeFinder Integration for Microsoft Exchange 2000* white paper.

Exchange 2000/2003 Single Mailbox Recovery From an Offline Split

The single mailbox recovery procedure for Microsoft Exchange 2000/2003 Server is explained in detail in the *Mailbox Recovery for Microsoft Exchange 2000 Server* white paper.

A special dual-boot configuration is required for running the TEIM on a backup server where Microsoft Exchange 2000 single mailbox recoveries will take place. For more information, see Chapter 4.

Exchange 2000/2003 Hot Split Database Restore With Transaction Log Replay

This section highlights the steps necessary to perform a full Exchange 2000/2003 Server database restore with transaction log replay, using the Hot Split BCV backup copy. Typically, you would perform a full database restore when one or more production databases have failed.

In the following example, it is assumed that the production server database has failed, and has been dismounted from the specific storage group.

The BCV copy of the database will be preserved by splitting the BCV from the standard volume prior to initiating a production server transaction log recovery.

Note: During the Solutions Enabler TimeFinder restore operation for the specific database, all the remaining databases in the storage group remain mounted and available for access to the enterprise. But these databases will need to be dismounted in order to initiate the transaction log recovery.

To perform a full Exchange 2000/2003 Server database restore with transaction log replay, using a Hot Split BCV backup, complete the following steps:

1. Using SIU, dismount the BCV from the backup/recovery server.
2. Using SIU, dismount the standard volume from the production server.



CAUTION

Only dismount with SIU (`symmtctl umount -drive`) for both the BCV from the backup/recovery server and the standard volume from the production server. Do not use `mountvol` or other utilities (SIU has built-in knowledge of the establish process). Using non-SIU commands to dismount these volumes could result in corruption being transferred to either the standard or BCV volume data.

3. Using TimeFinder, perform a restore operation of the BCV (including the split of the BCV); or using EMC Snap, perform a restore of the VDEV.
4. Using SIU, mount the BCV on the backup/recovery server.
5. Using SIU, mount the standard volume on the production server.
6. Perform transaction log verification on the production host.
7. Dismount all of the Exchange databases in the storage group.
8. Rename the storage group checkpoint file.
9. Remount the Exchange databases in the storage group.

TimeFinder Restore of the Hot Split BCV

There are no exact TEIM guidelines for TimeFinder device group creation and there is no single set of commands that will complete the restore operation for all setups.

In the following example, it is assumed that a TimeFinder device group exists for each storage group, and the TimeFinder device group is named `sg1`. This restore example is for a single database in a storage group. In this situation, restoring the entire TimeFinder device group is not possible, since a single device within that TimeFinder device group needs to be restored. To restore the database that resides on DEV001 in device group `sg1`, enter TimeFinder command:

```
symmir -g sg1 restore dev DEV001
```

This command performs an incremental restore operation on just the tracks that have changed. The changed tracks will be copied back to the standard volume.

The restore operation can be monitored revealing status, using the following command:

```
symmir -g sg1 query
```

Once the copying of data from the BCV to the standard volume is complete and the BCV state is shown as *Restored*, the BCV can be split from the standard volume with the following command:

```
symmir -g sg1 split
```

Again, query the TimeFinder device group and check that the BCV state is now *Split*.

Remount Devices

Remount both the BCV to the backup/recovery server and the standard volume to the production server, using the following SIU command:

```
symntctl mount -drive n -vol HarddiskVolume9
```

You must use SIU to perform this mount; otherwise the volumes will be locked and all access will be denied.

It is also possible to mount the volumes using their GUID rather than their volume name.

Snap Restore of the Hot Split BCV

Once again, it is assumed that the current device group is named `sg1`, and the desire is to restore a single database that resides on `DEV001` of that device group.

First, to view the Snap session that currently exist for the standard device that needs to be restore, use:

```
symsnap -g sg1 query -multi
```

At this point, choose the VDEV that you would like to restore onto `DEV001`. In this example, we will assume that we want to restore `VDEV001` to `DEV001`. To initiate the restore operation, use:

```
symsnap -g sg1 restore DEV001 VDEV 1d VDEV001
```

To monitor the status of the restore operation, use:

```
symsnap -g sg1 query
```

Once the restore is complete, the state of the Snap session will be *Restored*. At this point, you should terminate the Snap session with the following:

```
symsnap -g sg1 terminate DEV001 VDEV 1d VDEV001
```

Now, the standard device has been brought back to the point in time of the backup. Note that the VDEV is no longer a valid snapshot of the standard device.

Transaction Log Verification

The transaction log verification process ensures that the production server has all the transaction logs necessary to complete recovery. This process involves identifying the Exchange 2000 *required logs*. The required logs are required in order to make the database logically consistent. Log verification is accomplished using the Exchange 2000 Server utility **eseutil.exe**. This utility extracts header information so that the log generations (`lGeneration`) can be identified.

To perform transaction log verification, perform the following steps:

1. Identify the *required logs* in a File Dump for the newly restored database by executing the following command:

```
eseutil /mh S:\exchsrvr\mdbdata\priv.edb
```

Obviously the database path will vary for different configurations. Because this is a hot split operation, the state of the database is properly reported as *Dirty Shutdown*.

Note: For Exchange 2000 without Service Pack 2, the state after a hot split will show as `Inconsistent` instead of `Dirty Shutdown`.

The field of most interest in the File Dump is the **Log Required** field. As shown in Figure 5-6 on page 5-26, this field shows a range of numbers indicating the range of transaction logs that are required for recovery. Note that the numbers in this range are decimal (for example 2184-2185), while the actual transaction log numbers are identified as hexadecimal in their file name, using the following form:

`E0000n.log`

As shown in Figure 5-6 on page 5-26, the first number in the **Log Required** field was identified as 2184, yet the corresponding transaction log file name is `E0000888.log`. (The decimal number 2184 translates to 888 in hexadecimal.)



```

TEIM CLI
J:\>eseutil /mh priv1.edb

Microsoft(R) Exchange Server(TM) Database Utilities
Version 6.0
Copyright (C) Microsoft Corporation 1991-2000. All Rights Reserved.

Initiating FILE DUMP mode...
Database: priv1.edb

File Type: Database
Format ulMagic: 0x89abcdef
Engine ulMagic: 0x89abcdef
Format ulVersion: 0x620,9
Engine ulVersion: 0x620,9
Created ulVersion: 0x620,9
DB Signature: Create time:01/02/2003 07:49:18 Rand:754006393 Computer:
cbDbPage: 4096
dbtime: 12463248 (0-12463248)
State: Dirty Shutdown
Log Required: 2184-2185
Streaming File: Yes
Shadowed: Yes
Last Objid: 43662
Scrub Dbtime: 0 (0-0)
Scrub Date: 00/00/1900 00:00:00
Repair Count: 0
Repair Date: 00/00/1900 00:00:00
Last Consistent: (0x885,D00,15D) 01/29/2003 15:09:58
Last Attach: (0x886,E,163) 01/29/2003 15:31:37
Last Detach: (0x0,0,0) 00/00/1900 00:00:00
Dbid: 1
Log Signature: Create time:01/02/2003 07:49:13 Rand:753995979 Computer:
OS Version: (5.0.2195 SP 3)

Previous Full Backup:
Log Gen: 0-2183 (0x0-0x887)
Mark: (0x2F,0,0)
Mark: 00/00/1900 00:00:00

Current Incremental Backup:
Log Gen: 0-0 (0x0-0x0)
Mark: (0x0,0,0)
Mark: 00/00/1900 00:00:00

Current Full Backup:
Log Gen: 0-0 (0x0-0x0)
Mark: (0x0,0,0)
Mark: 00/00/1900 00:00:00

Current snapshot backup:
Log Gen: 0-0 (0x0-0x0)
Mark: (0x0,0,0)
Mark: 00/00/1900 00:00:00

cpgUpgrade55Format: 0
cpgUpgradeFreePages: 0
cpgUpgradeSpaceMapPages: 0

Operation completed successfully in 1.62 seconds.

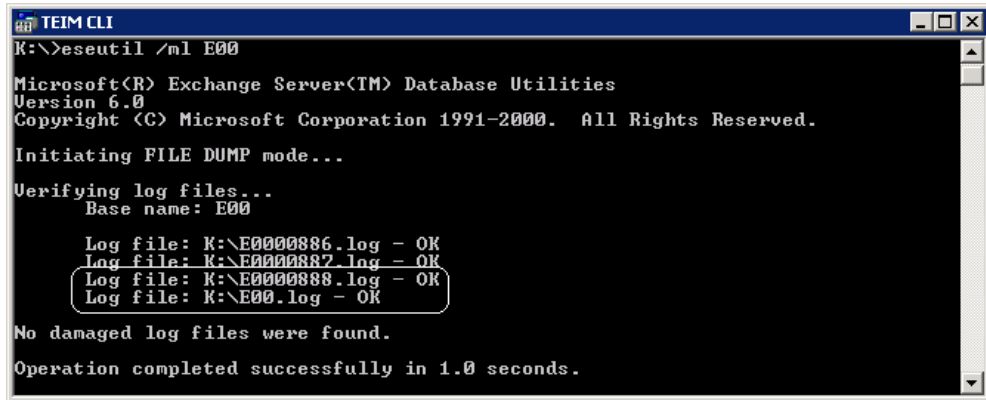
```

Figure 5-6 File Dump Sample for Log Required

2. Verify that the *required logs* are present in the transaction log directory, and that all transaction logs are sequential, by running the following command from the transaction log directory:

```
eseutil /ml E0n
```

Figure 5-7 is a sample output showing the transaction log listings in the hexadecimal format.



```

TEIM CLI
K:\>eseutil /ml E00

Microsoft(R) Exchange Server(TM) Database Utilities
Version 6.0
Copyright (C) Microsoft Corporation 1991-2000. All Rights Reserved.

Initiating FILE DUMP mode...

Verifying log files...
  Base name: E00
    Log file: K:\E00000886.log - OK
    Log file: K:\E00000887.log - OK
    Log file: K:\E00000888.log - OK
    Log file: K:\E00.log - OK

No damaged log files were found.
Operation completed successfully in 1.0 seconds.
  
```

Figure 5-7 Transaction Log Listing

The $E0n$ value is the log prefix for the particular storage group where the restore is taking place. This value is $E00$ for the first storage group on the server, $E01$ for the second storage group, $E02$ for the third storage group, and $E03$ for the fourth storage group. This value can be programmatically determined by opening the Exchange System Manager, selecting properties on the given storage group, and identifying the *Log file prefix* value.

First verify that this command reports that no damaged log files were found. Then verify that the *required logs* are all shown in the list of transaction logs (see Figure 5-7). Finally, verify that all transaction logs shown in the output are sequential (that is, no transaction log generations are missing).

If any of the above steps failed, then you will need to restore some log files from the backup in order to complete the restore.

Dismount Databases in Storage Group

Up to this point, the database being restored was dismounted, but all of the other databases on the production server were mounted and servicing users. Now, all of the databases in the storage group where the restore is taking place must be dismounted. Note that only the one storage group where the restore is occurring needs to be dismounted, not all storage groups.

All databases in this storage group need to be dismounted because these databases all share the same set of logs. So if transaction log

replay is going to be necessary on any one database in the storage group, all databases will need to be offline.

Using the Exchange System Manager, dismount all of the databases in this storage group.

Renaming the Storage Group Checkpoint File

Prior to mounting the databases in the storage group to initiate transaction log replay, the current checkpoint file (E0n.chk) must be renamed, or deleted. Renaming the checkpoint file is essential for a full recovery of the Exchange 2000 Server database. The checkpoint file is found in the system file path for the storage group. This path can be found by opening Exchange System Manager, selecting properties for the storage group, and noting the *System path location* value. The checkpoint file must not exist in the specified Exchange 2000 Server system path in order for transaction log replay to occur. Either delete this checkpoint file or rename it to anything other than its original E0n.chk name.

Note: Each storage group will have a unique system path and checkpoint file. Ensure that the correct checkpoint file is renamed or moved.

Remounting Exchange Databases in the Storage Group

Once the checkpoint file is deleted or renamed, all of the databases in the targeted storage group may be remounted in order begin the transaction log recovery process. The first database in the storage group to be mounted will begin the transaction log replay. It is not necessary that the restored database be the first database mounted; any of the databases in the storage group can be mounted first. Once the Exchange 2000 Server database engine (ESE98) begins to replay the logs, you can use the Windows 2000 Server Event Viewer to monitor the recovery process. The first database to be mounted will take the longest time since the transaction log replay will be occurring. The other databases in the storage group will be much faster to mount since the transaction log replay will have already completed.

Single Mailbox Recovery Using a Hot Split Database

This section highlights additional recovery setup considerations and tasks when a Hot Split database is in use.

A single mailbox recovery using a Hot Split Database is nearly identical to that for an offline split database. Therefore, follow the exact steps and procedures outlined in Microsoft's Mailbox Recovery for Microsoft Exchange 2000 Server white paper. This white paper can be found at:

www.microsoft.com/exchange/techinfo/administration/2000/MailboxRecover.asp

When using a Hot Split database to perform a single mailbox recovery, you must consider and perform the following tasks:

1. Perform the dual-boot mailbox recovery procedures described in *Dual-Boot for Single Mailbox Recoveries* on page 4-38.
2. When Hot Splits are being used, it is required to setup the production server so that all checkpoint files are located on the standard volumes, and subsequently copied to the BCVs. Therefore, these checkpoint files will be available to the backup server (for the sole purpose of the single mailbox recovery). The backup server must be configured to use the checkpoint files that originated from the production server, and now reside on the BCV, otherwise the single mailbox recovery process will fail.

Ensure that the **System file location** for the storage group on the backup server where the single mailbox recovery is taking place is set to point to the location of the checkpoint file on the BCV. The "System file location" can be changed by opening the Exchange System manager on the backup server, selecting **Properties** on the storage group, and browsing to the path for the "System file location." Failure to make this change will cause an Exchange error report that identifies the database as *inconsistent* when you attempt to mount it on the backup server.

3. The storage groups on the backup server must be configured exactly as they are on the production server. In particular, the order of the storage groups must be the same, due to the reliance on transaction log prefixes (which is determined by the order of storage groups). For example, assume that the storage group named "Executive SG" is the 2nd storage group on the production server. This would mean that the transaction log

prefix for all transaction logs in the “Executive SG” would be E01. Therefore, when the backup server is configured for single mailbox recoveries, the “Executive SG” must be the 2nd storage group on the backup server so that it will keep its transaction log prefix of E01. If “Executive SG” is configured as 1st, 3rd, or 4th storage group on the backup server, the transaction log prefix becomes different and the databases in that storage group will fail to mount.

4. All databases in the storage group must be accessible in order to perform a single mailbox recovery for any one database in that storage group. For example, assume that the storage group has 4 databases, and you are performing a single mailbox recovery from the 1st database in that storage group. All four of those databases must be present in order for the single mailbox recovery to work. In addition, the paths to all 4 databases must be identical (including the drive letters) on the backup server to what they were on the production server. This is because the database paths are hard-coded in the database headers.

Exchange 2000/2003 Database Restore From a Remote Site

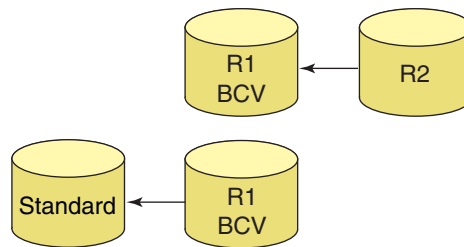
The flexibility of an SRDF Exchange storage environment that was established by the TEIM, offers the following SRDF restore and restart procedures:

- ◆ Restoring from the R2 to the Production server on the local Symmetrix.
- ◆ Restoring from the remote BCV to the Production server on the local Symmetrix.

Restoring Data From the R2

To restore the Exchange data from the R2 location, you can do two TimeFinder operations (shown in Figure 5-8):

1. Restore from the R2 to the R1/BCV.
2. Restore from the R1/BCV to the standard.



RP-000010

Figure 5-8 Restoring Data From the R2

To restore the R1/BCV from the R2:

1. From the TEIM server, unmount the R1BCVs by removing the drive letter assignment in Disk Administrator.
2. Open a command prompt.
3. Verify that the R1BCV and the R2 are in a split state:

```
symrdf -g DgName query -bcv
```

4. Restore the R2 to the R1BCV:

```
symrdf -g DgName restore -bcv
```

5. Verify the status:

```
symrdf -g DgName query -bcv
```

6. Once the status shows restored, split the pair:

```
symrdf -g DgName split -bcv
```

7. Verify the connection state:

```
symrdf -g DgName query -bcv
```

If the device groups that were created contain both the database volumes and the transaction log volumes, care must be taken during the restore procedures. By running the restore commands on the device group level, both the logs and the databases can be overwritten. To avoid this, specify a device number within the command. For example, to restore logical device number 001 in the device group, *sglrdf*, enter the following:

```
symrdf -g sglrdf restore DEV001 -bcv
```

To restore the standard from the R1/BCV:

1. Make sure that the volumes have been dismounted on the Production server.
2. Restore the BCV:

```
symmir -g DgName restore dev <dev#>
```

3. Verify the status:

```
symmir -g DgName query
```

4. Split the pair:

```
symmir -g DgName split
```

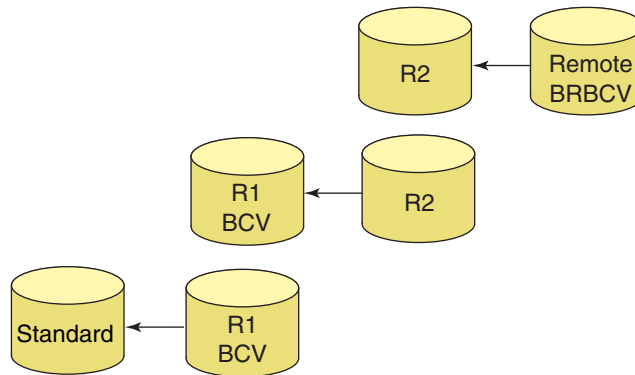
5. Verify connection state:

```
symmir -g DgName query
```

Restoring Data From the Remote BCV

To restore the Exchange data from the remote BCV device, you can do the following three TimeFinder operations (shown in Figure 5-9):

1. Restore the data from the remote BRBCV to the R2 mirror.
2. Restore the R2 to the R1/BCV mirror.
3. Restore from the R1/BCV mirror to the standard.



RP-000011

Figure 5-9 Restoring Data From the Remote BCV

To restore (in turn) the R2 mirror from the Remote BRBCV, the R1/BCV from the R2 mirror, and the standard from the R1/BCV:

1. Verify that the BRBCV and the R2 are in a split state.
2. Restore the BRBCV to the R2:


```
symmir -g DgName restore -rdf -bcv
```
3. Verify the status:


```
symmir -g DgName query -rdf -bcv
```
4. Once the status shows restored, split the pair:


```
symmir -g DgName split -rdf -bcv
```
5. Verify the connection state:


```
symmir -g DgName query -rdf -bcv
```
6. Restore the data from the R2 mirror to the R1/BCV, refer to page 5-31.
7. Restore the R1/BCV to the standard device, refer to page 5-32.

