*PRELIMINARY RELEASE*

HITACHI
DATA SYSTEMS

# Hitachi Freedom Storage

# HiCommand™ Protection Services User and Reference Guide

## © 2004 Hitachi Data Systems Corporation, ALL RIGHTS RESERVED

***Notice:*** No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Hitachi Data Systems Corporation.

Hitachi Data Systems reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. Hitachi Data Systems products and services can only be ordered under the terms and conditions of Hitachi Data Systems' applicable agreements. All of the features described in this document may not be currently available. Refer to the most recent product announcement or contact your local Hitachi Data Systems sales office for information on feature and product availability.

This document contains the most current information available at the time of publication. When new and/or revised information becomes available, this entire document will be updated and distributed to all registered users.

## Trademarks

Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., and the Hitachi Data Systems design mark is a trademark and service mark of Hitachi, Ltd.

HiCommand, Hitachi Freedom Storage, Lightning 9900, Thunder 9200, and Thunder 9500 are trademarks of Hitachi Data Systems Corporation in the United States and other countries.

Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

Solaris and Sun are registered trademarks or trademarks of Sun Microsystems in the United States and other countries.

VERITAS is a trademark of VERITAS Software in the United States and other countries.

All other brand or product names are or may be trademarks or service marks of and are used to identify products or services of their respective owners.

## Notice of Export Controls

Export of technical data contained in this document may require an export license from the United States government and/or the government of Japan. Please contact the Hitachi Data Systems Legal Department for any export compliance questions.

## Document Revision Level

| Revision | Date | Description |
|---|---|---|
| MK-93HC039-P | January 2004 | Preliminary Release |

## Source Documents for this Revision

- *HiCommand Protection Services - Copy Controller User's Guide*, 3020-3-D53-30(E) (October 2003) (Hitachi TI source document)
  - Release Notes, HiCommand Protection Service – Copy Controller 01-04 (Windows) (Appendix A of ECN SSD-HPTS-008, rev 0, 27 Nov 2003)
  - Release Notes, HiCommand Protection Service – Copy Controller 01-04 (Solaris) (Appendix A of ECN SSD-HPTS-009, rev 0, 27 Nov 2003)
  - Release Notes, HiCommand Protection Service – Copy Controller 01-04 (HP-UX) (Appendix A of ECN SSD-HPTS-010, rev 0, 27 Nov 2003)
- *HiCommand Protection Services for Microsoft® SQL Server User's Guide*, 3020-3-D55-30(E), Edition 4, October 2003 (Hitachi TI source document)
  - Release Notes, HiCommand Protection Service for Microsoft (R) SQL Server 01-04 (Appendix B of ECN SSD-HPTS-008, rev 0, 27 Nov 2003)
- *HiCommand Protection Services for Microsoft® Exchange Server User's Guide*, 3020-3-D56-30(E), Edition 4, October 2003 (Hitachi TI source document)
  - Release Notes, HiCommand Protection Service for Microsoft (R) Exchange Server 01-04 (Appendix C of ECN SSD-HPTS-008, rev 0, 27 Nov 2003)

## Changes in this Revision

Not applicable (initial release)

## Referenced Documents

- *Hitachi Lightning 9900™ V Series User and Reference Guide*, MK-92RD100
  *Hitachi Lightning 9900™ V Series TrueCopy User and Reference Guide*, MK-92RD108
  *Hitachi Lightning 9900™ V Series ShadowImage User's Guide*, MK-92RD110
  *Hitachi Lightning 9900™ V Series and Lightning 9900™ Command Control Interface (CCI) User and Reference Guide*, MK-90RD011
- *Hitachi Lightning 9900™ User and Reference Guide*, MK-90RD008
  *Hitachi Lightning 9900™ ShadowImage User's Guide*, MK-91RD031
  *Hitachi Lightning 9900™ TrueCopy User and Reference Guide*, MK-91RD051
- *Hitachi Thunder 9500™ V Series User and Reference Guide*, MK-92DF601
  *Hitachi Thunder 9500™ V Series ShadowImage User's Guide*, MK-92DF607
  *Hitachi Thunder 9500™ V Series QuickShadow User's Guide*, MK-93DF666
  *Hitachi Thunder 9500™ V Series Synchronous TrueCopy User's Guide*, MK-92DF608
  *Hitachi Thunder 9500™ V Series Command Control Interface (CCI) User and Reference Guide*, MK-92DF609
- *Hitachi Thunder 9200™ User and Reference Guide*, MK-90DF504
  *Hitachi Thunder 9200™ ShadowImage User's Guide*, MK-91DF541
  *Hitachi Thunder 9200™ Synchronous TrueCopy User's Guide*, MK-92DF579
  *Hitachi Thunder 9200™ Command Control Interface (CCI) User and Reference Guide*, MK-91DF557