Troubleshooting

The following table lists and describes some typical errors (with possible cause and action) that can occur in a Windows Exchange environment.

Table 5-6 Troubleshooting an Exchange 2000 Server Operation

Error Code	Error String	Cause	Action
18	"Failed to create a handle to \\?\Volume{6de534a0-8adf-11d6-bd71-00d0b7081386}.	The TEIM is being run from a Terminal Services session.	If remote access is necessary, use a true console emulator such as VNC, RemotelyAnywhere, or PCAnywhere.
265	ERROR = The process cannot access the file because another process has locked a portion of the file." "Failed to mount \Device\HarddiskVolume3 at E:\ on API1102. ERROR = Cannot create a file when that file already exists."		
48	"Failed to initialize SYMAPI session on API1100. ERROR = The remote connection is refused. The symapi server is probably not running."	The symapi service (symapisrv) is not installed or started on the production server.	Install and start symapisrv. Installing WideSky Solutions Enabler will prompt the installer to install and start the symapi service.
52	"Failed to get information for device on API1102. ERROR = The Symmetrix ID is not known."	A database or set of logs is not stored on the Symmetrix with a BCV.	Review all database and log paths to ensure that they are pointing to a Symmetrix disk which has a BCV.
92	"Failed to find the target volume name for the M:\ mount point. ERROR = The device is not connected."	Exchange IFS (M:\) drive not fully dismounted from backup server.	To fully dismount the m: drive, open a command window and make the entry: subst m: /d
104	"Failed to construct an ExServer object with name Shyexclus2. ERROR = Failed to create an ExStorageGroup object."	The local language for the backup server is different from that of the production server.	Change the local language of the backup server to match the production server.
112	"Call to CoCreateInstance failed for the class ExchangeServer. ERROR = Class not registered."	Exchange 2000 not installed on backup server.	Install Exchange 2000 on backup server.
138	"Circular logging is currently enabled for the SG2 storage group. Please disable circular logging on all storage groups before running TEIM."	Circular logging is enabled on production server.	Disable circular logging and reboot production server (or restart the Exchange services).

Table 5-6 Troubleshooting an Exchange 2000 Server Operation (continued)

Error Code	Error String	Cause	Action
306	"There is nothing to backup on <i>ServerName</i> ."	All public and mailbox stores on the Exchange 2000 server are dismounted.	Remount any stores that you would like to backup.
323	"ESEUTIL failed to verify the consistency of F:\SG2PrivA.edb. ERROR = 4294967295."	Version of ESEUTIL.exe is too old and does not have the checksum (-k) options.	Upgrade to Exchange with 2000 Service Pack 1 or greater.
408	"Failed to load esebcli2.dll on API1102. ERROR = The specified module could not be found."	The Exchange bin directory is not in the system path. This is a result of installing the TEIM before Exchange 2000 on the backup server.	Manually add the Exchange bin path to the system path. Or re-install the TEIM after Exchange 2000 has been installed on the backup server.
904	"Error Msg: Event ID 904, Category: Callback, Source: ESE Backup, Description: Information Store (2136) Callback function call ErrESECBGetDatabasesInfo ended with error 0x8004010F."	The fully qualified domain name (FQDN) is being passed to the TEIM instead of the NetBIOS name.	Pass the NetBIOS name to the TEIM. For Example, use Exch1 rather than Exch1.emc.com. Or, Install hotfix Q314606.

TSIM Overview and Setup

This chapter provides a brief description of the EMC TimeFinder-SQL Server Integration Module (TSIM) and related software that manage the Microsoft SQL Server environment. The chapter also describes the complete setup of an SQL Server enterprise business continuance environment.

- ◆ Overview 6-2
- ◆ Setting Up an SQL Server Storage Environment..... 6-8
- ◆ Setting Up the Production Server Storage With Local BCV 6-10
- ◆ Setting Up the Production Server Storage With Concurrent BCV 6-12
- ◆ Setting Up the Production Server Storage in SRDF 6-14
- ◆ Setting Up the Standby Server Storage With Local BCV..... 6-15
- ◆ Setting Up the Standby Server Storage (Remote BCV Side)..... 6-17
- ◆ Setting Up the Production Server Storage With Snap Devices . 6-18
- ◆ Configuring Windows Server Disks..... 6-20

Overview

The TimeFinder-SQL Server Integration Module (TSIM) provides a comprehensive backup and recovery management interface specifically for Windows servers that support Microsoft SQL Server databases. The TSIM integrates and collectively automates the command actions and behavioral features of EMC TimeFinder, SRDF, and the tools supplied with Microsoft SQL Server 2000 products.

The TSIM provides a command line interface that you can use to back up and restore SQL databases, using both the Microsoft *Virtual Device Interface* (VDI) and the database *snapshot* functionality. The TSIM provides an integrated method for quickly creating point-in-time database copies that can be used for decision support systems or database maintenance. The TSIM also provides a database backup that can be quickly restored in disaster-recovery scenarios.

The TSIM further enhances the availability of the database to mission critical applications. The TSIM can be used to greatly reduce backup and restore times and, in conjunction with typical database administration tasks, provide a more stable and available production database platform.

To use the TSIM, you should have experience using TimeFinder and SRDF CLIs, and SQL Server-based commands. You should also have a working knowledge of SQL Server 2000 backup and recovery methodologies.

For SQL Server databases managed by the TSIM, you can:

- ◆ Back up either a database, multiple databases, or a specified database filegroup. The TSIM provides a near instantaneous point-in-time back up of the production database/filegroup or multiple database(s) from a single instance of SQL Server, with little impact on your application (by hot splitting TimeFinder local or remote BCV or RDF devices, or activating a virtual copy session with snap devices).
- ◆ Integrate EMC and Microsoft solutions to fast restore a database from the BCV and allow transaction backups from the production server to roll forward on the restored database in case of disaster recovery.
- ◆ Restore either a single database, multiple databases, or a specified database filegroup for a disaster recovery situation.
- ◆ Restore a standby database with the new location.

- ◆ Create a near instantaneous standby database that can be used for decision support and a transactionally consistent way to update a database guarding against logical corruption.

Requirements

The various TSIM backup and restore commands target different combinations and versions of the Microsoft Windows operating system and the SQL Server versions. The TSIM commands integrate with and support the following environments:

- ◆ SQL Server 2000 Enterprise Edition on Windows 2000, Windows 2000 Datacenter Server, or Windows 2003 Server
- ◆ Stand-alone or clustered servers using Microsoft Cluster Services (MSCS)
- ◆ EMC WideSky TimeFinder, SRDF, and SIU command line environments

The TSIM requires the Symmetrix Enginuity version to be 5x65 or greater. To use the instant or hot split features, the Symmetrix Enginuity versions must be at least 5x66 or 5x67. Note that for 5x68 versions and greater, the instant split behavior is the default mode.

When your SQL Server databases have dynamic disks on your server, VERITAS Volume Manager (VxVM) V 2.5 is required. For more information, see *Volume Management Software* on page 3-3.

Business Continuity Storage Environment

The Symmetrix business continuance storage environment for the SQL database is based on the integration of the TSIM with TimeFinder, SRDF, and Snap technologies.

EMC TimeFinder

EMC TimeFinder works by creating multiple, independently addressable online Business Continuity Volumes (BCVs) for information storage (Figure 6-1 on page 6-4). Each BCV is a Symmetrix device and configured as a single mirror which independently supports host applications.

BCVs, created as mirror images of active production volumes, give you another source of data with which to work. This is ideal for backup and recovery, as well as offline operations. The principal Symmetric device, known as the standard device, remains online for regular Symmetrix operation so no interruption of service with the original production server occurs.

Each BCV contains a unique host address making it accessible to a separate backup/recovery server.

A business continuance sequence first involves setting, or establishing, the BCV device as a mirror of a standard Symmetrix device, making the BCV device temporarily inaccessible through its original device address. The BCV device may later be separated, or *split*, from the standard Symmetrix device with which it was previously established. The split BCV device has valid data, and is available for backup or other host processes through its original device address.

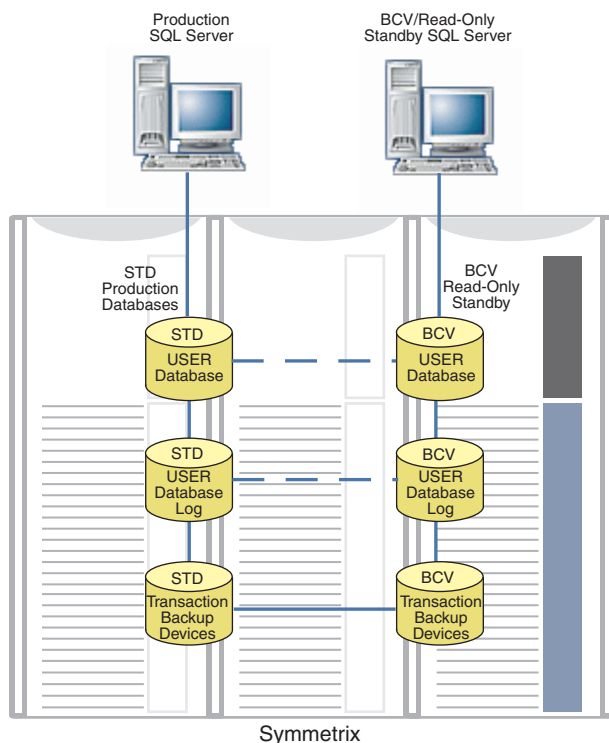


Figure 6-1 SQL Enterprise Storage Business Continuance System

SRDF Symmetrix Remote Data Facility (SRDF) provides a disaster tolerant business continuance environment. SRDF with the TSIM allows for the recovery from local database corruption and local site disasters as well as restart capabilities from the remote site.

With the TSIM integrating your SQL Server with both TimeFinder and SRDF, you can recover from any disaster. You can also restart the SQL Server database at the remote location in the event something happened to the production site. For more information about BCV mirroring configurations in an SRDF environment, see *SRDF BCV Mirroring* on page 4-6.

EMC Snap EMC Snap allows you to create virtual copy sessions between a source device and multiple *virtual* (VDEV) target devices. The source device can be either a standard device or a BCV device. The target device(s) must be virtual device(s).

EMC Snap is useful in situations where multiple copies of production data are needed for testing, backups or report generation. It can also be used to reduce disk contention and improve data access speed, by assigning users to copies of data rather than accessing the one production copy.

EMC Snap functionality is controlled via copy sessions, which pair the source and target devices. Sessions are maintained on the Symmetrix unit and can be queried to verify the current state of the devices. A copy session must first be created and then activated for the target virtual devices to become accessible to its host. When the information is no longer needed, the session can be terminated.

SQL Server Snapshots

SQL Server contains a Virtual Device Interface (VDI) that allows for snapshot backups. It provides a high-performance alternative to using named pipes for backups. Creating an SQL Server snapshot of a database enables you to roll forward transactions from a transaction backup device to a separate instance. An original standard host instance that has been restored from TimeFinder BCVs can also be rolled forward. You can use the BCV copy for backup or for a near-instantaneous creation of a standby database.

In SQL Server 2000, information provided in VDI metadata can be used to restore a database from existing files created by TimeFinder. Using SQL Server with TimeFinder, a standby database can be created in seconds, where it may take hours for very large databases without the integration of TimeFinder technologies.

Standby Database

A standby database is an exact copy of a production database that can be brought online in the event the Standard production host or SQL Server fails. It can also be used as a reporting server for decision support. The read-only, standby database is created by performing a snapshot backup of the database on the Standard host and a snapshot restore from the BCV host.

The normal operation is read only, but it is possible to have a read/write standby database for restoring.

Periodically, transaction log backups from the production Standard server are applied to the BCV standby database to ensure that the standby remains up-to-date with the Standard production server. In the event of a production database or server failure, one or more of the databases on the standby server are made available to the user process.

You can also combine EMC TimeFinder with the new SQL Server 2000 standby feature as a tool for updating a standby database without impacting production. The transaction log on the standard host is backed up to a BCV paired device and synchronized periodically to the BCV host. The database server on the BCV side applies those transaction logs to the standby database. The standby server can be updated after every transaction backup, or as needed.

You may choose to keep the second standby server hours behind, in case of logical corruption or operator error, with the knowledge that in the event of disaster, the logs are physically on the backup device and available for application. The standby server may also be used for read-only operations. This allows the database to be used for decision-support queries or DBCC checks.

Disaster Recovery Backup

A copy of the database files created on BCVs is split from the production database and retained as a disaster recovery backup. The point-in-time database copy created by a TSIM backup action can be used to restore a production database using a TSIM restore action.

If the production database fails, but the server is still available, a TSIM restore command is issued from the standard host to allow the BCV copy to replace the corrupt database and allow transactions to be replayed to a known point-in-time.

Long Duration Locks

To protect TSIM target devices from being used by other applications, the TSIM uses WideSky long duration locks. Once a device is locked, it is not available to other applications.

To use the long duration locks, use the `-lock` option. To list the locks held by the TSIM, use `-lock list`. To release a lock, use `-lock release`.

Once the TSIM locks a device, any manual operation to establish/split/restore TimeFinder or virtual snap devices should use `-preservetgtlock -lockid LockID`.

Concurrent BCVs

The TSIM supports concurrent BCVs to provide two sets of point-in-time production database backups using concurrent BCV split. To use this feature, establish two concurrent BCV pairs before running `tsimsnap/tsimsnap2 backup`. The TSIM will automatically detect and use the concurrent BCVs. Be sure to verify the concurrent BCV pair and establish all devices used by the database(s) with concurrent BCVs; otherwise, `tsimsnap/tsimsnap2 backup` will only backup the database with a single set of BCVs.

Setting Up an SQL Server Storage Environment

The following sections describe how to setup an SQL Server business continuance environment, involving the various production and standby servers. The environment setup includes certain setup requirements for the volume configurations, plus the Windows operating systems, SQL Server software, and the EMC WideSky software in the server system. The proper operation of the WideSky TSIM backup/restore interface is dependent on the resulting configuration.

Figure 6-2 illustrates an SQL Server storage environment that incorporates a local site connected to the remote site through an SRDF link. Both production and standby server storage environments need to be setup.

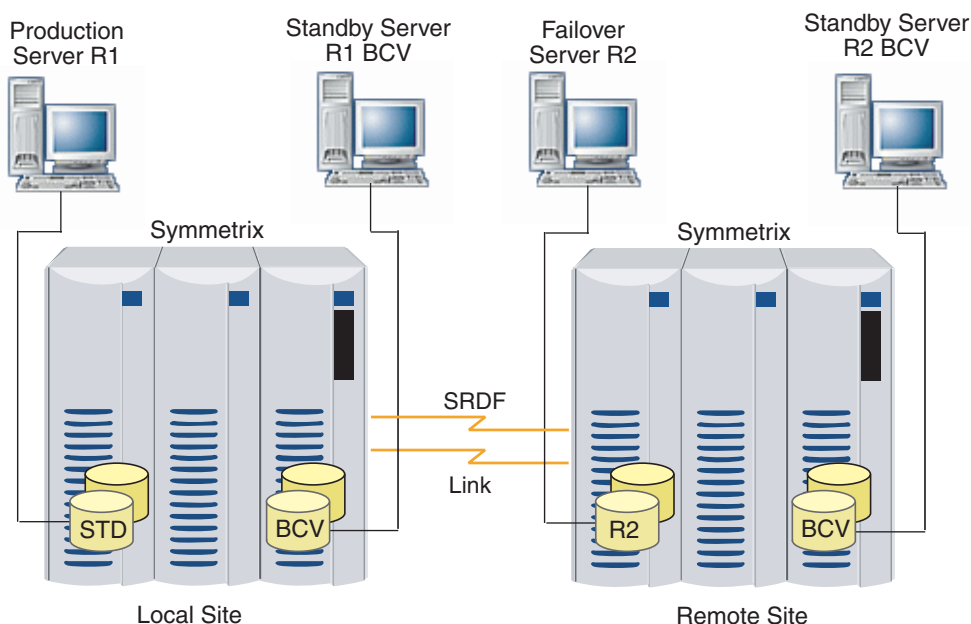


Figure 6-2 SQL Server Business Continuance Environment

The following setup procedures use MS-DOS, TimeFinder and SRDF SYMCLI, and SIU commands. Separate setup procedures target the:

- ◆ Production server storage
- ◆ Backup or Standby server storage
- ◆ Storage for both production and standby servers

Symmetrix storage must be configured with TimeFinder BCV devices of the appropriate type, size, and internal location to mirror the SQL Server storage and log devices that you intend to backup and restore. Ensure the SYMCLI environment is enabled. If not, run `symlmf` and enter the WideSky licensing keys for Base, and TimeFinder. If you are using remote BCV or RDF devices, enter the additional license key for SRDF.

Environment Variable Convenience

For ease of use, add the environment variable `C:\Program Files\EMC\WideSky\bin` to the path in the Environment settings on all hosts.

For Windows systems, open **Computer Management**, right-click **Computer Management (local)**, and select **Properties**. Click the **Advanced** tab, click **Environment Variables**, and add `C:\Program Files\EMC\WideSky\bin` to the path variable.

Drive Letter Designations

Use Windows Computer Management to make sure that all the drive letters are set correctly.

The recommended setting for the CD-ROM is the Z:\ drive.

Transaction Log Considerations

It is often the case that the SQL transaction logs are placed on a Windows volume set and the SQL databases are placed on Windows stripe sets (without parity). Although it is not required, separating the transaction log volume from the database volume has its benefits. Transaction logs are written sequentially while the database is a random read/write I/O. Therefore, isolating the volumes improves performance and fault tolerance, while enhancing recoverability. Moreover, a separate backup device for the transaction log enables you to update a standby database.

Setting Up the Production Server Storage With Local BCV

Perform the following steps to setup the SQL backup or standby server storage on the local Symmetrix (BCV) side:

1. Create a group with the same name that was used for the production server with the following SYMCLI base command:

```
symdg create DgName -type GroupType
```

where:

GroupType is either REGULAR, RDF1, or RDF2, as in the example:

```
symdg create sqadg1 -type REGULAR
```

2. Verify the creation of the group by entering one of the following commands:

```
symdg list
symdg show DgName
```

3. Add devices to the new group:

```
symld -g DgName add pd PdevName [LdevName]
```

Repeat for each device. The default logical device name (*LdevName*) is Dev### unless assigned in the command, for example:

```
symld -g sqadg1 add pd PHYSICALDRIVE2 DriveE
```

4. Associate BCV devices with the group:

```
symbcv -g DgName associate dev SymDevName [LdevName]
```

Repeat for each device. The default logical device name (*LdevName*) is BCV###, unless assigned in the command:

```
symbcv -g sqadg1 associate dev 061 BCVdriveE
```

5. Verify that all devices have been created correctly:

```
symdg show DgName
```

For example:

```
symdg show sqadg1
```

6. Synchronize the BCV devices by using the following SYMCLI TimeFinder component command:

```
symmir -g DgName -full establish [LdevName]
```

7. View the status by performing a TimeFinder query:

```
symmir -g DgName query
```

Once all devices are synchronized, you can now run a TSIM backup command.