# Preface

This document describes and provides instructions for using the HiCommand™ Protection Services software to manage storage on the Hitachi Freedom Storage™ RAID subsystems. This document assumes that:

- The user has a background in data processing and understands peripheral storage device subsystems and their basic functions.
- The user has read and understands the user guide for the subsystem: *Hitachi Lightning 9900™ V Series User and Reference Guide*, *Hitachi Lightning 9900™ User and Reference Guide*, *Hitachi Thunder 9500™ V Series User and Reference Guide*, *Hitachi Thunder 9200™ User and Reference Guide*.
- The user has read and understands the user guide(s) for the data replication functions (e.g., *Hitachi Lightning 9900™ V Series TrueCopy User and Reference Guide*, *Hitachi Lightning 9500™ V Series ShadowImage User's Guide*).
- The user is familiar with the operating system which hosts the HiCommand™ Protection Services software (e.g., Solaris™ OS, Windows® OS).

***Note:*** The term "9900V" refers to the entire Lightning 9900™ V Series subsystem family (e.g., 9980V, 9970V), unless otherwise noted. The term "9900" refers to the entire Lightning 9900™ subsystem family (e.g., 9960, 9910), unless otherwise noted. The term "9500V" refers to the entire Thunder 9500V subsystem family (e.g., 9570V, 9580V), unless otherwise noted.

***Note:*** The use of HiCommand™ Protection Services and all other Hitachi Data Systems services and products is governed by the terms of your license agreement(s) with Hitachi Data Systems.

## Software Version

This document revision applies to HiCommand™ Protection Services version 1.4 and higher.

## Comments

Please send us your comments on this document. Make sure to include the document title, number, and revision. Please refer to specific section(s) and paragraph(s) whenever possible.

- **E-mail:** doc.comments@hds.com
- **Fax:** 858-695-1186
- **Mail:**
  Technical Writing, M/S 35-50
  Hitachi Data Systems
  10277 Scripps Ranch Blvd.
  San Diego, CA 92131

***Thank you!*** (All comments become the property of Hitachi Data Systems Corporation.)

# Contents

**Chapter 1 Overview of HiCommand™ Protection Services ..... 1**

1.1 Protection Services Features ..... 2
1.2 Key Concepts ..... 4
1.2.1 Dictionary Map File ..... 4
1.2.2 Copy Group ..... 5
1.3 Protection Services Functions ..... 6
1.4 Protection Services Components ..... 7
1.5 Protection Services System Requirements ..... 8
1.5.1 Host Requirements ..... 8
1.5.2 Storage Subsystem Requirements ..... 10
1.5.3 Notes on Volume Configuration ..... 11
1.5.4 Notes on Using an Exchange Server Database ..... 15
1.5.5 Notes on Using an SQL Server Database ..... 17
1.6 Protection Services-Cooperative Software ..... 18
1.7 Protection Services System Configurations ..... 19
1.7.1 Configuration for Backing Up and Restoring Data Between Volumes ..... 20
1.7.2 Configuration for Backing Up and Restoring Data to/from Tape ..... 21
1.7.3 Configuration for Restoring Data on a Different Host (SQL Server only) ..... 22
1.7.4 Configuration for Using the SQL Server Log-Shipping Functionality ..... 23

**Chapter 2 Creating an Environment for Protection Services ..... 25**

2.1 Overview of Environment Setup ..... 25
2.2 Setting up the Environment for Prerequisite Products ..... 27
2.2.1 Setting Up CCI ..... 27
2.3 Installing Protection Services ..... 31
2.3.1 Installing Protection Services in the Solaris Environment ..... 31
2.3.2 Installing Protection Services in the HP-UX Environment ..... 32
2.3.3 Installing Protection Services for SQL Server or Exchange Server ..... 33
2.4 Setting Environment Variables in UNIX ..... 35
2.4.1 PATH Environment Variable ..... 35
2.4.2 MANPATH Environment Variable ..... 35
2.5 Setting Up Linkage with a Backup Management Product ..... 36
2.5.1 Registering Parameters ..... 36
2.5.2 Creating Configuration Definition Files ..... 37
2.6 Setting Up Linkage with CCI ..... 40
2.6.1 Setting Up Instance Numbers ..... 40
2.6.2 Setting Up the Parameters for Checking the Status of a Pair ..... 41
2.6.3 Setting Up the Track Size for Copying Data ..... 43
2.7 Setting Up Operation of Protection Services ..... 44
2.7.1 Setting Up the Parameters for Checking the Status of Cluster Resources ..... 44
2.7.2 Setting up the Parameters for Checking the Status of a Process ..... 45
2.7.3 Setting Up the Backup Option (SQL Server only) ..... 46
2.7.4 Setting Up the Dictionary Map Synchronous Option ..... 46

2.8 Setting Up a Cluster Environment ..... 47
2.8.1 Using a Cluster Configuration in the Active-Passive Type ..... 47
2.8.2 Using a Cluster Configuration in the Active-Active Type ..... 48
2.9 Creating the Dictionary Map File ..... 49
2.10 Backing Up the Operating Environment of Protection Services ..... 50
2.11 Uninstalling Protection Services ..... 51
2.11.1 Uninstalling Protection Services in Solaris ..... 52
2.11.2 Uninstalling Protection Services in HP-UX ..... 52
2.11.3 Uninstalling Protection Services in Windows ..... 53

**Chapter 3 Using Extended Commands ..... 55**

3.1 Overview of Extended Commands ..... 56
3.1.1 List of Extended Commands ..... 57
3.1.2 Before Executing Extended Commands ..... 58
3.1.3 Notes on Executing the Extended Commands ..... 60
3.2 System Configuration Examples ..... 61
3.2.1 System Configuration: Backing Up and Restoring Data Between Volumes ..... 61
3.2.2 System Configuration: Performing Tape Backups and Restorations ..... 62
3.2.3 System Configuration: File/Database Server in a Cluster Configuration ..... 63
3.3 Preparations for Executing Extended Commands ..... 66
3.3.1 Creating VDI Metafile Storage Directories (SQL Server) ..... 67
3.3.2 Creating a Temporary Directory for Extended Commands ..... 67
3.3.3 Setting the Operating Environment for Executing Extended Commands ..... 69
3.3.4 Creating an Operation Definition File (for UNIX) ..... 70
3.3.5 Creating an Operation Definition File (for Windows) ..... 74
3.3.6 Creating Host Environment Settings Files ..... 84
3.3.7 Checking the FTP Service (for Tape Backups) ..... 85
3.4 Procedures of Extended Commands ..... 86
3.4.1 Backing Up a File System or Database to a Secondary Volume ..... 86
3.4.2 Restoring a File System or Database to a Primary Volume ..... 88
3.4.3 Backing Up a File System or Database to Tape (Always-Split Mode) ..... 90
3.4.4 Backing Up a File System or Database to Tape (Always-Paired Mode) ..... 96
3.4.5 Restoring a File System or Database from Tape ..... 102
3.5 Examples of Using Extended Commands (Copy Controller in UNIX) ..... 105
3.5.1 Example of Backing Up File Systems ..... 107
3.5.2 Example of Restoring a File System ..... 108
3.5.3 Example of Restoring Data Between Volumes ..... 109
3.6 Examples of Using Extended Commands (Copy Controller in Windows) ..... 110
3.6.1 Example of Backing Up File Systems ..... 112
3.6.2 Example of Restoring a File System ..... 113
3.6.3 Example of Restoring Data Between Volumes ..... 114
3.7 Examples of Using Extended Commands (SQL Server) ..... 115
3.7.1 Example of Backing Up the SQL Server Database ..... 117
3.7.2 Example of Restoring the SQL Server Database ..... 119
3.7.3 Example of Restoring Data Between Volumes for SQL Server ..... 121