Setting Up the Production Server Storage With Concurrent BCV

Perform the following steps to setup the SQL backup or standby server storage on the local Symmetrix (BCV) side:

1. Create a group with the same name that was used for the production server with the following SYMCLI base command:

```
symdg create DgName -type GroupType
```

where:

GroupType is either REGULAR, RDF1, or RDF2, as in the example:

```
symdg create sqadg1 -type REGULAR
```

2. Verify the creation of the group by entering one of the following commands:

```
symdg list
symdg show DgName
```

3. Add devices to the new group:

```
symld -g DgName add pd PdevName [LdevName]
```

Repeat for each device. The default logical device name (*LdevName*) is Dev### unless assigned in the command, for example:

```
symld -g sqadg1 add pd PHYSICALDRIVE2 DriveE
```

4. Associate BCV devices with the group:

```
symbcv -g DgName associate dev SymDevName [LdevName]
```

Repeat for each device. The default logical device name (*LdevName*) is BCV###, unless assigned in the command:

```
symbcv -g sqadg1 associate dev 061 BCVdriveE
```

5. Verify that all devices have been created correctly:

```
symdg show DgName
```

For example:

```
symdg show sqadg1
```

There should be twice as many BCV devices as there are STD devices.

6. Synchronize the concurrent BCV devices by using the following SYMCLI TimeFinder component command:

```
symmir -g DgName -full establish LdevName BCV dev  
          LdevName
```

7. View the concurrent BCV device status by performing a TimeFinder query:

```
symmir -g DgName query -multi
```

Once all devices are synchronized, you can run a TSIM backup command.

Setting Up the Production Server Storage in SRDF

Perform the following steps to set up the SQL production server storage in an SRDF environment:

1. Create a group with the following SYMCLI base command:

```
symdg create DgName -type GroupType
```

where:

GroupType is either RDF1 or RDF2, as in the example:

```
symdg create sqadg1 -type RDF1
```

If the database uses devices from multiple Symmetrix systems, you must create one device group per Symmetrix.

2. Verify the creation of the group by entering one of the following commands:

```
symdg list
symdg show DgName
```

3. Add devices to the new group with the following SYMCLI base command:

```
symld -g DgName add pd PdevName [LdevName]
```

for each device. The default logical device name (*LdevName*) is Dev###, unless assigned in the command, for example:

```
symld -g sqadg1 add pd PHYSICALDRIVE2 DriveE
```

4. Verify that all devices have been created correctly:

```
symdg show DgName
```

For example:

```
symdg show sqadg1
```

Setting Up the Standby Server Storage With Local BCV

Perform the following steps to setup the SQL backup or standby server storage on the local Symmetrix (BCV) side:

1. Create a group with the same name that was used for the production server with the following SYMCLI base command:

```
symdg create DgName -type GroupType
```

where:

GroupType is either REGULAR, RDF1, or RDF2, as in the example:

```
symdg create sqadg1 -type REGULAR
```

2. Verify the creation of the group by entering one of the following commands:

```
symdg list
symdg show DgName
```

3. Add devices to the new group:

```
symld -g DgName add pd PdevName [LdevName]
```

Repeat for each device. The default logical device name (*LdevName*) is Dev###, unless assigned in the command, for example:

```
symld -g sqadg1 add pd PHYSICALDRIVE2 DriveE
```

4. Associate BCV devices with the group:

```
symbcv -g DgName associate dev SymDevName [LdevName]
```

Repeat for each device. The default logical device name (*LdevName*) is BCV###, unless assigned in the command:

```
symbcv -g sqadg1 associate dev 061 BCVdriveE
```

5. Verify that all devices have been created correctly:

```
symdg show DgName
```

For example:

```
symdg show sqadg1
```

6. Synchronize the BCV devices by using the following SYMCLI TimeFinder component command:

```
symmir -g DgName -full establish [LdevName]
```

For example:

```
symmir -g sqadg1 -full establish -noprompt
```

7. View the status by performing a TimeFinder query:

```
symmir -g DgName query
```

Once all devices are synchronized, you can run a TSIM backup command.

Setting Up the Standby Server Storage (Remote BCV Side)

Using the R1 host, perform the following steps to set up a remote BCV pair on the standby SQL server in an SRDF environment:

1. Check the RDF paired devices status:

```
symrdf -g DgName query
```

2. If the device group is not synchronized, synchronize R2 with R1 devices:

```
symrdf -g DgName establish
```

3. Additionally, associate the R2 BCV devices to the new device group:

```
symbcv -g DgName -rdf associate dev SymDevName  
[LdevName]
```

4. For BCV pairs, to synchronize R2 and BCV devices, enter:

```
symmir -g DgName -rdf -full establish LdevName BCV  
dev SymDevName
```

In an SRDF environment, R2 devices are always synchronized with R1 devices, waiting for the failure to happen. You can periodically synchronize and split R2 BCV devices to obtain an updated standby database on the R2 BCV host.

Setting Up the Production Server Storage With Snap Devices

Perform the following steps to set up the SQL production server storage in an EMC Snap environment:

1. Create a group with the following SYMCLI base command:

```
symdg create DgName -type GroupType
```

where:

GroupType is either REGULAR, RDF1, or RDF2, as in the example:

```
symdg create sqadg1 -type REGULAR
```

If the database uses devices from multiple Symmetrix systems, you must create one device group per Symmetrix.

2. Verify the creation of the group by entering one of the following commands:

```
symdg list
symdg show DgName
```

3. Add devices to the new group:

```
symld -g DgName add pd PdevName [LdevName]
```

Repeat for each device. The default logical device name (*LdevName*) is Dev###, unless assigned in the command, for example:

```
symld -g sqadg1 add pd PHYSICALDRIVE2 DriveE
```

4. Add VDEV devices to the new group with the following SYMCLI base command:

```
symld -g DgName add pd PdevName [LdevName]
```

for each device. The default logical device name (*LdevName*) is Dev### unless assigned in the command, for example:

```
symld -g sqadg1 add pd PHYSICALDRIVE2 DriveE
```

5. Verify that all devices have been created correctly by entering the following command:

```
symdg show DgName
```

6. Create the virtual copy session by entering the following SYMCLI Snap component command:

```
symsnap -g DgName create
```

7. View the status by performing a symsnap query:

```
symsnap -g DgName query
```

Configuring Windows Server Disks

Windows platforms support mount points. Make use of a mount point and create the directory of the mount point on both the standard and BCV host. Only a single mount point for the file system used for the database is supported.

Basic Disks

To use basic disks with a single mount point:

1. From the standard host, start with all Symmetrix device groups in a synchronized state and use **Computer Management** to create volumes.
2. After creation, flush the newly created file system with the following SIU command:

```
symmctl flush -drive DriveLetter: | -path MountPoint
```

3. Split the device group that contains the new volumes with the following TimeFinder command:

```
symmir -g DgName split
```

4. From the BCV host, run **Computer Management** to rescan the disks.
5. Change the drive letters or mount points to match the corresponding setup on the standard production host.

Dynamic Disks

The initial setup of the dynamic disks on a server determines the outcome of using EMC TimeFinder for backup and recovery:

- ◆ It is important to keep dynamic disk groups and TimeFinder device groups on a one-to-one basis. For every dynamic disk group, create a TimeFinder device group, and vice versa. To help keep the one-to-one relationship clear, consider naming the dynamic disk groups the same as the TimeFinder device groups.
- ◆ It is not necessary to create the disk group on the backup server. Since the LDM database is resident on every dynamic disk, it is copied over to the backup server on each of the BCVs. All disk group definitions are stored in this database and will immediately appear on the backup server (in an offline state). You can create the TimeFinder device groups on either the production server or the backup server.

With Dynamic disks, you must have VxVM installed. For more information, see *Volume Management Software* on page 3-3.

Creating a Backup for Dynamic Disks With TimeFinder

The following procedure describes the process for using TimeFinder to create a BCV of a dynamic disk. If the disk group on the backup server containing the BCVs is not online, skip steps 1 and 2.

To create a backup for a dynamic disk:

1. Dismount any drive letters or reparse points currently assigned to the BCVs in the dynamic disk group on the backup server. Do not use `mountvol` to perform this dismount. The following SIU command is recommended:

```
symntctl umount -drive DriveLetter: | -path MountPoint -nolock
```

2. Deport the dynamic disk group on the backup server. This step is only a precaution, the dynamic disk groups are deported automatically once the TimeFinder establish is performed and the BCVs become not ready to the server.

```
symntctl deport -dg DgName
```

3. Establish the TimeFinder device group:

```
symmir -g DgName establish
```

4. Rescan the storage bus on the backup server. The dynamic disk group and all of its dynamic disks are listed as unreadable, and therefore, offline.

```
symntctl rescan
```

5. Split the TimeFinder device group:

```
symmir -g DgName split
```

6. Rescan the storage bus on the backup server. The dynamic disk group and all of its dynamic disks are readable, but still offline and foreign to the host.

```
symntctl rescan
```

7. Import the dynamic disk group. Accept the default to keep the dynamic disk group name the same. The final result is that the dynamic disk group and all of its dynamic disks are online and healthy. Mount the file system on the backup server.

```
symntctl import -dg DgName  
symntctl mount -drive DriveLetter: -vol VolName
```

This backup procedure is the same for all types of dynamic volumes.

SQL Server Backup and Restore Operations With TSIM

This chapter describes how to perform backup and restore operations to Microsoft SQL Server databases using the EMC TimeFinder-SQL Server Integration Module (TSIM) command line interface.

- ◆ TSIM Execution Environments7-2
- ◆ Backing Up a Database or Filegroup.....7-5
- ◆ Restoring a Database or Filegroup7-8
- ◆ Backing Up Multiple Databases.....7-12
- ◆ Restoring Multiple Databases7-15
- ◆ SQL Backup and Restore Methods7-22

TSIM Execution Environments

The various TSIM backup and restore commands target different combinations and versions of the Microsoft Windows operating system. The TSIM commands integrate with and support the following environments:

- ◆ SQL Server 2000 Enterprise Edition on Windows 2000, Windows 2000 Datacenter Server, or Windows 2003 Server
- ◆ Microsoft Cluster Services (MSCS)
- ◆ EMC WideSky TimeFinder and SRDF environments

The TSIM commands with their brief descriptions are listed in Table 7-1.

Table 7-1 TSIM Commands

Command	Description
tsimsnap	For a stand-alone or a clustered Windows Server, backs up or restores a Microsoft SQL Server database.
tsimsnap2	For Windows Server, backs up or restores multiple databases of the specified SQL Server instance through a single backup or standby server.

For more information about the syntax of these commands, see Appendix A.

Considerations and Guidelines

Consider the following guidelines before running the TSIM:

- ◆ The snap device support is primarily targeted for point-in-time restore in case of database corruption. Though you may mount the VDEV devices to another host and use it to initialize the standby database, it is not recommended, as all reads from the standby database would eventually come from the source devices. This would degrade the production database performance.
- ◆ Always run the backup/restore command on the local SQL Server host since SQL Server 2000 does not support remote snapshot backup/restore. In an MSCS environment, run the backup/restore command on the active node where the production database resides. To run the backup/restore command from the remote host, the service `rcmdsvc` from the

Windows 2000 Resource Kit can be installed and started on the SQL Server host; use `rcmd` to run `tsimsnap.exe` or `tsimsnap2.exe` remotely. The extended SQL Server stored procedure `xp_cmdshell` can also be used to run the command remotely.

- ◆ TSIM operation uses a Windows trusted connection to connect to the local SQL Server. The user account that executes the command must have SQL Server **sysadmin** role.
- ◆ For an individual database/filegroup restore for disaster recovery, each database should be located on its own volume so that file systems can be unmounted without impacting other databases. This allows you to detach a specific database, unmount its file system, and perform TimeFinder or SRDF restore operations while the remaining databases are online.
- ◆ For backup of multiple databases that reside on shared Symmetrix devices, consider using `tsimsnap2` to backup all the databases at the same time.
- ◆ Consider the performance impact when putting multiple databases on shared Symmetrix devices.
- ◆ For single-database backup using `tsimsnap` or multiple-database backup using `tsimsnap2`, the database can be in the simple recovery model if you do not need to perform transaction log backups. For filegroup backup using `tsimsnap`, the databases must be running in the full recovery model.

Event Logging and Error Files for Windows

The two basic TSIM executables (`tsimsnap` and `tsimsnap2`) are accompanied by the message file `tsim_err.dll` that ties in with the Windows operating system event logging. The message files allow the executable to log all important events, errors, and failures to the Windows event log. Each event has a corresponding event ID, event description, and possibly an accompanying block of data for debugging purposes. All events are logged to the Application event log with the `EMCtsim` source name. All the error messages generated by `tsimsnap` or `tsimsnap2` or can be found in the `tsim_err.h` file in the installation directory.

TSIM Execution Sequence

The TSIM commands streamline and simplify the various tasks and processes involved in, an otherwise complex SQL backup or restore operation. The following execution sequence overviews the tasks and processes performed by these commands:

- ◆ Backup:
 - Check the status of the devices used by the database/filegroup, and abort if they are in an invalid state.
 - Get file system information for the database/filegroup.
 - Initialize and create a Virtual device set.
 - Execute the SQL command to back up the database/filegroup with snapshot.
 - Write metadata information for the database.
 - Flush the file system and perform a TimeFinder BCV split.
 - Notify SQL Server of the completion of the backup event and update the database backup history information.
- ◆ Restore (disaster recovery in automatic mode):
 - Check the status of the devices used by the database, and abort if they are in an invalid state (BCV must be split).
 - Get device group information, initialize and create a Virtual device set, unmount the file system, restore the device group, and mount the file systems.
 - Restore the database/filegroup with snapshot using metadata information.

Command Line Start Up

The two basic TSIM commands (`tsimsnap` and `tsimsnap2`) have various arguments and options. See this chapter and Appendix A for command syntax and descriptions.

To use the TSIM console for command line entry:

1. From the **Start** menu, select **Programs, EMC, ResourcePak, TimeFinder-SQL Server Integration Module, TSIM CLI**.

The TSIM Console (MS-DOS command prompt window) opens to the `\Program Files\EMC\ResourcePak\TSIM` directory.

2. Enter DOS commands at the prompt.
3. Enter **exit** to close the Console window.

Backing Up a Database or Filegroup

You can backup an SQL Server database or filegroup on a Windows server with just one TSIM command. The TSIM command `tsimsnap backup` produces an exact copy of the database or filegroup on the standby or backup server. Once you have backed up an exact copy of the production devices that hold the SQL Server Information (data and logs), you can perform database or filegroup restore actions when needed.

The `tsimsnap backup` command is issued only from the production connected host or the standard/R1 device host for SRDF environments. The TSIM backup operation:

- ◆ Suspends writes to the specified database/filegroup.
- ◆ Automatically writes metadata information about the specific database/filegroup. Metadata information is normally measured in kilobytes, so it is not necessary to have additional storage.
- ◆ Does the following, depending on whether using TimeFinder or Snap:
 - For TimeFinder, it performs an automatic TimeFinder/SRDF split of the devices associated with the database/filegroup.
 - For Snap, it activates the virtual copy session for the devices used by the database/filegroup.

The backup operation splits the production and standby devices while they are in online mode (hot split). The TSIM checks to see if the instant split TimeFinder feature is supported by all Symmetrix systems used by the database. If supported (Engenuity versions 5x66 and above), the instant split behavior assists the hot split action.

Running TSIM Backup

Before running a backup, make sure the devices used by the specified database data and log files, or specified filegroup data files, are in synchronized mode.

- ◆ In a SRDF environment, R2 devices must be synchronized with R1 devices. Also, any R2 BCV devices must be synchronized with R2 STD devices and R2 devices must be synchronized with R1 devices if a remote BCV split is performed with `tsimsnap backup`. Before establishing the local or remote BCV or RDF devices, make sure you unmount the file systems, if the file systems have been mounted on any host.

- ◆ If concurrent BCV is used to get two concurrent point-in-time backups of the production database, make sure all concurrent BCVs are synchronized with either the devices used by the production database data and log files, or with the specified file group data files.
- ◆ In a virtual snap environment, VDEV devices must be in the created mode with standard devices.

To backup a Microsoft SQL Server database, use the following form:

```
tssnap backup -d SqlDbName -f MetaFile
```

In addition to targeting a specific database with the `-d` option, you must specify a meta file name that holds the storage parameters concerning the database. If you do not wish to use the default TSIM directory, you can specify a full path name to the meta file.

The meta data file should be located on a normal Symmetrix device or local host drive. Optionally, it can be on a shared device and be made accessible through the network. This file is generally small, and can be copied on a diskette for backup purposes.

Optional Selections

The following are optional selections to this TSIM backup command:

```
[ -fg FileGrpName ]
[ -s VirtSqlServName [ \InstanceName ] |
  HostName [ \InstanceName ] ]
[ -nrtgt | -rbcvsplit | -rdfsplitt | -snap ]
[ -lock [ -lockid LockID ] [ -sid SymID ] ]
[ -overwrite ]
```

You can confine the backup to a specific filegroup name within the specified database, using the `-fg` option. On the production server, using the `-s` option, you can target a specific:

- ◆ Virtual SQL Server name with or without an instance name, or
- ◆ Host name with or without an instance name.

In a TimeFinder environment, you can use the `-nrtgt` option to make the BCV devices not ready after a TimeFinder split.

In a SRDF environment, you can use the `-rbcvsplit` option to split the remote BCV from its R2 mirror, or use the `-rdfsplitt` option to split the R2 from the R1 device.

In a virtual snap environment, you can use the `-snap` option to activate a virtual copy session.

You can specify to overwrite any existing database dump file, using the `-overwrite` option.

Note that the `-remote` option is considered obsolete, but still will work in old scripts for compatibility.

Restoring a Database or Filegroup

For a disaster recovery situation, you can restore an SQL Server database or filegroup on a Windows server using a single TSIM command. Using the command `tsimsnap restore` from the production (standard) host, you can restore the production server from its local BCV, or from the remote R2 mirror in an SRDF environment.

This command is not intended to create a database that runs as a separate instance. The command should only be used in a disaster recovery scenario to restore a database/filegroup from a TimeFinder BCV or VDEV to the standard devices.

The restore operation automatically performs the following tasks:

- ◆ Suspends any writes to the database and/or filegroups.
- ◆ Unmounts the file system on the standard host.
- ◆ Does the following, depending on whether using TimeFinder or Snap:
 - For TimeFinder, it performs a TimeFinder restore action, and then splits the restored device from the backup devices.
 - For Snap, it performs a `symsnap restore` action.
- ◆ Mounts the file system on the standard side host.
- ◆ Restores the database or filegroup with snapshot.

Running TSIM Restore

Before running the `TSIM restore` command in this automatic mode, make sure the devices used by the database/filegroup are in the split status. Make sure the file system on which the metadata file resides is not used by the database, and no application or service is holding the file system handles for the database. You can issue the `symntctl openhandle` command to check if applications other than SQL Server are holding the file system handle.

If the file systems used by the BCV devices are mounted on a BCV host, unmount those file systems before running a TSIM restore or a TimeFinder (`symmir`) restore action.

To restore a Microsoft SQL Server database, use the following form:

```
tsimsnap restore -d SqlDbName -f MetaFile
                    -norecovery|-recovery|-standby|
```

In addition to targeting a specific database with the `-d` option, you must specify the meta file name (or full path) that has the meta data information concerning the database you want to restore (`-f` option).

If you are restoring just a filegroup, you can specify the filegroup with the `-fg` option. If you are restoring the whole database (not a filegroup), you must specify one of three modes to identify the state you need when the database becomes restored. The possible database final states are `norecovery`, `recovery`, or `standby`.

To restore the database/filegroup for virtual snap devices, you must specify the `-snap` option.

Optional Selections

The following are optional selections to the TSIM restore command:

```
[-s VirtSqlServName[\InstanceName] |
    HostName[\InstanceName]]
[-m [-rf LocateFileName]]
[-fg FileGrpName]
[-snap]
[-lock [-lockid LockID] [-sid SymID]]
```

Manual Mode

Using the `-m` option, you can override the default automatic mode by selecting manual mode, which breaks this overall restore operation into individual tasks. This mode is used for clustered servers and dynamic disks, or other services that must be turned off with manual intervention. It also allows for a restored database to be relocated on different devices.

Manual mode requires you to do the following:

- ◆ Detach the database using the `sp_detach_db` stored procedure or SQL Enterprise Manager on the standard host.
- ◆ Unmount the file systems.
- ◆ Do the following, depending on whether you are using TimeFinder or Snap:
 - For TimeFinder, perform a TimeFinder restore, and then once the devices are restored, split those devices.
 - For Snap, perform a `symsnap restore` action.

- ◆ Manually mount the file systems on the standard host where the selected database resides before executing the manual restore operation.
- ◆ Restore the database/filegroup with snapshot.

With the manual mode, you can specify the name of the relocation text file (.txt) using the `-rf` option. To move the database to different devices, first mount all file systems used by the database to the new location before running with this option. This relocation text file contains and lists the logical and physical device name where each file resides in the database storage.

If only a single filegroup needs to be restored, and you need to restore the transaction log to the end of the transaction log backup chain, you must use the automatic mode to restore the filegroup from the BCV back to a standard device.

If a point-in-time restore is required, the complete set of the filegroup backups must be restored, using either manual or automatic mode. When restoring in automatic mode, the restore sequence does not matter. For restoring in manual mode, the primary filegroup needs to be restored first, then restore all the other filegroups used by the database.

It is strongly recommended to split the device group before running this command to preserve the BCV copy of the database.

The point-in-time database backup copy can be used for either the complete database or individual filegroup restores. If any BCV copy of the filegroup gets updated after the point-in-time database backup, only individual filegroup restores can be used.

Example

For a relocation example, Figure 7-1 shows `databaseXYZ` original logical filename and physical filename pair from the database query. To relocate the database, create a new text file `databaseXYZ_relocation.txt` and put the original logical filename and the new physical filename in each line of the file (as shown in Figure 7-2). Run the following command to restore the `databaseXYZ` to the new location with standby state:

```
tsimsnap restore -d databaseXYZ -f n:\databaseXYZ.dmp
-rf n:\databaseXYZ_relocation.txt -m -standby
```

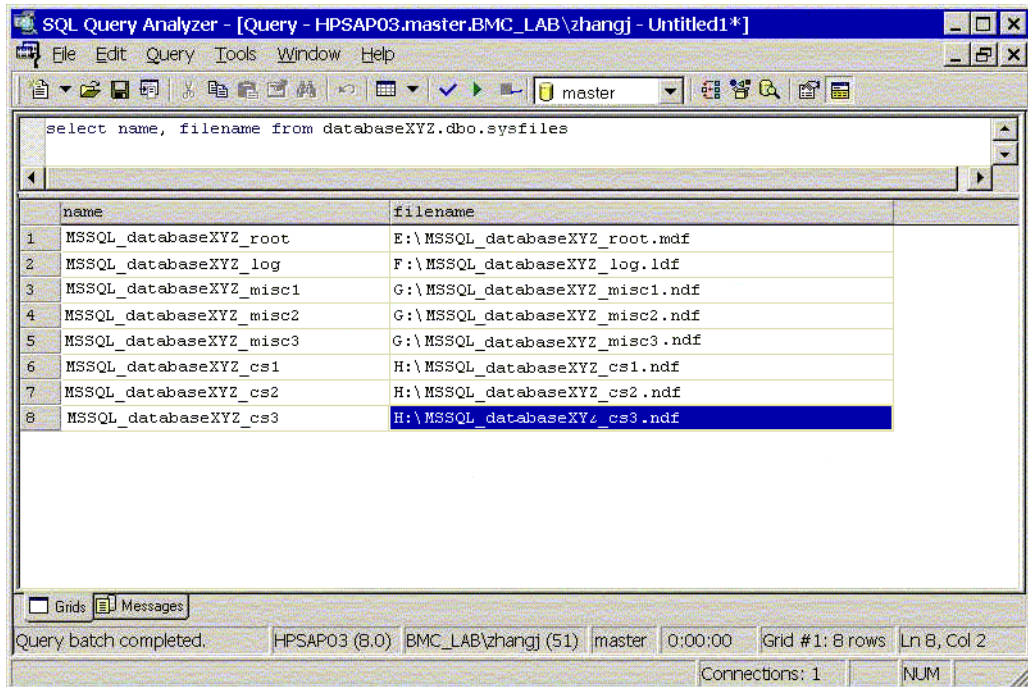


Figure 7-1 Database Query: Logical and Physical Filename Pairs

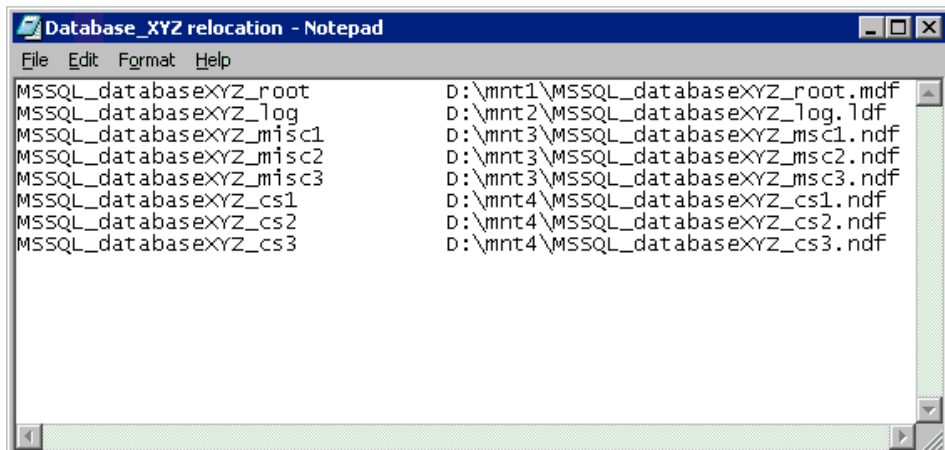


Figure 7-2 Relocation File With Old Logical and New Physical Filenames

Backing Up Multiple Databases

You can backup multiple SQL Server databases on a Windows server using just one TSIM command. The TSIM command `tsimsnap2 backup` produces an exact copy of the databases on the standby or backup server. Once you have backed up an exact copy of the production devices that hold the SQL Server information (data and logs), you can perform database or filegroup restore actions on any or all of the databases when needed.

The `tsimsnap2 backup` command is issued only from the production connected host or the standard/R1 device host for SRDF environments. The TSIM backup operation:

- ◆ Suspends writes to the specified databases.
- ◆ Automatically writes metadata information about each of the specific databases. Metadata information for each database is normally measured in kilobytes, so it is not necessary to have additional storage.
- ◆ Does the following, depending on whether using TimeFinder or Snap:
 - For TimeFinder, it performs an automatic TimeFinder/SRDF split of the devices associated with the specified databases.
 - For Snap, it activates the virtual copy session for the devices used by the specified databases.

This TSIM command backs up or restores multiple databases for a stand-alone or a clustered Windows SQL Server instance that reside Symmetrix devices. The backup operation consolidates the backup timeframes by concurrently backing up multiple databases together. Once you have backed up an exact copy of the production devices that hold the SQL Server information (data and logs), you can perform database or filegroup restore actions on any or all databases when needed. The backup operation writes information about the specific databases in metafiles stored in the specified meta directory. The default file names take on the form `DbName_snapshot.dmp` for the various meta files in this directory.

If the Symmetrix supports instant split, then instant split TimeFinder behavior will assist a hot-split task portion of the backup activities. Before starting a backup operation, all database devices must be synchronized, and if an SRDF environment exists, R2 devices and their BCVs are synchronized with R1 devices.

The command, issued only from the standard/R1 host, automatically writes metadata information about the specific databases in the specified directory. Metadata information is normally measured in kilobytes, so it is not necessary to have additional storage.

The command performs an automatic TimeFinder local/remote BCV or RDF split of the devices associated with the databases, during the database write suspension period. The backup process splits the production and standby devices while they are in online mode (hot split). The TSIM checks to see if the instant split TimeFinder feature is supported by all Symmetrix systems used by the database. If supported (Enginuity versions 5x66 and above), the instant split behavior assists the hot split action.

Running TSIM Backup

Before running a multiple backup operation, make sure all the devices used by the databases are in synchronized mode. In an SRDF environment, R2 devices must be synchronized with R1 devices, and R2 BCV devices must be synchronized with R2 devices. Before establishing the local or remote BCV or RDF devices, make sure you unmount the file systems, if the file systems have been mounted on any host.

To backup multiple Microsoft SQL Server databases, use the following form:

```
tsimsnap2 backup -alludb | -d SqlDbName SqlDbName... |  
-instance
```

You can target all user databases in your database instance with the `-alludb` option, or you can specify a series of databases with the `-d` option, or you can target all the databases in your database instance, using the `-instance` option. There is no limit on the number of the databases to be backed up. You need to consider the appropriate number of the databases to be backed up according to the host CPU and memory resource availability.

Optional Selections

The following syntax are optional selections for this multiple TSIM backup command:

```
[ -f MetaFileDir ]
[ -s ClustServName | SqlServName\InstanceName ]
[ -nrtgt | -rbcvsplit | -rdfsplitt | -snap ]
[ -lock [-lockid LockID] [-sid SymID] ]
[ -overwrite ]
```

Using the `-f` option, you can specify a directory for various metafiles that are created for the various databases specified in the backup action. The default file names take on the form *DbName_snapshot.dmp* for the various meta files in this directory.

You can target a specific clustered server name or a production server name with or without an instance name, using the `-s` option.

In a TimeFinder environment, you can use the `-nrtgt` option to make the BCV devices not ready after a TimeFinder split.

In a SRDF environment, you can specify to split the remote BCV from its R2 mirror, using the `-rbcvsplit` option or split the R2 device from the R1, using the `-rdfsplitt` option.

In a virtual snap environment, you can use the `-snap` option to activate a virtual copy session.

Note that the `-remote` option is still supported for script compatibility only.

Also, you can specify to overwrite any existing database dump files, using the `-overwrite` option.

Restoring Multiple Databases

For a disaster recovery situation, you can restore multiple SQL Server databases on a Windows server using a TSIM command. For example, using `tsimsnap2 restore` from the production (standard) host, you can restore the production server from its local BCV or from the remote R2 mirror in an SRDF environment.

Running TSIM Restore

Before running the TSIM restore command, you must mount the file system for the specified databases first. The `tsimsnap2 restore` command restores the specified databases into `norecovery`, `standby`, or `recovery` status. If either the `norecovery` or `standby` option has been used to restore the databases, then additional transaction logs from the production databases can be rolled forward.

Make sure the devices used by each database are in the split status. Make sure the file system where the metadata file resides is not used by the particular database, and no application or service is holding the file system handles for the database. You can execute `symntctl openhandle` to check if there is any application other than SQL Server holding the file system handle.

If the file systems used by the BCV devices are mounted on a BCV host, unmount those file systems before running a TSIM restore or a TimeFinder (`symmir`) restore action.

To restore multiple Microsoft SQL Server databases, use the following form:

```
tsimsnap2 restore -d SqlDbName SqlDbName...  
                  -f MetaFileDir  
                  -norecovery|-recovery|-standby
```

You can target and specify a series of databases with the `-d` option. There is no limit on the number of the databases to be restored. You need to consider the appropriate number of the databases to be restored according to the host CPU and memory resource availability.

You must specify one of three possible states to have the databases restored to: `norecovery`, `recovery`, or `standby` state.

Optional Selections

The following syntax are optional selections for this multiple TSIM backup command:

```
[ -s ClustServName | SqlServName \ InstanceName ]
```

You can target a specific clustered server name or a specific instance on the production server, using the `-s` option.

Initializing Multiple Databases on Standby Host

Using the multiple TSIM restore command, you can initialize (create) multiple standby databases to another instance on the standby host side.

Before running the TSIM restore command, you must mount the file system disks for the specified dataset first. Using the locally-attached BCV host, you specify the BCV databases, the standby server name, and its target instance name:

```
tsimsnap2 restore -d SqlDbName SqlDbName...
                  -f MetaFileDir
                  -norecovery | -recovery | -standby
                  [-s VirtSqlServName [ \ InstanceName ] |
                  HostName [ \ InstanceName ] ]
```

Initializing Multiple Databases on BCV Host

This section presents a TSIM backup and restore method to initialize multiple standby databases under the BCV host. Once standby databases have been initialized on the BCV side, you can update them using either TimeFinder log shipping or network log shipping.

The `tsimsnap2 backup` suspends writes to multiple databases and automatically writes metadata information about those databases. It also performs an automatic TimeFinder split of the devices associated with the databases. You enter the databases and directory name where the metadata information files reside.

The TSIM multiple restore command makes use of the combination of the point-in-time BCV backup copy of the databases and the metadata files to instantaneously restore the databases with standby mode.

The following steps describe how multiple standby databases can be created on the BCV side with TSIM multiple backup and restore actions. If the file system is not mounted on the BCV host, start from step 5:

1. On the BCV host, detach those multiple standby databases using the SQL command, `sp_detach_db dbname`, or SQL Server Enterprise Manager.
2. Unmount the standby database file systems by executing the SIU command:

```
symntctl umount -drive DriveLetter | -path MountPoint
```

If Windows dynamic disks are used, apply the `-nolock` option with this command.

3. If Windows dynamic disks are used, deport the disk group used by the databases on BCV host:

```
symntctl deport -dg DgName
```

4. Establish the devices used by the databases, using TimeFinder:

```
symmir -g DgName establish
```

5. If Windows dynamic disks are used, rescan the disks on the BCV host, using the SIU command:

```
symntctl rescan
```

6. Once the device group is synchronized, run a TSIM multiple backup command on the standard host to get a point-in-time backup of the production databases:

```
tsimsnap2 backup -d DbName DbName... -f MetaDirName
```

7. If Windows dynamic disks are used, rescan the disks and import the disk group on the BCV host by executing the following SIU commands:

```
symntctl rescan
symntctl import -dg DgName
```

8. Mount the file systems used by the databases on the BCV host by running the command:

```
symntctl mount -drive DriveLetter -vol VolName
[-dg DgName]
```

9. Run a TSIM multiple restore to restore those multiple databases with snapshot:


```
tsimsnap2 restore -d DbName DbName... -f MetaDirName
               -standby
```
10. Backup the transaction log from the production databases on the standard host.
11. Restore the transaction log backups to the multiple databases, using the SQL commands.
12. Use network or TimeFinder log shipping to update the standby databases.

Restoring a Database on a Production Clustered Host

To restore an SQL Server database on a production host in an MSCS clustered environment, do the following:

1. Detach the corrupt SQL database.
2. In Cluster Administrator, remove the dependencies in SQL Server on the disks that contain the databases.
3. In Cluster Administrator, take offline all disks that contain the database you want to restore.
4. From a command prompt, execute the following TimeFinder restore command that targets the device group that contains the disks that hold the SQL database:


```
symmir -g DgName restore
```
5. Once the device group is restored, split the device group database:


```
symmir -g DgName split
```
6. Repeat steps 4 and 5 for all device groups that contain the SQL database you want to restore.
7. In Cluster Administrator, take offline the entire SQL Cluster Resource.
8. In Cluster Administrator, add the disk dependencies of all disks containing the SQL database files to the SQL Server resource.
9. In Cluster Administrator, bring the entire SQL resource online.

10. Restore the database using the appropriate `tsimsnap` or `tsimsnap2 restore` command.

Disaster Recovery Strategy for Multiple Databases

In a disaster recovery situation, you may need to restore the standard or production side database devices with the BCV standby side databases. The standard side databases must be recovered to either the `norecovery`, `recovery` or `standby` state.

If multiple databases are sharing Symmetrix devices, the granularity of a single database BCV/RDF restore becomes impossible because this command restores every database in the directory. In this situation, you must use Solutions Enabler commands to execute the restore operations separately for all databases that share the Symmetrix devices, or manually copy the single database files from the backup server back to the standard side for a single database restore.

From the Local BCV

To restore the production databases from the local BCV on the production host:

1. Detach or drop the specified databases first.
2. Unmount the file systems of the databases to be restored using the `SIU` command:

```
symmtctl umount -drive DriveLetter | -path MountPoint
```

3. Execute the TimeFinder restore command, targeting the database device group to restore the database from the local BCV:

```
symmir -g DbDgName restore
```

4. Once the device group is restored, split the device group, using the TimeFinder command:

```
symmir -g DbDgName split
```

5. Mount the file systems of the specified databases:

```
symmtctl mount
```

6. Restore the databases with a TSIM SQL snapshot:

```
tsimsnap2 restore -d DbName DbName...  
-norecovery|-standby
```

7. Using SQL commands, restore additional transaction logs to the point-in-time before the database corruption (the databases from the last TSIM command must now be in the norecovery or standby state).

The production restore operation from the local BCV is complete.