3.8 Examples of Using Extended Commands (Exchange Server) ..... 122
3.8.1 Examples of Backing Up the Exchange Database ..... 124
3.8.2 Example of Restoring Exchange Server ..... 126
3.8.3 Example of Restoring Data Between Volumes ..... 128
3.9 Log Files for Extended Commands ..... 129
3.10 Extended Command Specifications ..... 131
3.10.1 EX_DRM_BACKUPID_SET (generate a backup ID file) ..... 131
3.10.2 EX_DRM_CACHE_PURGE (clear the secondary-volume cache)..... 132
3.10.3 EX_DRM_CG_DEF_CHECK (check the contents of a copy group list file)..... 135
3.10.4 EX_DRM_DB_EXPORT (export a backup record to a file) ..... 136
3.10.5 EX_DRM_DB_IMPORT (import a backup record from a file)..... 138
3.10.6 EX_DRM_FS_BACKUP (back up the file system)..... 139
3.10.7 EX_DRM_FS_DEF_CHECK (check contents of operation definition file)..... 141
3.10.8 EX_DRM_FS_RESTORE (restore a file system to the primary volume)..... 144
3.10.9 EX_DRM_FTP_GET (get backup record file/metafiles from backup server). 146
3.10.10EX_DRM_FTP_PUT (send backup record file/metafiles to backup server) .. 148
3.10.11EX_DRM_HOST_DEF_CHECK (check contents of host env. settings file) ..... 150
3.10.12EX_DRM_RESYNC (resynchronize a copy group) ..... 153
3.10.13EX_DRM_TAPE_BACKUP (back up secondary vol. data/metafiles to tape) .. 156
3.10.14EX_DRM_TAPE_RESTORE (restore data from backup tape to S-VOL)..... 159
3.11 Extended Command Specifications (SQL Server only) ..... 164
3.11.1 EX_DRM_SQL_BACKUP (back up the file system) ..... 164
3.11.2 EX_DRM_SQL_DEF_CHECK (check the operation definition file)..... 166
3.11.3 EX_DRM_SQL_RESTORE (restore SQL Server DB to primary volume) ..... 168
3.11.4 EX_DRM_SQL_TLOG_BACKUP (back up the SQL Server transaction log) ..... 170
3.11.5 EX_DRM_SQLFILE_EXTRACT (deploy the SQL Server metafiles)..... 171
3.11.6 EX_DRM_SQLFILE_PACK (back up the SQL Server metafiles) ..... 172
3.12 Extended Command Specifications (Exchange Server only) ..... 174
3.12.1 EX_DRM_EXG_BACKUP (back up the file system)..... 174
3.12.2 EX_DRM_EXG_DEF_CHECK (check contents of operation definition file).... 177
3.12.3 EX_DRM_EXG_VERIFY (verify consistency of Exchange database) ..... 179

**Chapter 4 Operations (for UNIX)..... 183**

4.1 Creating the Dictionary Map File..... 184
4.2 Backing Up and Restoring a File System (Offline Tape Storage) ..... 185
4.2.1 Backing Up a File System to Tape ..... 187
4.2.2 Restoring a File System..... 189
4.3 Deleting Backup Data ..... 192

**Chapter 5 Operations (for Windows)..... 193**

5.1 Notes on Use ..... 195
5.1.1 Exchange Server ..... 195
5.2 Creating the Dictionary Map File..... 196
5.3 Deleting Backup Data ..... 197
5.4 Backing Up and Restoring a File System (Offline Tape Storage) ..... 198
5.4.1 Backing Up a File System to Tape ..... 199
5.4.2 Restoring a File System..... 202

5.5 Backing up, Restoring, and Recovering an SQL Server DB (online tape storage) .... 205
5.5.1 Backing Up an SQL Server Database ..... 206
5.5.2 Backing Up an SQL Server Transaction Log ..... 209
5.5.3 Restoring and Recovering an SQL Server Database ..... 209
5.5.4 Recovering SQL Server Transaction Logs ..... 213
5.6 Backing up, Restoring, and Recovering an SQL Server DB (from a different host) .. 214
5.7 Using the SQL Server Log-Shipping Functionality ..... 219
5.7.1 Before Using the SQL Server Log-Shipping Functionality ..... 219
5.7.2 Setting a Distribution Target Server to be an Operating Server ..... 223
5.8 Backing Up, Restoring, and Recovering Storage Groups (online backup to tape) ... 225
5.8.1 Backing Up Storage Groups (Exchange Server online backup) ..... 226
5.8.2 Restoring and Recovering Storage Groups (Exchange Server online backup) 232
5.9 Backing Up, Restoring, and Recovering Storage Groups (cold backup to tape) ..... 238
5.9.1 Backing Up Storage Groups (Exchange Server cold backup) ..... 240
5.9.2 Restoring and Recovering Storage Groups (Exchange Server cold backup) . 249

**Chapter 6 Commands ..... 257**

6.1 Overview of Commands ..... 258
6.1.1 Preventing the System from Indefinitely Executing a Command ..... 260
6.1.2 Executing Commands in a Cluster Environment ..... 260
6.2 Requirements for Executing Commands for SQL Server ..... 261
6.2.1 Relationship between Service Status and Commands ..... 261
6.2.2 Relationship between Database Status and Commands ..... 262
6.2.3 Relationship between Database Type and Commands ..... 263
6.3 Before Reading the Command Descriptions ..... 264
6.3.1 Usage Precautions ..... 264
6.3.2 Command Path ..... 264
6.3.3 Conventions in Syntax Explanations for Command Arguments ..... 264
6.3.4 Conventions for Creating a Target Definition File ..... 265
6.3.5 Coding Rules for Creating a Transaction Log Target Definition File ..... 266
6.4 Copy Controller Command Specifications ..... 267
6.4.1 drmcgctl (lock or unlock a copy group) ..... 267
6.4.2 drmclusinit (register the parameters for a cluster product) ..... 269
6.4.3 drmdbexport (export backup information to a file) ..... 270
6.4.4 drmdbimport (import backup information from a file) ..... 271
6.4.5 drmfsbackup (back up a file system to a secondary volume) ..... 272
6.4.6 drmfscat (display backup information for a file system) ..... 276
6.4.7 drmfsdisplay (display or update file system information) ..... 284
6.4.8 drmfsrestore (restore a file system from a backup to a primary volume) .. 291
6.4.9 drmlicense (display or update license information) ..... 294
6.4.10 drmmediabackup (back up data from a secondary volume to tape) ..... 295
6.4.11 drmmediarestore (restore data from tape to the secondary volume) ..... 297
6.4.12 drmmount (mount a secondary volume) ..... 299
6.4.13 drmresync (resynchronize copy groups) ..... 303
6.4.14 drmtapebackup (back up data from a secondary volume to tape) ..... 304
6.4.15 drmtapecat (display or delete backup information in a backup catalog) ... 307
6.4.16 drmtapeinit (register parameters for a backup management product) ..... 315
6.4.17 drmtaperestore (restore data from tape to a secondary volume) ..... 317
6.4.18 drmumount (unmount secondary volume) ..... 319

6.5 SQL Server Command Specifications ..... 321
6.5.1 drmsqlbackup (back up an SQL Server database to a secondary volume) ... 321
6.5.2 drmsqlcat (display backup information for a SQL Server database) ..... 323
6.5.3 drmsqldisplay (display or update information for a SQL Server database) .. 330
6.5.4 drmsqlinit (register parameters for SQL Server) ..... 336
6.5.5 drmsqllogbackup (back up the transaction log of a SQL Server) ..... 337
6.5.6 drmsqlrecover (recover restored SQL Server databases) ..... 341
6.5.7 drmsqlrecovertool (recover restored SQL Server DB through a GUI) ..... 343
6.5.8 drmsqlrestore (restore SQL Server DBs from backups to a primary vol.) .... 345
6.6 Exchange Server Command Specifications ..... 350
6.6.1 drmexgbackup (back up a storage group to a secondary volume) ..... 350
6.6.2 drmexgcat (display backup information for a storage group) ..... 353
6.6.3 drmexgdisplay (display or update information for storage groups) ..... 359
6.6.4 drmexgrestore (restore storage groups from secondary to primary vol) .... 365
6.6.5 drmexgverify (verify the integrity of backup data) ..... 369

**Chapter 7 Troubleshooting ..... 371**

7.1 General Troubleshooting ..... 371
7.2 Troubleshooting Extended Commands ..... 372
7.3 Data to be Collected When a Problem Occurs ..... 373
7.3.1 Data to be Collected (in UNIX) ..... 373
7.3.2 Data to be Collected (in Windows) ..... 377
7.4 Collecting the Required Data ..... 381
7.4.1 Collecting Data (in UNIX) ..... 381
7.4.2 Collecting Data (in Windows) ..... 382
7.4.3 Adjusting the Output Level for Processed Trace Log Information ..... 383
7.4.4 Adjusting the Number of Log Files for Internal Trace Log Information ..... 383
7.5 Investigating the Collected Data ..... 384
7.5.1 Investigating standard output logs ..... 384
7.5.2 Investigating the Trace Logs for Protection Services-Cooperative Software ..... 384
7.5.3 Investigating Internal Trace Logs ..... 385
7.6 Calling the Support Center ..... 387

**Chapter 8 Messages ..... 389**

8.1 Message Overview ..... 389
8.2 KAVX0001-I - KAVX0485-W ..... 390
8.3 KAVX1000-I - KAVX1400-I (SQL Server) ..... 406
8.4 KAVX1500-E - KAVX1901-E (Exchange Server) ..... 413
8.5 KAVX2500-E - KAVX2525-E ..... 419
8.6 Detailed Messages ..... 422
8.7 Actions Taken for the Message KAVX0070-W ..... 436

**Acronyms and Abbreviations ..... 441**

# List of Figures


Figure 1.1 Copy Group Consisting of More Than One Pair Volume ..... 5
Figure 1.2 ShadowImage and TrueCopy System Configuration (Shared P-VOL/P-VOL) ..... 13
Figure 1.3 ShadowImage and TrueCopy System Configuration (Shared S-VOL/P-VOL) ..... 14
Figure 1.4 System Configured to Back Up and Restore Data Between Volumes ..... 20
Figure 1.5 System Configured to Back Up Data to Tape ..... 21
Figure 1.6 System Configured to Restore Data on a Different Host ..... 22
Figure 1.7 System Configured to Use the SQL Server Log-Shipping Functionality ..... 23