From the Remote BCV

To restore the production database from a remote BCV on the production host:

1. Detach or drop the specified database first.
2. Unmount the file systems of the databases to be restored using the SIU command:

```
symntctl umount -drive DriveLetter | -path MountPoint
```

3. Split the RDF link using the SRDF command:

```
symrdf -g DbDgName split
```

4. Restore devices from the R2 BCV to the R2, using the following TimeFinder command on the R1 host:

```
symmir -g DbDgName restore -rdf
```

5. Once the device group is restored, split the device group using the TimeFinder command:

```
symmir -g DbDgName split -rdf
```

6. Restore devices from R2 to R1, using the SRDF command on the R1 host:

```
symrdf -g DbDgName restore
```

7. Once the device group is restored, split the RDF link using the SRDF command:

```
symrdf -g DbDgName split
```

8. Mount the file systems used by the specified database:

```
symntctl mount
```

9. Restore the specified databases with a TSIM SQL snapshot:

```
tsimsnap2 restore -d DbName DbName...  
-norecovery|-standby
```

10. Using SQL commands, restore additional transaction logs to the point-in-time before the database corruption (the databases from the last TSIM command must now be in the norecovery or standby state).

The production restore operation from the remote BCV is now.

From the Remote R2

To restore the production database from a remote R2 device on the backup server:

1. Detach or drop the specified database first.
2. Unmount the file systems of the databases to be restored using the SIU command:


```
symntctl umount -drive DriveLetter | -path MountPoint
```
3. Restore devices from R2 to R1, using the SRDF command on the R1 host:


```
symrdf -g DbDgName restore
```
4. Once the device group is restored, split the RDF link using the SRDF command:


```
symrdf -g DbDgName split
```
5. Mount the file systems used by the specified database:


```
symntctl mount
```
6. Restore the specified databases with a TSIM SQL snapshot:


```
tsimsnap2 restore -d DbName DbName...  
-norecovery|-standby
```
7. Using SQL commands, restore additional transaction logs to the point-in-time before the database corruption (the databases from the last TSIM command must now be in the norecovery or standby state).

The production restore operation from the remote R2 on the backup server is complete.

SQL Backup and Restore Methods

There are many task sequences and command options in SQL, TSIM, and TimeFinder management utilities for you to choose to initialize and restore a database. In some cases, a site may have multiple BCVs, which translates into multiple copies. Some sites may want to have total control over recovery and perform these tasks in a very controlled and methodical manner. Other sites prefer executing a command and letting a program automatically handle the recovery.

This section presents some additional recovery methods (not previously described) you might use or optimize that best meets your needs.

This section describes how to use the TSIM to automate recovery tasks, including the following:

- ◆ Initializing and updating the standby database
- ◆ Initializing an instantaneous database backup on a local BCV and restoring it for disaster recovery
- ◆ Initializing an instantaneous database backup on a virtual snap and restoring it for disaster recovery
- ◆ Database filegroup backup and restore considerations and scenarios for disaster recovery

Initializing and Updating the Standby Database

The combination of the point-in-time BCV backup copy of the database and the metadata file can be used to initialize the standby database instantaneously. After the standby database has been initialized on the BCV host, it can be updated by either TimeFinder log shipping or network log shipping. (Log shipping feeds transaction log backup files from a source database to the destination database, keeping them synchronized).

The `tsimsnap backup` command suspends writes to a database and automatically writes metadata information about the specific database. It also performs an automatic TimeFinder split of the devices associated with the database. You enter a database name and filename where the metadata information will reside.

The following steps initialize a standby database for the BCV host. If the file system has not been mounted on the BCV host, start at step 5.

1. On the BCV host, detach the standby database using the SQL command `sp_detach_db dbname` or SQL Server Enterprise Manager.
2. Unmount the standby database file systems by executing the SIU command:

```
symntctl umount -drive DriveLetter | -path MountPoint
```

If Windows dynamic disks are used, use the `-nolock` option with this command.

3. If Windows dynamic disks are used, deport the disk group used by the databases on BCV host:

```
symntctl deport -dg DgName
```

4. Establish the devices used by the databases, using TimeFinder:

```
symmir -g DgName establish
```

5. If Windows dynamic disks are used, rescan the disks on the BCV host, using the SIU command:

```
symntctl rescan
```

6. Once the device group is synchronized, run a TSIM backup on the standard host to get a point-in-time backup of the production database:

```
tsimsnap backup -d DbName -f MetaFileName
```

7. If Windows dynamic disks are used, rescan the disks and import the disk group on the BCV host by executing the following SIU commands:

```
symntctl rescan
symntctl import -dg DgName
```

8. Then mount the file systems used by the database on BCV host by running the command:

```
symntctl mount -drive DriveLetter -vol VolName
[-dg DgName]
```

9. Run a TSIM restore action in manual mode to restore the standby database with snapshot:

```
tsimsnap restore -d DbName -f MetaFileName -m
```

After the standby database is initialized on the BCV host, you can update it by shipping the transaction log from the production database. This can be done by either network log shipping using the SQL Server maintenance plan or by TimeFinder log shipping. The following steps describe how to ship the transaction log (update), using TimeFinder and SIU commands:

1. Establish the device group used by the transaction log backup device:
`symmir -g DgName establish`
2. If Windows dynamic disks are used, rescan the disks on the BCV host, using the SIU command:
`symmtctl rescan`
3. After the device group is synchronized, use the SQL Server Enterprise Manager or SQL command to back up the transaction log to the transaction backup device from the standard or production host as shown in Figure 7-3.

You must choose how often the standby database will be updated and how often the transaction log is backed up.

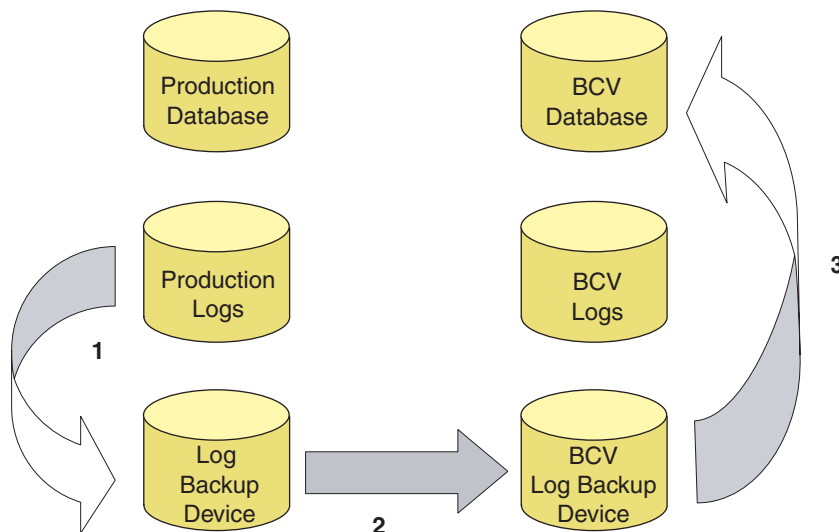


Figure 7-3 Updating Standby Database Using BCV Transaction Backup

4. Flush the file system used by the transaction log backup device from the standard host, by entering:

```
symntctl flush -drive DriveLetter | -path MountPoint
```

5. Split the transaction log backup device, using the TimeFinder command:

```
symmir -g DgName split
```

6. If Windows dynamic disks are used, rescan the disks and import the disk group on the BCV host by executing the following SIU commands:

```
symntctl rescan  
symntctl import -dg DgName
```

7. From the BCV host, mount the transaction log backup device by running the SIU command:

```
symntctl mount -drive DriveLetter -vol VolName  
[-dg DgName]
```

8. From the BCV host, use the SQL Server Enterprise Manager or the SQL command to restore the transaction log backup file to update the standby database.

9. Unmount the file system from the BCV host by executing the SIU command:

```
symntctl umount -drive DriveLetter | -path MountPoint
```

If Windows dynamic disks are used, use the `-nolock` option with this command.

10. If Windows dynamic disks are used, deport the disk group used by the databases on the BCV host:

```
symntctl deport -dg DgName
```

11. Repeat steps 1 through 7 to update the remaining standby databases.

The standby databases are now initialized and updated.

Initialize/Recovery of Backup Database on Local BCV

You can create an instantaneous database backup to have the local BCV available for disaster recovery (restore) operations. If you are splitting off a local BCV and do not plan on using the copy as a standby database, you can choose the metadata location to be a normal device on the standard host. The metadata file can be written to either a Symmetrix mirrored device or a local disk on the host. This is important for restore purposes in automatic mode as the file must be available to read at all times. Part of the restore process unmounts the file systems on which the database resides. This procedure temporarily makes the file unavailable. For this reason, you should keep the metadata information in more than one place. Typically, the general file size is in kilobytes, so storage should not be an issue.

The `tsimsnap backup` suspends writes to a database and automatically writes metadata information about the specific database. It also performs an automatic TimeFinder split of the local BCV devices associated with the database. You can enter a database name and filename where the metadata information will reside. After `tsimsnap backup` completes, keep frequent backups of the database transaction log to reduce recovery time.

The following steps initialize the backup database on the local BCV:

1. Establish the device groups used by the production database, using the TimeFinder command:
2. After the device group is synchronized, perform a TSIM backup to get a point-in-time back up of the production database:

```
symmir -g DgName establish
```

```
tsimsnap backup -d DbName -f MetaFileName
```

At this point, the file systems used by the database on the BCV host can be mounted to be backed up from disk to tape or other media.

3. Back up the additional transaction log from the production database in the scheduled time interval.

If at some point for a point-in-time recovery, the production database becomes corrupt, analyze the time of the corruption and back up the trailing transaction log from the production database. Unmount the file systems used by the BCV devices on the BCV host if they have been mounted. Use `symmtctl openhandle` to see if there is any

process or service other than SQL Server that holds the filesystem handles used by the production database. Stop those processes or services if they are holding file system handles.

1. Run a TSIM restore command in automatic mode to restore the corrupt database to the previous point-in-time of the database back up with snapshot in standby mode:

```
tsimsnap restore -d DbName -f MetaFileName -standby
```

If the production database is running on top of MSCS or you want to take control of every step during the restore process, the following procedure can be used on the standard host:

- a. Detach or drop the corrupt database.
- b. Unmount the file systems by executing the SIU command:

```
symntctl umount -drive DriveLetter | -path MountPoint
```

If Windows dynamic disks are used, apply the `-nolock` option with this command.

- c. Restore the BCV back to standard devices using the TimeFinder restore command:

```
symmir -g DgName restore
```

- d. After the device group is restored, split the device group:

```
symmir -g DgName split
```

- e. Mount the file systems used by the database:

```
symntctl mount -drive DriveLetter -vol VolName  
[-dg DgName]
```

- f. Run the TSIM restore command in manual mode to restore the production database with snapshot in standby mode:

```
tsimsnap restore -d DbName -f MetaFileName  
-m -standby
```

2. Restore additional transaction log backups to the standby and stop the transaction log recovery database with standby mode. Restore the last transaction log backup before the point-in-time of the database corruption. Make the restored database read/write.
3. Once restore is successful, resync the device group and issue `tsimsnap backup` to get a new point-in-time backup of the production database for disaster recovery.

Initialize/Recovery of Backup Database on Virtual Snap

You can create an instantaneous database backup to have the VDEV available for disaster recovery (restore) operations. The metadata file can be written to either a Symmetrix mirrored device or a local disk on the host. This is important for restore purposes in automatic mode as the file must be available to read at all times. Part of the restore process unmounts the file systems on which the database resides. This procedure temporarily makes the file unavailable. For this reason, you should keep the metadata information in more than one place. Typically, the general file size is in kilobytes, so storage should not be an issue.

The `tsimsnap backup -snap` suspends writes to a database and automatically writes metadata information about the specific database. It also automatically activates the virtual copy session to the local VDEV devices associated with the database. You can enter a database name and filename where the metadata information will reside. After `tsimsnap backup` completes, keep frequent backups of the database transaction log to reduce recovery time.

The following steps initialize the backup database on the VDEV:

1. Create the virtual copy session for the device groups used by the production database, using the TimeFinder command:

```
symsnap -g DgName create
```

2. After the virtual copy session is enabled, perform a TSIM backup to get a point-in-time back up of the production database:

```
tsimsnap backup -d DbName -f MetaFileName -snap
```

3. Back up the additional transaction log from the production database in the scheduled time interval.

If at some point for a point-in-time recovery, the production database becomes corrupt, analyze the time of the corruption and back up the trailing transaction log from the production database. Unmount the file systems used by the VDEV devices if they have been mounted to any host. Use `symmtctl openhandle` to see if there is any process or service other than SQL Server that holds the filesystem handles used by the production database. Stop those processes or services if they are holding file system handles.

1. Run a TSIM restore command in automatic mode to restore the corrupt database to the previous point-in-time of the database back up with snapshot in standby mode:

```
tsimsnap restore -d DbName -f MetaFileName -standby
-snap
```

If the production database is running on top of MSCS or you want to take control of every step during the restore process, the following procedure can be used on the standard host:

- a. Detach or drop the corrupt database.
- b. Unmount the file systems by executing the SIU command:

```
symntctl umount -drive DriveLetter | -path
MountPoint
```

If Windows dynamic disks are used, apply the `-nolock` option with this command.

- c. Restore the VDEV back to standard devices:

```
symsnap -g DgName restore
```

- d. Mount the file systems used by the database:

```
symntctl mount -drive DriveLetter -vol VolName
[-dg DgName]
```

- e. Run the TSIM restore command in manual mode to restore the production database with snapshot in standby mode:

```
tsimsnap restore -d DbName -f MetaFileName
-m -standby
```

2. Restore additional transaction log backups to the standby and stop the transaction log recovery database with standby mode. Restore the last transaction log backup before the point-in-time of the database corruption. Make the restored database read/write.

3. Once restore is successful, terminate the old virtual copy session:

```
symsnap -g DgName terminate
```

4. Create a new virtual copy session:

```
symsnap -g DgName create
```

5. Issue `tsimsnap backup` to get a new point-in-time backup of the production database for disaster recovery.

Database Filegroup Backup and Recovery

A filegroup backup/restore operation can dramatically reduce the overall backup/recovery time if well planned. A complete database filegroup backup set and transaction log backup chain are needed to restore the database to the consistent state. The complete filegroup backup set for a database can come from a TSIM database backup operation, and from an individual TSIM filegroup backup operation.

After getting the complete filegroup backup set, you can update a specific filegroup depending on the amount of data changed in the filegroup to reduce the recovery time in case of any failure in the production database. However, by doing that, the integrity of the database backup may be destroyed if the same BCV pair has been used for that case. The only way to restore the database is to use an individual filegroup restore. To restore a specific filegroup from the database backup, specify the metadata file created by them when using:

```
tsimsnap restore -d DbName -fg FileGrpName -f MetaFile
```

There are basically two scenarios for filegroup restore: database corruption and media failure. In both cases, we assume that the complete filegroup backup set has been created and the transaction log backup chain has been maintained.

◆ Database Corruption

In the case of database corruption such as table truncation and logical database corruption, backup the trailing transaction log from the production database. In this case, the transaction log backup includes the transactions that corrupt the database, therefore, a restore to the point-in-time before the corruption is needed to recover the database. Restore the complete filegroup backup set by restoring each filegroup separately using `tsimsnap restore -fg` (in manual or automatic mode); then restore with no recovery the transaction log backup chains that cover the first filegroup backup, and restore with recovery the last transaction log backup (to the point-in-time before the corruption).

◆ Media Failure

When a disk in a specific filegroup gets damaged, back up the trailing transaction log from the damaged database. If the database gets into suspect mode:

- Run the SQL command `backup log with no_truncate` to back up the active portion of the log without truncating it.
- Replace the damaged disk and recreate the file system on that disk.
- Restore that specific filegroup by executing `tsimsnap restore -fg` (in automatic mode for basic disks in a non-clustered environment only).
- Restore additional transaction log backup versions that include the time frame after the specific filegroup backup with no recovery.
- Restore the last transaction log backup with recovery to bring the database back to a consistent state.

Filegroup Backup/Restore Considerations

In a filegroup backup/restore scenario consider the following:

- ◆ The database needs to be in the full recovery mode. Unlike `tsimsnap backup` for a full database, log writes are not suspended, so it is necessary to do a transaction log backup from the Enterprise Manager or with Transact SQL.
- ◆ All devices used by the specific filegroup must be in a synchronized state before running `tsimsnap backup -fg` (devices used by the filegroup may exist in single or multiple Symmetrix device groups).

To allow greater flexibility and granularity, put all filegroup data files in their own Symmetrix device group and put the log files in a separate device group.

- ◆ To leverage the ability to restore single filegroups, only files from a single filegroup should exist on Symmetrix logical devices.
- ◆ TSIM operations must be performed on the same SQL Server host targeted for backup/restore as remote snapshot backup/restore is not supported.

Filegroup Best Practice Backup and Restore Examples

The following example scenarios illustrate the best practices for implementing backup and restore operations assisted with the TSIM. In these scenario examples, we are managing database `emcdb`, which includes three filegroups, `primary`, `emcdb_fg1`, `emcdb_fg2`, and log files. The database is in the full recovery mode, see Figure 7-4.

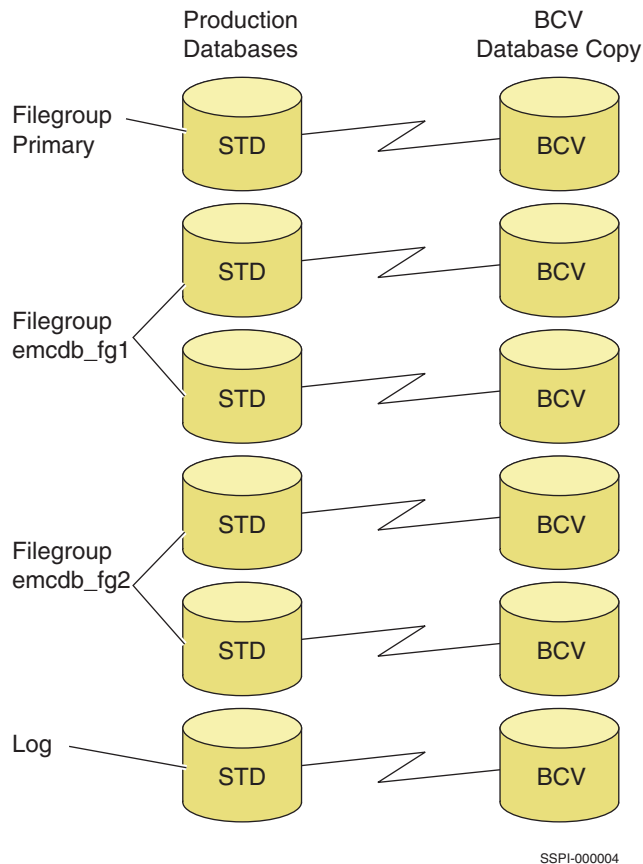


Figure 7-4 Filegroup Backup Example Environment

Table 7-2 shows the components of the example database `emcdb`.