Figure 2.1 Example Configuration: Multiple Generations of Backups ..... 28
Figure 2.2 Example Configuration: Backing Up Multiple P-VOLs ..... 29
Figure 2.3 Example Configuration: Backing Up Multiple Generations of Pair Volumes ..... 30

Figure 3.1 System Configuration for Backing Up and Restoring Data Between Volumes ... 61
Figure 3.2 System Configuration for Performing a Tape Backup and Restoration ..... 62
Figure 3.3 System Configuration: File Server in a Cluster Configuration ..... 63
Figure 3.4 System Configuration: SQL Server in a Cluster Configuration ..... 64
Figure 3.5 System Configuration: Exchange Server in a Cluster Configuration ..... 65
Figure 3.6 Locations of Operation Definition Files (UNIX) ..... 70
Figure 3.7 Locations of Operation Definition Files (Windows, File Servers) ..... 74
Figure 3.8 Locations of Operation Definition Files (Windows, SQL Server shown) ..... 75
Figure 3.9 Backing Up a File System to a Secondary Volume ..... 86
Figure 3.10 Backing Up a Database to a Secondary Volume ..... 87
Figure 3.11 Restoring a File System to a Primary Volume ..... 88
Figure 3.12 Restoring an SQL Server Database to a Primary Volume ..... 89
Figure 3.13 Backing Up a File System to Tape (Always-Split Mode) ..... 90
Figure 3.14 Backing Up a Database to Tape (Always-Split Mode) (SQL Server shown) ..... 92
Figure 3.15 Performing Online Backup of an Exchange DB to Tape (Always-Split Mode) ... 94
Figure 3.16 Backing Up a File System to Tape (Always-Paired Mode) ..... 96
Figure 3.17 Backing Up a Database to Tape (Always-Paired Mode) (SQL Server shown) ..... 98
Figure 3.18 Performing Online Backup of an Exchange DB to Tape (Always-Paired Mode) ..... 100
Figure 3.19 Restoring a File System from Tape ..... 102
Figure 3.20 Restoring a Database from Tape (SQL Server shown) ..... 103
Figure 3.21 System Configuration: Back Up and Restore a File System to Tape (UNIX) .... 105
Figure 3.22 System Configuration: Back Up and Restore a File System to Tape (Windows) ..... 110
Figure 3.23 System Configuration: Back Up and Restore an SQL Server DB to Tape ..... 115
Figure 3.24 System Configuration: Back Up and Restore an Exchange Server DB to Tape ..... 122

Figure 4.1 Flow of Operations (for UNIX) ..... 183
Figure 4.2 System Configuration: Back Up and Restore a File System to Tape ..... 185

Figure 5.1 Flow of Operations (Windows, Copy Controller only) ..... 193
Figure 5.2 Flow of Operations (SQL Server) ..... 194
Figure 5.3 Flow of Operations (Exchange Server) ..... 194
Figure 5.4 System Configuration: Tape Backup and Restoration (File System) ..... 198
Figure 5.5 System Configuration: Tape Backup and Restoration (SQL Server DB) ..... 205

Figure 5.6 System Configuration: Restoring and Recovering from a Different Host (backup) ..... 214
Figure 5.7 System Configuration: Restoring and Recovering from a Different Host (restoring) ..... 215
Figure 5.8 System Configuration: SQL Server Logship Operations ..... 219
Figure 5.9 System Configuration: Setting a Distribution Target Server as an Operating Server ..... 223
Figure 5.10 System Configuration: Online Tape Backup and Restoration (Exchange) ..... 225
Figure 5.11 System Configuration: Cold Backup to Tape and Restoration (Exchange)..... 238

Figure 6.1 drmsqlrecovertool Dialog Box ..... 343

# List of Tables

Table 1.1 Required Functions on the Storage Subsystem ..... 10

Table 2.1 Environment Setup Tasks for the Servers..... 26
Table 2.2 Prerequisite Products and Environment Setup Requirements..... 27
Table 2.3 Storage Term of Media and Restorability..... 36
Table 2.4 Configuration File Parameters for Tape Backup (VERITAS NetBackup) ..... 37
Table 2.5 Configuration File Parameters for Tape Backup (VERITAS Backup Exec)..... 38
Table 2.6 Parameter in DEFAULT.dat for Instance Number..... 40
Table 2.7 Parameters in DEFAULT.dat for Retry Count and Retry Interval ..... 41
Table 2.8 Values in the RETRY_WAIT Parameter Set for Storage Subsystems ..... 41
Table 2.9 Parameters in DEFAULT.dat for Retry Count and Pair Status Check Interval... 42
Table 2.10 Parameter in DEFAULT.dat for Track Size for Copying Data ..... 43
Table 2.11 Parameters in init.conf for Checking the Status of Cluster Resources..... 44
Table 2.12 Parameters in init.conf for Checking the Status of a Process..... 45
Table 2.13 Parameters in init.conf (Backup Option) ..... 46
Table 2.14 Parameter of init.conf (Dictionary Map synchronous option) ..... 46
Table 2.15 Environment Setup Tasks for Servers (Uninstalling Protection Services)..... 51

Table 3.1 Extended Commands for Copy Controller ..... 57
Table 3.2 Extended Commands for SQL Server ..... 57
Table 3.3 Extended Commands for Exchange Server ..... 58
Table 3.4 Preparation Tasks for Servers for Extended Commands..... 66
Table 3.5 Example: Contents of Entries in an Operation Definition File (UNIX)..... 71
Table 3.6 Storage Directories for Extended Command Temporary Files (UNIX) ..... 72
Table 3.7 Operation IDs for which an Operation Definition File is Created (UNIX) ..... 72
Table 3.8 Contents of Entries in an Operation Definition File (Windows) ..... 76
Table 3.9 Cluster Resources (Copy Controller) ..... 78
Table 3.10 Storage Directories for Extended Command Temporary Files (Windows) ..... 78
Table 3.11 Operation IDs for which an Operation Definition File is Created (Windows) ... 78
Table 3.12 Cluster Resource Example (SQL Server) ..... 80
Table 3.13 Example: Storage Directories for Extended Command Temporary Files and VDI Metafiles..... 80
Table 3.14 Operation ID for which to Create an Operation Definition File (SQL Server) ... 80
Table 3.15 Cluster Resource Example (Exchange Server) ..... 82
Table 3.16 Example: Extended Command Temporary File Storage Directory and VDI Metafile Storage Directory..... 82

Table 3.17 Operation ID for which to Create an Operation Definition File (Exchange Server) ..... 82
Table 3.18 Value of Entries in a Host Environment Settings File ..... 84
Table 3.19 Items that are Output to the Log File for Extended Commands ..... 130
Table 3.20 Details Checked in the Operation Definition File ..... 142
Table 3.21 Items Checked for the Host Environment Settings File..... 152
Table 3.22 Items Checked in the Operation Definition File ..... 167
Table 3.23 Details Checked in the Operation Definition File ..... 177

Table 5.1 Correspondence of Primary and Secondary Volumes (online backup on storage groups) ..... 226
Table 5.2 Correspondence of Primary Volume and Secondary Volume (cold backup on storage groups) ..... 239

Table 6.1 List of Commands (Copy Controller) ..... 258
Table 6.2 List of Commands (SQL Server only) ..... 259
Table 6.3 List of Commands (Exchange Server only)..... 259
Table 6.4 Relationship between Service Status and Commands (SQL Server) ..... 261
Table 6.5 Relationship between Database Status and Commands (SQL Server) ..... 262
Table 6.6 Relationship between Database Status and Commands (SQL Server) ..... 263
Table 6.7 Conventions in Syntax Explanations for Arguments..... 264
Table 6.8 Commands that Support a Target Definition File ..... 265
Table 6.9 Parameters of the Cluster Product ..... 269
Table 6.10 Items Displayed by the drmfscat Command..... 278
Table 6.11 Items Displayed by the drmfsdisplay Command ..... 286
Table 6.12 Items displayed by the drmtapecat command..... 309
Table 6.13 Parameters for Backup Management Products ..... 315
Table 6.14 Items Displayed by the drmsqlcat Command ..... 323
Table 6.15 Items Displayed by the drmsqldisplay Command..... 330
Table 6.16 Parameters for the SQL Server..... 336
Table 6.17 Items Displayed by the drmexgcat Command..... 353
Table 6.18 Items Displayed by the drmexgdisplay Command ..... 359

Table 7.1 OS Log Information (UNIX) ..... 373
Table 7.2 Protection Services Information (UNIX)..... 375
Table 7.3 CCI Information (UNIX) ..... 376
Table 7.4 OS Log Information (Windows) ..... 377
Table 7.5 Protection Services Information (Windows)..... 378
Table 7.6 CCI Information (Windows) ..... 379
Table 7.7 Database Information..... 380
Table 7.8 Output Items for Internal Trace Logs ..... 385
Table 7.9 Causes of Messages Output to Internal Trace Logs..... 386