Table 7-2 Filegroup Backup Example Environment

Filegroup Name	Description
Primary	One file on one Symmetrix device.
emcdb_fg1	Three files on two Symmetrix devices. Each Symmetrix device contains only files from filegroup <code>emcdb_fg1</code> .
emcdb_fg2	Three files on two Symmetrix devices. Each Symmetrix device contains only files from filegroup <code>emcdb_fg2</code> .
Log files	Two files on one Symmetrix device.

Backup Scenario 1

For Backup Scenario 1, we need to back up the full database with `tsimsnap backup`, and then use `tsimsnap backup -fg` to back up the individual filegroup during the week, see Figure 7-5 on page 7-34.

1. Create a full database backup every Sunday at 12:00 midnight:

```
tsimsnap backup -d emcdb -f c:\metadata\emcdb.dmp
```

2. Back up the transaction log every 15 minutes (Enterprise Manager or Transact SQL).
3. Back up filegroup `emcdb_fg1` Monday at midnight (updated frequently):

```
tsimsnap backup -d emcdb -fg emcdb_fg1
-f c:\metadata\emcdb_fg1.dmp
```

This backup overwrites the BCV copy of the filegroup created by the previous full database backup.

4. Back up the transaction log every 15 minutes (Enterprise Manager or Transact SQL).
5. Back up filegroup `emcdb_fg2` Wednesday at midnight (updated frequently):

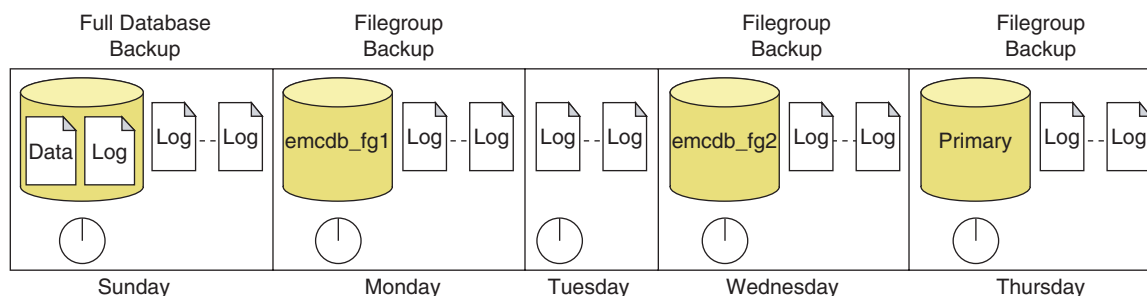
```
tsimsnap backup -d emcdb -fg emcdb_fg2
-f c:\metadata\emcdb_fg2.dmp
```

This backup overwrites the BCV copy of the filegroup created by the previous full database backup.

6. Back up the transaction log every 15 minutes (Enterprise Manager or Transact SQL).
7. Back up the filegroup `primary` Thursday at midnight (updated frequently):

```
tsimsnap backup -d emcdb -fg Primary
-f c:\metadata\emcdb_primary.dmp
```

This back up overwrites the BCV copy of the filegroup created by the previous full database backup.



SSPI-000005

Figure 7-5 Database Backup Schedule for Example Scenario 1

In the following scenarios, the filegroup name and metadata file names vary depending on when the corruption occurs.

Restore 1 of Scenario 1

In the following Restore 1 of Scenario 1, corruption in filegroup `emcdb_fg1` was discovered at 10:00 AM on Tuesday morning:

1. Back up the trailing transaction log.
2. Restore all individual filegroups one at a time:

```
tsimsnap restore -d emcdb -fg Primary
-f c:\metadata\emcdb.dmp
tsimsnap restore -d emcdb -fg emcdb_fg1
-f c:\metadata\emcdb_fg1.dmp
tsimsnap restore -d emcdb -fg emcdb_fg2
-f c:\metadata\emcdb.dmp
```

3. Restore all transaction log backups that were created since Sunday 12:00 PM.

4. Restore the transaction log created at the beginning of the restore process, and stop at a point-in-time before the corruption to recover the database into a consistent state.

Then, corruption in filegroup `emcdb_fg1` was discovered at 10:00 AM on Thursday:

1. Back up the trailing transaction log.
2. Restore all individual filegroups one at a time:

```
tsimsnap restore -d emcdb -fg primary
-f c:\metadata\emcdb.dmp
tsimsnap restore -d emcdb -fg emcdb_fg1
-f c:\metadata\emcdb_fg1.dmp
tsimsnap restore -d emcdb -fg emcdb_fg2
-f c:\metadata\emcdb_fg2.dmp
```

3. Restore all transaction log backups that were created since Sunday 12:00 PM.
4. Restore the transaction log created at the beginning of the restore process, and stop at the point-in-time before the corruption to recover the database into a consistent state.

Again, corruption was discovered on Thursday night:

1. Back up the trailing transaction log.
2. Restore all individual filegroups one at a time:

```
tsimsnap restore -d emcdb -fg primary
-f c:\metadata\emcdb_primary.dmp
tsimsnap restore -d emcdb -fg emcdb_fg1
-f c:\metadata\emcdb_fg1.dmp
tsimsnap restore -d emcdb -fg emcdb_fg2
-f c:\metadata\emcdb_fg2.dmp
```

3. Restore all transaction log back ups that were created since Monday 12:00 PM.
4. Restore the transaction log created at the beginning of the restore process, and stop at the point-in-time before the corruption to recover the database into a consistent state.

Restore 2 of Scenario 1

In the following Restore 2 of Scenario 1, a media failure on a Symmetrix device used by `emcdb_fg1` was discovered at 10:00 AM on Tuesday.

1. Back up the trailing transaction log.
2. Restore filegroup `emcdb_fg1`:

```
tsimsnap restore -d emcdb -fg emcdb_fg1
-f c:\metadata\emcdb_fg1.dmp
```
3. Restore all transaction log backups that were created since filegroup `emcdb_fg1` was backed up on Monday at 12:00 PM.
4. Restore the transaction log created at the beginning of the restore process to recover the database into consistent state.

Backup Scenario 2

For Backup Scenario 2, we need to back up the full database once a week using `tsimsnap backup -fg` on each filegroup in the database. Then use `tsimsnap backup -fg` to back up individual filegroups during the week, see Figure 7-6:

1. Create a complete database filegroup backup set every Sunday at midnight:

```
tsimsnap backup -d emcdb -fg primary
-f c:\metadata\emcdb_primary.dmp
tsimsnap backup -d emcdb -fg emcdb_fg1
-f c:\metadata\emcdb_fg1.dmp
tsimsnap backup -d emcdb -fg emcdb_fg2
-f c:\metadata\emcdb_fg2.dmp
```
2. Back up the transaction log every 15 minutes (Enterprise Manager or Transact SQL).
3. Back up filegroup `emcdb_fg1` Monday at midnight (updated frequently):

```
tsimsnap backup -d emcdb -fg emcdb_fg1
-f c:\metadata\emcdb_fg1.dmp
```

This backup overwrites the BCV copy of the filegroup created by previous full database backup.

4. Back up the transaction log every 15 minutes (Enterprise Manager or Transact SQL).

5. Back up filegroup `emcdb_fg` Wednesday at midnight (updated frequently):

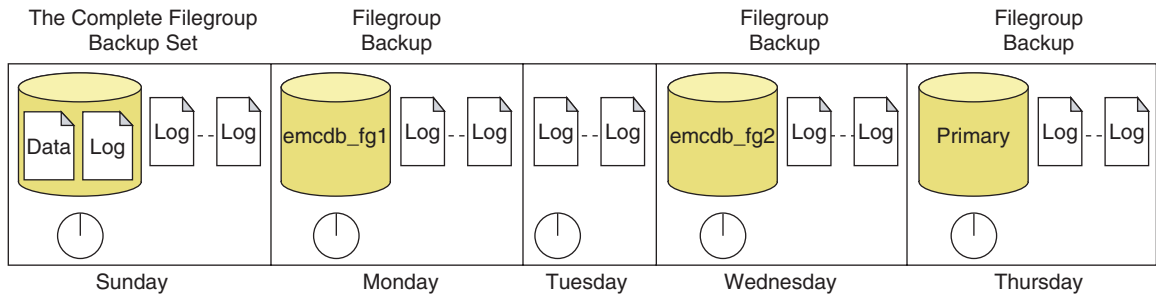
```
tsimsnap backup -d emcdb -fg emcdb_fg2
-f c:\metadata\emcdb_fg2.dmp
```

This back up overwrites the BCV copy of the filegroup created by previous full database backup.

6. Back up the transaction log every 15 minutes (Enterprise Manager or Transact SQL).
7. Back up filegroup `primary` Thursday at midnight (updated frequently):

```
tsimsnap backup -d emcdb -fg primary
-f c:\metadata\emcdb_primary.dmp
```

This backup overwrites the BCV copy of the filegroup created by previous full database backup.



SSPI-000006

Figure 7-6 Database Backup Schedule for Example Scenario 2

Restore 1 of Scenario 2

In the following Restore 1 of Scenario 2, corruption in filegroup emcdb_fg1 was discovered at 10:00 AM on Tuesday.

1. Back up the trailing transaction log.
2. Restore all individual filegroups one at a time.


```
tsimsnap restore -d emcdb -fg primary
                -f c:\metadata\emcdb_primary.dmp
tsimsnap restore -d emcdb -fg emcdb_fg1
                -f c:\metadata\emcdb_fg1.dmp
tsimsnap restore -d emcdb -fg emcdb_fg2
                -f c:\metadata\emcdb_fg2.dmp
```
3. Restore all transaction log backups that were created since Sunday 12:00 PM.
4. Restore the transaction log created at the beginning of the restore process, and stop at the point-in-time before the corruption to recover the database into a consistent state.

Restore 2 of Scenario 2

In the following Restore 2 of Scenario 2, corruption in filegroup emcdb_fg1 was discovered at 10:00 AM on Thursday.

1. Back up the trailing transaction log.
2. Restore all individual filegroups one at a time:


```
tsimsnap restore -d emcdb -fg primary
                -f c:\metadata\emcdb_primary.dmp
tsimsnap restore -d emcdb -fg emcdb_fg1
                -f c:\metadata\emcdb_fg1.dmp
tsimsnap restore -d emcdb -fg emcdb_fg2
                -f c:\metadata\emcdb_fg2.dmp
```
3. Restore all transaction log backups that were created since Sunday 12:00 PM.
4. Restore the transaction log created at the beginning of the restore process, and stop at the point-in-time before the corruption to recover the database into a consistent state.

Restore 3 of Scenario 2

Then, if the corruption was discovered after the primary filegroup on Thursday night, we would need to do the following:

1. Back up the trailing transaction log.
2. Restore all individual filegroups one at a time:

```
tsimsnap restore -d emcdb -fg primary
                  -f c:\metadata\emcdb_primary.dmp
tsimsnap restore -d emcdb -fg emcdb_fg1
                  -f c:\metadata\emcdb_fg1.dmp
tsimsnap restore -d emcdb -fg emcdb_fg2
                  -f c:\metadata\emcdb_fg2.dmp
```

3. Restore all the transaction log backups that were created since Monday 12:00 PM.
4. Restore the transaction log created at the beginning of the restore process, and stop at the point-in-time before the corruption to recover the database into a consistent state.

Restore 4 of Scenario 2

Again, a media failure on a Symmetrix device used by `emcdb_fg1` was discovered at 10:00 AM on Tuesday.

1. Back up the trailing transaction log.
2. Restore filegroup `emcdb_fg1`:

```
tsimsnap restore -d emcdb -fg emcdb_fg1
                  -f c:\metadata\emcdb_fg1.dmp
```

3. Restore all transaction log backups that were created since filegroup `emcdb_fg1` was backed up on Monday at 12:00 PM.
4. Restore the transaction log created at the beginning of the restore process to recover the database into a consistent state.

ResourcePak Command Reference

This appendix describes the syntax and parameters of the SYMCLI ResourcePak commands that support Windows disk management and backup operations in a TimeFinder or business continuance storage environment. The commands appear in the following order:

◆ symntctl	A-3
◆ ExBackup2.....	A-11
◆ ExBackup2000.....	A-15
◆ ExBackup2003.....	A-20
◆ ExBackupCommander2	A-24
◆ tsimsnap	A-28
◆ tsimsnap2	A-33

SYMCLI Conventions

Categories of information shown below (similar to UNIX man pages) are listed for each command, where applicable.

- ◆ **Command name** appears in **bold** typeface at the top of a page followed by a brief description of what the function does.
- ◆ **SYNTAX** lists the arguments and options for each command.
- ◆ **DESCRIPTION** provides a description of the command.
- ◆ **ARGUMENTS** explains the command arguments.
- ◆ **OPTIONS** explains the command options.
- ◆ **PARAMETERS** explains the command parameters.
- ◆ **RETURN CODES** specifies the primary success and failure codes for each command.
- ◆ **EXAMPLES** provides examples of the syntax and output, if any, of the command.

symntctl

This SIU command integrates and extends the, otherwise limited, Windows 2000 disk management functionality so that it operates with and on the Symmetrix Business Continuance storage devices more effectively.

SYNTAX

```
symntctl -h
```

```
symntctl
  list
```

```
    -physical [-brief]
    -volume [-brief]
    -pd diskN
    -vol VolName [-dg DgName] [-brief]
```

```
signature -pd diskN -save|-restore|-sig Signature|
          -erase|-initialize
```

```
mount <-vol VolName [-dg DgName]>|-guid VolGuid|-sid SymId -symdev SymDev
      -drive DriveLetter
      -path MountPnt
      -part Partition
```

```
umount [-nolock]
      -drive DriveLetter
      -path MountPnt
      -vol VolName
      -guid VolGuid
```

```
flush
      -drive DriveLetter
      -path MountPnt
      -vol VolName [-dg DgName]
      -guid VolGuid
```

```
openhandle
      -drive DriveLetter
      -path MountPnt
      -vol VolName [-dg DgName]
      -guid VolGuid
```

```
locks
      -releaseall
      -release VolGuid
      -listall
```

```
mask -sid SymID -symdev SymDev
```

```

unmask -sid SymID -symdev SymDev

symntctl rescan

symntctl -dg DgName [-c]
    deport
    import

```

DESCRIPTION This command integrates and extends the, otherwise limited, Windows 2000 resource management functionality so that it operates with and on the Symmetrix Business Continuance storage devices (volumes) more effectively.

ARGUMENTS `deport`

Deports dynamic disks of a specified VxVM disk group. A disk group consists of devices that are logically grouped together in a VERITAS database. (VxVM must be installed.)

`import`

Imports a specified disk group from another system (such as a production server). (VxVM must be installed.)

`flush`

Causes all pending unwritten file system entries in cache to be flushed to disk.

`list`

Lists all visible physical devices or volumes. Or lists specific disk numbers or volume names.

`locks`

Controls file system locks held on devices typically during TimeFinder establish and split operations. Currently, you can only release locks.

`mask`

Removes access to the specified Symmetrix device on all HBAs on the host where the specified device is visible.

`unmask`

Adds access to the specified Symmetrix device on all HBAs on the host that are connected to the specified Symmetrix unit.

mount

Mounts the specified volume name or GUID to the specified drive letter or mount point.

openhandle

Displays any open sessions (processes) working with the specified drive or mount point. This command is typically called prior to an unmount or split command while running diagnostics.

umount

Unmounts the specified volume from the specified drive letter or mount point. The unmount process flushes any pending writes to it and locks the driver from further use.

rescan

Scans the drive connections and discovers any new disks available to the system. (VxVM must be installed.)

signature

Manipulates the disk signature of a specified disk.

OPTIONS**-brief**

Requests an abbreviated display of information associated with the specified list action.

-c

Clears the host id.

-dg

Specifies a device group (volume group) as the target for the specified action.

-drive

Specifies a drive as the target for the specified action.

-erase

Requests the signature of the specified disk to be erased.

`-guid`

Specifies a volume's global unique identifier as the target for the specified action.

`-initialize`

Assigns a signature to any disks found without a signature.

`-listall`

Lists all of the locks currently held by the SIU service.

`-nolock`

Skips the auto-lock behavior in the specified (`umount`) action.

`-path`

Specifies a device mount point as the target to the specified action. This directory path (of the form `device:\dir`) must be empty.

`-pd`

Specifies a physical disk as the target for the specified action. Note that the host-visible disk identifiers of the form `diskN` can be viewed with the `list -physical` command.

`-physical`

Specifies a drive as the target for the specified action.

`-release`

Releases the lock on a specified volume, as identified by its GUID.

`-releaseall`

Releases all file system locks held on devices.

`-restore`

Requests the signature of the specified disk to be restored from the `EMC_TEMP_SIGNATURE` registry.

`-save`

Requests the signature of the specified disk to be saved to the `EMC_TEMP_SIGNATURE` registry.

-sid

Specifies the ID of the Symmetrix unit containing the volume on which the action is to be performed.

-symdev

Specifies the ID of the Symmetrix device on which the action is to be performed.

-sig

Specifies a new signature to the specified disk.

-vol

Specifies a volume name as the target for the specified action.

-volume

Confines the list action to just displaying volume configuration across the system.

PARAMETERS

diskN

The number of the physical disk in the system of the form diskN.

DgName

The name of the device group.

DriveLetter

The drive letter designation as viewed in the Windows directories (such as E:).

MountPnt

A device mount point or directory path (of the form *device:\dir*).

Partition

The partition number (greater than, or equal to one) on the Symmetrix device that is to be mounted. If omitted, this value defaults to one.

Signature

An 8-digit hex number for each disk. A record of assigned signatures are saved in the EMC_TEMP_SIGNATURE registry.

SymID

A 2 to 12-digit Symmetrix ID.

SymDev

A 3 to 5-digit Symmetrix device ID.

VolName

The volume name of the device.

VolGuid

The global unique identifier (128-bit integer) of a volume. For example: Volume{d33eea9d6-1320-11d5-b37c-806d6172696f}

RETURN CODES

The following are possible status or error codes that can be returned by this command:

- 0 Command was successful
- 1 Command failed

EXAMPLES

To deport VxVM disk group *group1*, enter:

```
symmtctl deport -dg group1
```

To import VxVM disk group *group1* to the system, enter:

```
symmtctl import -dg group1
```

To flush any unwritten file system buffers to drive *E*, enter:

```
symmtctl flush -drive E:
```

To flush any unwritten file system buffers to mount point *E:\drivex*, enter:

```
symmtctl flush -path E:\drivex
```

To flush any unwritten file system buffers to volume *volumex*, enter:

```
symmtctl flush -vol volumex
```

To flush a volume with a GUID of

Volume{ecba40b5-d522-11d5-98cb-00b0d0b03303}, enter:

```
symmtctl flush -guid Volume{ecba40b5-d522-11d5-98cb-00b0d0b03303}
```

To list information about the physical configuration of all devices, enter:

```
symmtctl list -physical
```

To list the physical configuration for disk 3, enter:

```
symntctl list -pd disk3
```

The following example output displays after entering `symntctl list -vol` for volume `HarddiskVolume7`:

Volume Information

```
[6] Vol Name: HarddiskVolume7
    Dev Group:
    GUID: Volume{ecba40b5-d522-11d5-98cb-00b0d0b03303}
    Mount Point: 1
    h:\
    Partition:
    Disk 6, Starting: 0 MB Length: 4494 MB
```

To release all the locks cached by the SIU service, enter:

```
symntctl locks -releaseall
```

To mount a basic volume called `volumex` to drive `x`, enter:

```
symntctl mount -drive x -vol volumex
```

To mount a dynamic volume called `volumex` of `devicegroupx` to mount point `x:\volumex`, enter:

```
symntctl mount -path x:\volumex -vol volumex -dg devicegroupx
```

To mount a volume with the a GUID of

`Volume{ecba40b5-d522-11d5-98cb-00b0d0b03303}` to drive `x`, enter:

```
symntctl mount -drive x -guid Volume{ecba40b5-d522-11d5-98cb-00b0d0b03303}
```

To unmount a volume associated with drive `x`, enter:

```
symntctl umount -drive x
```

To unmount a volume called `volumex` of `devicegroupx`, enter:

```
symntctl umount -vol volumex -dg devicegroupx
```

To unmount a volume with a GUID of

`Volume{ecba40b5-d522-11d5-98cb-00b0d0b03303}` from drive `x`, enter:

```
symntctl umount -drive x:
```

To save the current disk signature, enter:

```
symntctl signature -pd disk1 -save
```

To restore the current disk signature, enter:

```
symntctl signature -pd disk1 -restore
```

To change the signature of disk 4 to 1ED67A70, enter:

```
symntctl signature -pd disk4 -sig 1ED67A70
```

To erase the signature of disk 4, enter:

```
symntctl signature -pd disk4 -erase
```

To initialize the signature of all disks that have 0 for their signatures, enter:

```
symntctl signature -initialize
```

ExBackup2

For Windows 2000, this TEIM command backs up a single or a clustered Exchange 5.5 Server.

SYNTAX

ExBackup2 -h

```
ExBackup2 [-f InitFile | -F InitPath] [-sd symapidb] \
          [-t TimeOut] [-o OutFile] [-p] [-nologdelete]\
          [-hot | -instant] [-norestart] [-v]\
          -s ExchgServer |
          -c ClustName
```

DESCRIPTION

This command for Windows 2000 with Exchange Server 5.5, produces an exact copy of the production devices that hold the Exchange information (data and logs). With the valid backup copy, you can perform both full and single mailbox restores when needed.

ARGUMENTS

None.

OPTIONS

-c

Specifies an MSCS cluster name for the backup operation.

-f

Specifies an initialization file (in the SYMCLI working directory) that contains the services to stop and restart (freeze), during the backup. For information about creating this file, see *Creating a Backup Command Initialization File* on page 5-15.

-F

Specifies an initialization file (full path when not in SYMCLI directory) that contains the services to stop and restart (freeze), during the backup operation.

-h

Provides brief, online help information.

-hot

Specifies that a hot split will be performed in the backup operation, where TEIM performs an online snapshot of the Exchange database (Exchange is not stopped before the split). The split is assisted with the instant TimeFinder split behavior. Note that this option overrides and ignores the StopServices request list in the initialization file.

-instant

Specifies an instant split be performed (as opposed to a normal split) on the production/BCV pair (for Enginuity 5x66 or 5x67 versions). (Not required when the -hot option is being specified or for 5x68 versions or greater.)

-nologdelete

Specifies that TEIM is not the manager of the production server transaction logs. No logs will be deleted by TEIM.

-norestart



CAUTION

Specifies that the backup services are not restarted when this backup command fails. Be sure this is the behavior you need to apply as your services will remain off.

-o

Specifies a program output file to record backup activity.

-p

Specifies a pause action at the end of the backup operation that keeps the console window open.

-s

Specifies an Exchange server name for the backup operation. (For non-clustered servers.)

-sd

Specifies an alternate WideSky SYMAPI database file when not using the WideSky default file name.

-t

Specifies a timeout period for backup operation if other than the default value of 10 minutes.

-v

Provides a more detailed, verbose listing.

PARAMETERS

InitFile

The initialization file name in the SYMCLI working directory containing the services to stop and restart (freeze), during the backup. For file format, see *Creating a Backup Command Initialization File* on page 5-15.

InitPath

The initialization file full path name (when not in SYMCLI directory) containing the services to stop and restart, during the backup.

OutFile

Program output file name to record backup activity.

symapidb

An alternate WideSky SYMAPI database file name when not using the default WideSky SYMAPI file name.

TimeOut

Timeout period in minutes for full BCV synchronization (establish).

RETURN CODES

Upon success, the command returns a zero. For various failures and warnings, the command returns a non-zero value. For further information about all possible return codes, see header file `ExBackup2Err.h` in the TEIM directory.

EXAMPLES

To backup the stand alone Exchange server, Ex1:

1. Stop and start the services identified in `exbackup.ini` using the default SYMAPI database.
2. Run the backup and extend the synchronization timeout to 20 minutes, enter:

```
ExBackup2 -s Ex1 -f exbackup.ini -t 20
```

To backup the MSCS clustered Exchange server, `Excs1`:

1. Use `exchclus.ini` to identify the resources to be stopped.
2. Run the backup using the `sac1sdb.bin` SYMAPI database with a verbose output to file `ex1bulog`, enter:

```
ExBackup2 -c Excs1 -f exchclus.ini -sd sac1sdb.bin  
          -o ex1bulog -v
```

ExBackup2000

For Windows 2000 Servers, this TEIM command backs up a single or a clustered Exchange 2000 Server or SharePoint Portal Server.

SYNTAX

```
ExBackup2000 -h
```

```
ExBackup2000 <-s ServerName [-sps]>|
               -c ClustName

               [-sg StorGroup] [-o OutFile] [-f InitFile]\
               [-srdf [-nobrbcv]] [-hot | -instant]\
               [-v] [-nologdelete] [-test]\
               [-full] [-multi] [-snap]\
               [-lock [list | releaseall |
                       release -sid SymID]
               [-lockid LockID] [-sid SymID]]
```

DESCRIPTION

This command for Windows 2000 with Exchange Server 2000 or SharePoint Portal Server, produces an exact copy of the production devices that hold the Exchange Information (data and logs). With the valid backup copy, you can perform both full and single mailbox restores when needed.

ARGUMENTS

None.

OPTIONS

-c

Specifies an MSCS cluster name for the backup operation.

-f

Specifies an initialization file that lists multiple production server names to be involved in the backup operation.

-full

Performs a full establish on all BCVs in the backup.

-h

Provides brief, online help information.

`-hot`

Specifies that a hot split will be performed in the backup operation, where TEIM performs an online snapshot of the Exchange database (Exchange is not stopped before the split). The split is assisted with the instant TimeFinder split behavior.

`-instant`

Specifies an instant split be performed (as opposed to a normal split) on the production/BCV pair (for Symmetrix Enginuity versions 5x66 or 5x67). Not required when the `-hot` option is being specified or for 5x68 or greater. Instant split behavior is the default mode for Symmetrix 5x68 Enginuity levels and above.

`-lock`

Specifies to use long duration locks on all BCVs/VDEVs. `-lock list` lists all of the locks currently held by the TEIM. `-lock releaseall` releases all the locks held by the TEIM. `-lock release -sid SymID` releases the locks for the specified Symmetrix unit.

`-lockid`

Specifies that the TEIM should use an existing lock holder ID.

`-multi`

Uses multiple BCVs in a rotating fashion (oldest first).

`-nobrabcv`

Specifies that no BCVs should be used on the remote Symmetrix for this SRDF backup.

`-nologdelete`

Specifies that TEIM is not the manager of the production server transaction logs. No logs will be deleted by TEIM.

`-o`

Specifies a program output file to record backup activity.

`-s`

Specifies a server name (Exchange or SharePoint server) for the backup operation. (For non-clustered servers.)

-sg

Targets a specific storage group to back up.

-sid

Specifies the ID of the Symmetrix unit on which the action is to be performed.

When used with the -lockid option, this option identifies the ID of the locked Symmetrix unit.

-snap

Use EMC Snap to perform the snapshots.

-sps

Specifies that the *ServerName* specified with the -s option is a SharePoint Portal Server name for the backup operation.

-srdf

The operation will be a backup to the remote Symmetrix using the SRDF.

-test

Specifies that the backup command execution entered on the command line is a test and will not execute any controls on devices, BCV devices in the database and not actually start the backup processes (such as establishing BCV pairs or dismounting devices). Only the command validation and checking elements are performed (such as checking Engineuity levels or Exchange versions).

-v

Provides a more detailed, verbose listing.

PARAMETERS

ClustServer

An MSCS cluster name for the backup operation.

InitFile

Initialization file name that contains a list of multiple production server names involved in the backup operation.

OutFile

Program output file name to record backup activity.

ServerName

An Exchange or SharePoint Portal server name for the backup operation.

StorGroup

The storage group name to be backed up.

SymID

A 2 to 12-digit Symmetrix ID.

RETURN CODES

Upon success, the command returns a zero. For various failures and warnings, the command returns a non-zero value. For further information about all possible return codes, see header file `ExBackup2000Err.h` in the TEIM directory.

EXAMPLES

To back up an Exchange 2000 server named `Ex1` in verbose mode, enter:

```
ExBackup2000 -s Ex1 -v
```

To back up a single storage group, `SG1`, on the Exchange 2000 server named `Ex1` using instant splits, enter:

```
ExBackup2000 -s Ex1 -sg SG1 -instant
```

To back up a single virtual server, `VS1`, of the clustered Exchange 2000 server named `Excs1` in verbose mode, enter:

```
ExBackup2000 -s VS1 -v
```

To perform a local TimeFinder backup and a remote SRDF backup of server `EX1`, exercising the instant split behavior, enter:

```
ExBackup2000 -s EX1 -srdf -instant
```

To test a hot split backup of a single server, `Ex1` in verbose mode, enter:

```
ExBackup2000 -s Ex1 -hot -v -test
```

To backup a single SharePoint Portal Server, `SPS1`, using hot splits and sending all output to `sps.out`, enter:

```
ExBackup2000 -s SPS1 -sps -hot -o sps.out
```

To back up an Exchange 2000 server named `Ex1`, using long duration locks, hot splits, and in verbose mode, enter:

```
ExBackup2000 -s Ex1 -hot -lock -v
```

To list the long duration locks held by the TEIM, enter:

```
ExBackup2000 -lock list
```

To release all of the TEIM's long duration locks for Symmetrix 000187900754, enter:

```
ExBackup2000 -lock release -sid 000187900754
```

ExBackup2003

For Windows 2000/2003 Servers, this TEIM command backs up a single or a clustered Exchange 2003 Server.

SYNTAX

```
ExBackup2003 -h

ExBackup2003 <-s ServerName> |
    -c ClustName

    [-sg StorGroup] [-o OutFile] [-f InitFile]\
    [-srdf [-nobrabcv]] [-hot | -instant]\
    [-v] [-nologdelete] [-test]\
    [-full] [-multi] [-snap]\
    [-lock [list | releaseall |
        release -sid SymID]
        [-lockid LockID] [-sid SymID]]
```

DESCRIPTION

This command for Windows 2000 with Exchange Server 2000 or SharePoint Portal Server, produces an exact copy of the production devices that hold the Exchange Information (data and logs). With the valid backup copy, you can perform both full and single mailbox restores when needed.

ARGUMENTS

None.

OPTIONS

-c

Specifies an MSCS cluster name for the backup operation.

-f

Specifies an initialization file that lists multiple production server names to be involved in the backup operation.

-full

Performs a full establish on all BCVs in the backup.

-h

Provides brief, online help information.

-hot

Specifies that a hot split will be performed in the backup operation, where TEIM performs an online snapshot of the Exchange database (Exchange is not stopped before the split). The split is assisted with the instant TimeFinder split behavior.

-instant

Specifies an instant split be performed (as opposed to a normal split) on the production/BCV pair (for Symmetrix Enginuity versions 5x66 or 5x67). Not required when the -hot option is being specified or for 5x68 or greater. Instant split behavior is the default mode for Symmetrix 5x68 Enginuity levels and above.

-lock

Specifies to use long duration locks on all BCVs/VDEVs. -lock list lists all of the locks currently held by the TEIM. -lock releaseall releases all the locks held by the TEIM. -lock release -sid *SymID* releases the locks for the specified Symmetrix unit.

-lockid

Specifies that the TEIM should use an existing lock holder ID.

-multi

Uses multiple BCVs in a rotating fashion (oldest first).

-nobrabcv

Specifies that no BCVs should be used on the remote Symmetrix for this SRDF backup.

-o

Specifies a program output file to record backup activity.

-s

Specifies a server name (Exchange or SharePoint server) for the backup operation. (For non-clustered servers.)

-sg

Targets a specific storage group to back up.

`-sid`

Specifies the ID of the Symmetrix unit on which the action is to be performed.

When used with the `-lockid` option, this option identifies the ID of the locked Symmetrix unit.

`-snap`

Use EMC Snap to perform the snapshots.

`-srdf`

The operation will be a backup to the remote Symmetrix using the SRDF.

`-test`

Specifies that the backup command execution entered on the command line is a test and will not execute any controls on devices, BCV devices in the database and not actually start the backup processes (such as establishing BCV pairs or dismounting devices). Only the command validation and checking elements are performed (such as checking Enginuity levels or Exchange versions).

`-v`

Provides a more detailed, verbose listing.

PARAMETERS

ClustServer

An MSCS cluster name for the backup operation.

InitFile

Initialization file name that contains a list of multiple production server names involved in the backup operation.

LockID

A lock holder ID.

OutFile

Program output file name to record backup activity.

ServerName

An Exchange or SharePoint Portal server name for the backup operation.

StorGroup

The storage group name to be backed up.

SymID

A 2 to 12-digit Symmetrix ID.

RETURN CODES

Upon success, the command returns a zero. For various failures and warnings, the command returns a non-zero value. For further information about all possible return codes, see header file `ExBackup2003Err.h` in the TEIM directory.

EXAMPLES

To back up an Exchange 2003 server named `Ex1` in verbose mode, enter:

```
ExBackup2003 -s Ex1 -v
```

To back up a single storage group, `SG1`, on the Exchange 2003 server named `Ex1` using instant splits, enter:

```
ExBackup2003 -s Ex1 -sg SG1 -instant
```

To back up a single virtual server, `VS1`, of the clustered Exchange 2003 server named `Excs1` in verbose mode, enter:

```
ExBackup2003 -s VS1 -v
```

To perform a local TimeFinder backup and a remote SRDF backup of server `EX1`, exercising the instant split behavior, enter:

```
ExBackup2003 -s EX1 -srdf -instant
```

To test a hot split backup of a single server, `Ex1` in verbose mode, enter:

```
ExBackup2003 -s Ex1 -hot -v -test
```

To back up an Exchange 2003 server named `Ex1`, using long duration locks, hot splits, and in verbose mode, enter:

```
ExBackup2003 -s Ex1 -hot -lock -v
```

To list the long duration locks held by the TEIM, enter:

```
ExBackup2003 -lock list
```

To release all of the TEIM's long duration locks for Symmetrix 000187900754, enter:

```
ExBackup2000 -lock release -sid 000187900754
```

ExBackupCommander2

For Windows 2000 systems, this TEIM command backs up multiple Exchange 5.5 Servers through a single backup server.

SYNTAX

`ExBackupCommander2 -h`

`ExBackupCommander2 -f InitFile | -F InitPath`

DESCRIPTION

From a single backup server, this command backs up multiple production Exchange 5.5 servers across a common network to produce exact BCV copies of the Exchange information (data and logs) unique to each specified production server.

The command executes an initialization file that is formatted with separate backup commands which can target each of the production server node names you select with different backup command parameters.

Once each backup command is started on all of the servers in the initialization command list, the ExBackupCommander quietly exits.

ARGUMENTS

None

OPTIONS

`-f`

Specifies an initialization file (in the SYMCLI working directory) that is formatted with separate backup commands which can target each of the production server node names you select with different backup command parameters. For information about creating this file, see *Creating a Backup Command Initialization File* on page 5-15.

`-F`

Specifies an initialization file (full path when not in SYMCLI directory) that contains the backup commands to each of the server nodes.

**INIT FILE COMMAND
PARAMETERS**

The following are possible command parameters to the entries in the initialization file:

cluster

Specifies whether the target server is clustered or stand-alone.
Possible values are:

TRUE — a clustered server

FALSE — a stand-alone server

data

Specifies the device group (name) that contains the Exchange database devices with data.

logs

Specifies the device group (name) that contains the Exchange database devices with transaction logs.

hotsplit

When set to TRUE, specifies that a hot split will be performed in the backup operation, where TEIM performs an online snapshot of the Exchange database (Exchange is not stopped before the split). The split is assisted with the instant TimeFinder split behavior (for 5x66 or greater). This parameter is optional. Possible values are TRUE and FALSE.

Note that this option overrides and ignores the StopServices request list in the initialization file.

output

Specifies a program output file to record backup activity. This parameter is optional.

pause

When set to TRUE, specifies a pause action at the end of the backup operation that keeps the console window open. This parameter is optional. Possible values are TRUE and FALSE.

`restart_services`

When set to TRUE, specifies that the backup services are restarted when this backup command fails. This parameter is optional. Possible values are TRUE and FALSE.

`services`

Specifies an initialization file (just file name or full path name) that contains the services to stop and start the backup operation on that server. This parameter is optional.

`symapidb`

Specifies an alternate WideSky SYMAPI database file when not using the WideSky default file name. This parameter is optional.

`sync_timeout`

Specifies a timeout period for the backup operation, if other than the default value of 600000 minutes. This parameter is optional.

`verbose`

When set to TRUE, provides a more detailed, verbose output display. This parameter is optional. Possible values are TRUE and FALSE

PARAMETERS

InitFile

The initialization file name in the SYMCLI working directory containing the backup commands for each server node. For file format, see *Creating a Backup Command Initialization File* on page 5-15.

InitPath

The initialization file full path name (when not in SYMCLI directory) containing the backup commands for each server node.

RETURN CODES

Upon success, the command returns a zero. For various failures and warnings, the command returns a non-zero value. For further information about all possible return codes, see header file `ExBackup2Err.h` in the TEIM directory.

EXAMPLES

To backup a number of production Exchange servers defined in the initialization file `exbackupglobal.ini` using a Windows 2000 backup server, do the following:

1. Build individual initialization files with start/stop services for each of the production Exchange servers (node names) on the network.
2. On the backup server, code specific command entries for each production server node name in `exbackupglobal.ini` and enter:

```
ExBackupCommander2 -f exbackupglobal.ini
```

tsimsnap

For a stand-alone or a virtual clustered Windows server, this TSIM command can back up or restore a Microsoft SQL Server database.

SYNTAX

```
tsimsnap backup -d SqlDbName -f MetaFile
    [-fg FileGrpName]
    [-s VirtSqlServName[\InstanceName] |
        HostName[\InstanceName]]
    [-nrtgt | -rbcvsplit | -rdfsplit | -snap]
    [-lock [-lockid LockID] [-sid SymID]]
    [-overwrite]

tsimsnap restore -d SqlDbName -f MetaFile
    -norecovery|-recovery|-standby|-fg FileGrpName
    [-s VirtSqlServName[\InstanceName] |
        HostName[\InstanceName]]
    [-snap]
    [-m [-rf LocateFileName]]
    [-lock [-lockid LockID] [-sid SymID]]

tsimsnap -lock [list | releaseall | release -sid SymID]
```

DESCRIPTION

This TSIM command backs up or restores a Microsoft SQL Server database for a stand-alone or a clustered Windows server. Both the backup and restore actions can be confined to a specified filegroup name in the database.

Once you have backed up an exact copy of the production devices that hold the SQL Server information (data and logs), you can perform database or file group restore actions when needed.

The TSIM backup operation:

- ◆ Suspends writes to the specified database/filegroup.
- ◆ Automatically writes metadata information about the specific database/filegroup. Metadata information is normally measured in kilobytes, so it is not necessary to have additional storage.
- ◆ Does the following, depending on whether using TimeFinder or Snap:
 - For TimeFinder, it performs an automatic TimeFinder/SRDF split of the devices associated with the database/filegroup.
 - For Snap, it activates the virtual copy session for the devices used by the database/filegroup.

The restore operation automatically performs the following tasks:

- ◆ Suspends any writes to the database and/or filegroups.
- ◆ Unmounts the file system on the standard host.
- ◆ Does the following, depending on whether using TimeFinder or Snap:
 - For TimeFinder, it performs a TimeFinder restore action, and then splits the restored device from the backup devices.
 - For Snap, it performs a `symsnap restore` action.
- ◆ Mounts the file system on the standard side host.
- ◆ Restores the database and/or filegroup from the metadata file.

If you select manual mode, you can break this overall restore operation into individual tasks. This mode is used for clustered servers or other services that must be turned off with manual intervention. It also allows for a restored database to be relocated. For more detail on manual mode tasks, see *Manual Mode* on page 7-9.

ARGUMENTS

`backup`

Requests a backup operation be performed on a specified SQL Server database or file group.

`restore`

Requests a restore operation be performed on a specified SQL Server database or file group.

OPTIONS

`-d`

Specifies the name of the SQL Server database for the backup or restore action.

`-f`

Specifies the name of a meta file to hold the metadata.

`-fg`

Confines the backup or restore action to a specific file group name.

`-lock`

Specifies to use long duration locks on all BCVs/VDEVs. `-lock list` lists all of the locks currently held by the TSIM. `-lock releaseall` releases all the locks held by the TSIM. `-lock release -sid SymID` releases the locks for the specified Symmetrix unit.

`-lockid`

Specifies that the TSIM should use an existing lock holder ID.

`-m`

Specifies the manual mode that enables you to break the restore operation into individual tasks. Use manual mode for clustered servers, dynamic disks and to initialize standby databases.

`-norecovery`

Requests the database be left in the norecovery mode after a restore operation. An additional transaction log needs to be restored to recover the database to a consistent state. This is one of three states (norecovery, recovery, and standby). (Not used with the `-fg` option.)

`-nrtgt`

Makes the local BCV devices not ready after the `tsimsnap backup` command split the local BCV devices. This option cannot be used with the `-rdfspl` option.

`-overwrite`

Specifies to overwrite any existing database dump file.

`-recovery`

Requests the database be left in the recovery mode (read/write) after a restore operation. This is one of three modes (norecovery, recovery, and standby). (Not used with the `-fg` option.)

`-rbcvsplit`

Specifies to split the remote BCV.

`-rdfspl`

Specifies to split the remote R2 device from the R1.

-remote

Obsolete, can be used for old script compatibility only. Specifies to split the remote BCV. Use **-rbcvsplit** option for this function.

-rf

Specifies the name of the relocation file when in manual mode (**-m**). To locate each database file, the file lists the logical and physical device name where each file resides in the database. For formatting this file, see Figure 7-2 on page 7-11.

-s

Specifies a clustered SQL Server name for its database to be backed up or restored. Or, it can specify a host name\database instance to target the action. Not required for a stand-alone SQL Server default install base.

-sid

Specifies the ID of the Symmetrix unit on which the action is to be performed.

When used with the **-lockid** option, this option identifies the ID of the locked Symmetrix unit.

-snap

Specifies to backup/restore the database using virtual snap devices.

-standby

Requests the database be left in the recovery mode (read/write) after a restore operation. This is one of three modes (norecovery, recovery, and standby). (Not used with the **-fg** option.)

PARAMETERS

HostName\InstanceName

A host name with or without a database instance name.

VirtSqlServName\InstanceName

A cluster name with or without a database instance name.

FileGrpName

The specific filegroup name.

LocateFileName

The name of the relocation file (*filename.txt*).

LockID

A lock holder ID.

MetaFile

The name of a meta file that holds the metadata. Can be a full path name.

SqlDbName

The name of the SQL Server database for the backup or restore action.

SymID

A 2 to 12-digit Symmetrix ID.

RETURN CODES

Upon success, the command returns a zero. For various failures and warnings, the command returns a non-zero value. For further information about all possible return codes, see header file `tsim_Err.h` in the TSIM install directory.

EXAMPLES

To backup filegroup `ProdDbfg03` in database `ProdDB` with the meta file is `n:\ProdDB.dmp`, enter:

```
tsimsnap backup -d ProdDb -f n:\ProdDB.dmp
                -fg ProdDbfg03
```

To restore database `ProdDB` with the meta file is `n:\ProdDB.dmp` and put the database in standby mode, enter:

```
tsimsnap restore -d ProdDb -f n:\ProdDB.dmp -standby
```

To manually restore database `ProdDB` with the meta file `n:\ProdDB.dmp` and put the database in norecovery mode, enter:

```
tsimsnap restore -d ProdDb -f n:\ProdDB.dmp -m
                -norecovery
```

To manually restore database `ProdDB` with the meta file `n:\ProdDB.dmp` and put the database in a new location with file `n:\ProdBlocation2.txt`, and to finally put it in standby mode, enter:

```
tsimsnap restore -d ProdDb -f n:\ProdDB.dmp -m
                -rf ProdBlocation2.txt -standby
```

tsimsnap2

For Windows systems, this TSIM command backs up and restores multiple databases from the specified SQL Server instance.

SYNTAX

```
tsimsnap2 backup -alludb | -instance |
    -d SqlDbName SqlDbName...
    [-f MetaFileDir]
    [-s VirtSqlServName[\InstanceName] |
        HostName[\InstanceName]]
    [-nrtgt | -rbcvsplit | -rdfssplit | -snap] [-overwrite]
    [-lock [-lockid LockID] [-sid SymID]]
```

```
tsimsnap2 restore -d SqlDbName SqlDbName...
    -f MetaFileDir
    -norecovery|-recovery|-standby
    [-s VirtSqlServName[\InstanceName] |
        HostName[\InstanceName]]
    [-lock [-lockid LockID] [-sid SymID]]
```

```
tsimsnap2 -lock [list | releaseall | release -sid SymID]
```

DESCRIPTION

This TSIM command backs up or restores multiple databases for a stand-alone or a clustered SQL Server instance that resides on Symmetrix devices.

The backup operation consolidates the backup timeframes by concurrently backing up the multiple databases. Once you have backed up an exact copy of the production devices that hold the SQL Server information (data and logs), you can perform database or file group restore actions when needed. The backup operation writes information about the specific databases in metafiles stored in the specified meta directory. The default file names take on the form *DbName_snapshot.dmp* for the various meta files in this directory.

If the Symmetrix supports instant split, then instant split TimeFinder behavior will assist a hot-split task portion of the backup activities. Before starting a backup operation, all database devices must be synchronized, and if an SRDF environment exists, R2 devices and their BCVs must be synchronized with R1 devices.

The TSIM backup operation:

- ◆ Suspends writes to the specified databases.
- ◆ Automatically writes metadata information about the specific database. Metadata information is normally measured in kilobytes, so it is not necessary to have additional storage.

- ◆ Performs an automatic TimeFinder/SRDF split of the devices associated with the databases.

The restore operation restores the specified database into the following recovery modes:

- ◆ Norecovery
- ◆ Standby
- ◆ Recovery

ARGUMENTS

backup

Requests a backup operation be performed on a specified SQL Server database or file group.

restore

Requests a restore operation be performed on a specified SQL Server database or file group.

OPTIONS

-alludb

Specifies the backup action to be performed on all user databases of the SQL Server instance.

-instance

Specifies the backup action to be performed on all databases of the SQL Server instance (`tempdb` excluded).

-d

Specifies the database name or names of the SQL Server instance for the backup or restore action.

-f

Specifies the name of the meta file directory to hold the metadata files.

-lock

Specifies to use long duration locks on all BCVs/VDEVs. `-lock list` lists all of the locks currently held by the TSIM. `-lock releaseall` releases all the locks held by the TSIM. `-lock release -sid SymID` releases the locks for the specified Symmetrix unit.

`-lockid`

Specifies that the TSIM should use an existing lock holder ID.

`-norecovery`

Requests the database be left in the norecovery mode after a restore operation. An additional transaction log needs to be restored to recover the database into a consistent state. This is one of three modes (norecovery, recovery, and standby).

`-nrtgt`

Makes the local BCV devices not ready after the `tsimsnap2 backup` command split the local BCV devices.

`-overwrite`

Specifies to overwrite any existing database dump file.

`-recovery`

Requests the database be left in the recovery mode (read/write) after a restore operation. This is one of three modes (norecovery, recovery, and standby).

`-rbcvsplit`

Specifies to split the remote BCV.

`-rdfsplitt`

Specifies to split the remote R2 device from the R1.

`-remote`

Obsolete, can only be used for old script compatibility. Specifies to split the remote BCV. Use `-rbcvsplit` option for this function.

`-s`

Specifies a clustered SQL Server name for its databases to be backed up or restored. Or, it can specify a host name\database instance to target the action. Not required for a stand-alone SQL Server default install base.

`-sid`

Specifies the ID of the Symmetrix unit on which the action is to be performed.

When used with the `-lockid` option, this option identifies the ID of the locked Symmetrix unit.

`-snap`

Specifies to backup/restore the database using virtual snap devices.

`-standby`

Requests the database be left in the recovery mode (read/write) after a restore operation. This is one of three modes (norecovery, recovery, and standby).

PARAMETERS

LockID

A lock holder ID.

MetaFileDir

The name of the meta file directory that holds the metadata files (*DbName_snapshot.dmp*).

HostName\InstanceName

A host name with or without a database instance name.

VirtSqlServName\InstanceName

A virtual SQL Server name with or without a database instance name.

SqlDbName

The name of the SQL Server database for the backup or restore action. More than one database name can be targeted.

SymID

A 2 to 12-digit Symmetrix ID.

RETURN CODES

Upon success, the command returns a zero. For various failures and warnings, the command returns a non-zero value. For further information about all possible return codes, see header file `tsim_Err.h` in the TSIM install directory.

EXAMPLES

To concurrently backup databases `ProdDb` and `ProdPMDB` with the meta files in `n:\SQLMetaFiles`, enter:

```
tsimsnap2 backup -d ProdDb ProdPMDB -f n:\SQLMetaFiles
```

To concurrently backup all user databases on SQL Server Production1\Batch2 instance with the meta files in n:\SQLMetaFiles, enter:

```
tsimsnap2 backup -alludb -f n:\SQLMetaFiles  
-s Production1\Batch2
```

To restore databases ProdDB and ProdPMDb into a recovery mode with the meta files in n:\SQLMetaFiles, enter:

```
tsimsnap2 restore -d ProdDb ProdPMDb -f n:\SQLMetaFiles  
-recovery
```


A

Automatic mode, overriding 7-9

B

backup

for disaster recovery 6-6

for Exchange 2000 server 5-8, 5-11

for Exchange 5.5 Server 5-6

multiple databases 7-13

multiple Exchange 2000 servers 5-14

server, configuring 6-15

backup recovery Exchange 2000 Server
setting up 4-15

BCV device 4-4, 6-4

BCV establishing 4-31

boot 1 configuration steps 4-39

Business Continuity Volumes 4-4, 6-3

C

cache buffer flush 3-13

checkpoint file

location requirement 4-12

circular logging, disabling 4-28

cluster servers

manual mode for 7-9

code examples

for ExBackup2 A-13

for ExBackup2000 A-18, A-19, A-23

for ExBackupCommander2 A-27

for symmctl A-8

for tsimsnap A-32

for tsimsnap2 A-36

concurrent BCVs 6-7

conventions xv

D

dedicated channels 4-25

deporting disk groups 3-9

device groups, creating 4-30

devices

discovering 3-7

scanning 3-7

disaster recovery backup 6-6

disk administrator 4-32

disk groups

configuring 3-4

defining 3-9

deporting 3-9

importing 3-10

disk signatures 3-11

DRU

overview 1-3

requirements 1-5

dual-boot configuration steps 4-39

dynamic disk, creating a BCV 3-19

E

error files, Windows 7-5

event logging, Windows 7-5

ExBackup 2000 syntax A-15, A-20

exbackup.ini 5-20

ExBackup2

code examples A-13

syntax A-11

ExBackup2000, code examples A-18, A-19, A-23

ExBackupCommander
 initialization file, creating 5-15
 ExBackupCommander2
 code examples for A-27
 syntax for A-24
 Exchange 2000 servers, backing up multiple 5-14
 Exchange backup 4-2
 Exchange backup API 1-3
 Exchange backup recovery server 4-15
 Exchange backup server
 configuring TimeFinder for 4-17
 dual-boot configuration steps 4-39
 Exchange Event Service 4-29
 Exchange Server, stand-alone installation steps
 4-27
 Exchange system software 4-9
 exchclus.ini 5-19
 Execution sequence for TSIM 7-4

F

filegroup recovery 7-30
 flush cache 3-13

H

handles 3-15
 HDA and performance 4-25

I

installation
 Exchange system software 4-9
 stand-alone Exchange Server 4-27
 WideSky 4-14, 4-29

L

license keys 1-5
 listing
 disks 3-8
 volumes 3-8
 locks
 on drives 3-16
 releasing 3-16
 Logical Disk Mangager 3-4
 Long Duration Locks
 TEIM 4-8

TSIM 6-7

M

mailbox
 recoveries, TEIM 4-38
 restores 1-3, 4-2
 Manual mode 7-9
 meta volumes, requirements 1-6
 metadata information, saving 7-26, 7-28
 mounting BCV or SRDF volumes 3-14
 multiple BCVs 4-18
 multiple BCVs with TEIM 5-10, 5-13
 multiple databases, backing up 7-13

N

NTFS partitions 4-26

O

open handles 3-15
 Outlook, testing Exchange using 4-29

P

partition cluster size 4-26
 Performance Optimizer 4-26
 Production Exchange 2000 Server, installation
 requirements 4-10
 Production Exchange Server, preinstallation tasks
 4-25
 production server, configuring 6-14, 6-18

R

recovery tips 5-34
 requirements
 DRU 1-5
 SIU 1-5, 3-3
 TEIM 1-5, 4-2
 TSIM 1-5, 6-3
 Rescan, SIU action 3-7
 ResourcePak utilities 1-3
 restoring
 data from the R2 5-31
 data from the remote BCV 5-33
 databases 7-8, 7-15
 other methods for 7-22

- procedures for 5-21
- standard from the R1/BCV 5-32
- the R2 mirror from the remote BRBCV 5-33

S

- setup, TEIM 4-9
- signatures, manipulating 3-11
- SIU
 - actions 3-4
 - command summary 3-6
 - overview 1-3, 3-2
 - requirements 1-5, 3-3
- Snapshot, SQL Server 2000 6-5
- SQL databases, restoring multiple 7-15
- SQL Server
 - and TSIM 1-4, 6-2
 - snapshots 6-5
- SRDF and TEIM 4-7
- standard device 4-4, 6-3
- standby databases 6-6
 - initializing multiple 7-16
- SYMAPI 4-2, 6-2
- symbcv 4-31
- SYMCLI 1-2
- symdbg create 4-31
- syminq 4-31
- symld add 4-31
- Symmetrix Command Line Interface 1-2
- Symmetrix Integration Utilities (see SIU) 3-1
- symmir 4-31
- symnctl
 - code examples A-8
 - flush 3-13
 - list 3-8
 - locks 3-16
 - mount 3-14
 - open handle 3-15
 - rescan 3-7
 - syntax A-3

T

- TEIM
 - action sequences for backup, Exchange 2000 server 5-8, 5-11
 - action sequences for backup, Exchange 5.5 5-6

- command start up 5-5
- configuring a dual-boot backup 4-38
- establishing BCVs 4-31
- operations 5-1
- overview of 4-2
- platforms supported 5-2
- requirements 1-5
- setup for 4-9
- transaction logs 4-25
- TimeFinder 4-2
 - and Exchange 1-3
 - and TSIM 6-3
 - configuring for Exchange backup server 4-17
 - creating a BCV of a dynamic disk 3-19
 - in SQL Server environment 6-9
 - overview 4-4
- TimeFinder device groups, creating 4-30
- TimeFinder-SQL Server Integration Module (see TSIM) 6-1
- transactions, rolling forward 6-5
- TSIM
 - command line entry 7-4
 - configuring backup server 6-15
 - configuring production server 6-14, 6-18
 - executable files 7-5
 - execution sequence 7-4
 - instantaneous database backup 7-26, 7-28
 - multiple standby databases, initializing 7-16
 - overview of 1-4
 - requirements 1-5
 - restore methods, other 7-22
- tsimsnap
 - code examples A-32
 - syntax A-28
- tsimsnap2
 - code examples A-36
 - syntax A-33

U

- unmount operations 3-14
- upgrade options for previous versions 2-2

V

- VERITAS Volume Manager 1-6
- VERITAS Volume Manager dynamic disk groups (VDGs) 3-4

VERITAS Volume Manager for Windows 2000
 (VxVM) 3-3
Virtual Device Interface (VDI) 1-4, 6-2
volume layout, TEIM requirements for 4-11
volume sets, defining 3-9

W

WideSky installation 4-14, 4-29
Windows
 environment 1-5
 error files 7-5
 event logging 7-5
Windows 2000 Exchange 2000 server
 backing up with TEIM 5-8, 5-11