Table 8.1 Message Types ..... 389
Table 8.2 KAVX0001-I - KAVX0485-W ..... 390
Table 8.3 KAVX1000-I - KAVX1400-I..... 406
Table 8.4 KAVX1500-E - KAVX1901-E ..... 413
Table 8.5 KAVX2500-E - KAVX2525-E ..... 419
Table 8.6 Detailed Messages..... 422

# Chapter 1 Overview of HiCommand™ Protection Services

The HiCommand™ Protection Services licensed software product systematically controls storage subsystems, backup/recovery products, databases, and other system components to provide efficient and reliable data protection that eases the workload on system administrators. This chapter describes the features and functions of Protection Services. This chapter also describes the requirements for using Protection Services.

1.1 Protection Services features

1.2 Protection Services key concepts

1.3 Protection Services functions

1.5 Protection Services system requirements

1.6 Protection Services-cooperative software

1.7 Protection Services system configurations

## 1.1 Protection Services Features

The Protection Services software product eases data maintenance operations, including operations for backup and restoration. Protection Services ensures protection of important data with minimum interruption to other processing jobs. Protection Services provides simple commands that accomplish data management operations that would otherwise require complex procedures and expertise, thus reducing the workload on the system administrator and reducing the cost of data management.

An enterprise information system must now be able to safely protect important data without interrupting other processing jobs, and restart such processing jobs quickly if an error occurs. To meet these needs, the storage subsystems of the Lightning/Thunder Series provide RAID management through Command Control Interface (CCI) and volume duplication functions (through ShadowImage). These duplication functions can quickly create a replica of a logical volume within a storage subsystem, without using a host. A system administrator who manages backups can use these functions to back up a replica (secondary volume) of a primary volume to tape without disconnecting the primary volume, which can continue to be used by the current processing job.

Until now, however, in using volume duplication functions to back up a database during online operations (an online backup), one would encounter the following problems:

- Extensive expertise is required:

  To use the volume duplication functions of the Lightning/Thunder Series, the user would have to determine which logical unit, from among the RAID devices, stores the database objects to be backed up. Acquiring mapping information between the database object and the logical unit requires expertise about databases, file systems, the logical volume manager, and RAID devices.

- Operation is complex:

  To perform an online backup of a database object, the following operations would have to be performed correctly:

  - Operations on the database and file system to prevent information from being altered and to maintain database integrity.
  - Operations on RAID devices by using CCI to create replicas of the volumes to be backed up.
  - Operations on the backup management product to back up replicas to tape.

Since the sequence of the above operations differs depending on the type of database application or file system, it can be difficult to learn how to perform all the operations. Also, since many complex operations must be performed across several layers, it is also difficult to avoid human error.

Protection Services resolves these problems and enables high-speed, reliable backup operations that make maximum use of the Lightning/Thunder Series functions.

Protection Services internally manages information about the relationships between the backup target object and the associated logical unit among the RAID devices, the relationship between the primary and secondary volumes, and the backup history. This information is contained in a dictionary map file. Protection Services references the information in the dictionary map file to control the database and RAID devices automatically, thus reducing the system administrator's workload and storage system's total cost of ownership (TCO).

## 1.2 Key Concepts

This section describes concepts specific to Protection Services that you need to understand to use Protection Services.

### 1.2.1 Dictionary Map File

To automate backup processing, Protection Services uses a dictionary map to manage the relationships among database management systems (DBMSs) or file systems and RAID devices.

The dictionary map file consists of the following three files and the backup catalog:

- Application map file

  This file stores information about relationships between backup-target database objects (such as tablespaces and journal logs) and their associated files.

- Core map file

  This file stores information about relationships between mount point directories for file systems and disk numbers across RAID devices.

- Copy group map file

  This file stores information about mapping between primary volumes and their secondary volumes. Protection Services can have up to three generations of secondary volumes for each primary volume.

- Backup catalog

  The backup catalog stores the backup operation history of Protection Services and information for generation management. When a backup is performed, a new record that contains information about the backup is created in the backup catalog. When Protection Services restores data from a backup, Protection Services references information in the backup catalog.

  Information stored in the backup catalog includes:

  - Backup ID
  - Backup start date and time
  - Backup source information
  - Backup destination information

### 1.2.2 Copy Group

Protection Services handles pair volumes (pairs of primary and secondary volumes) for which synchronization is started or stopped by the volume duplication functions (ShadowImage) or CCI as a copy group. CCI can handle multiple pair volumes as a group, and this group can be synchronized or divided into each group. Figure 1.1 shows the concept of a copy group that consists of more than one pair volume.

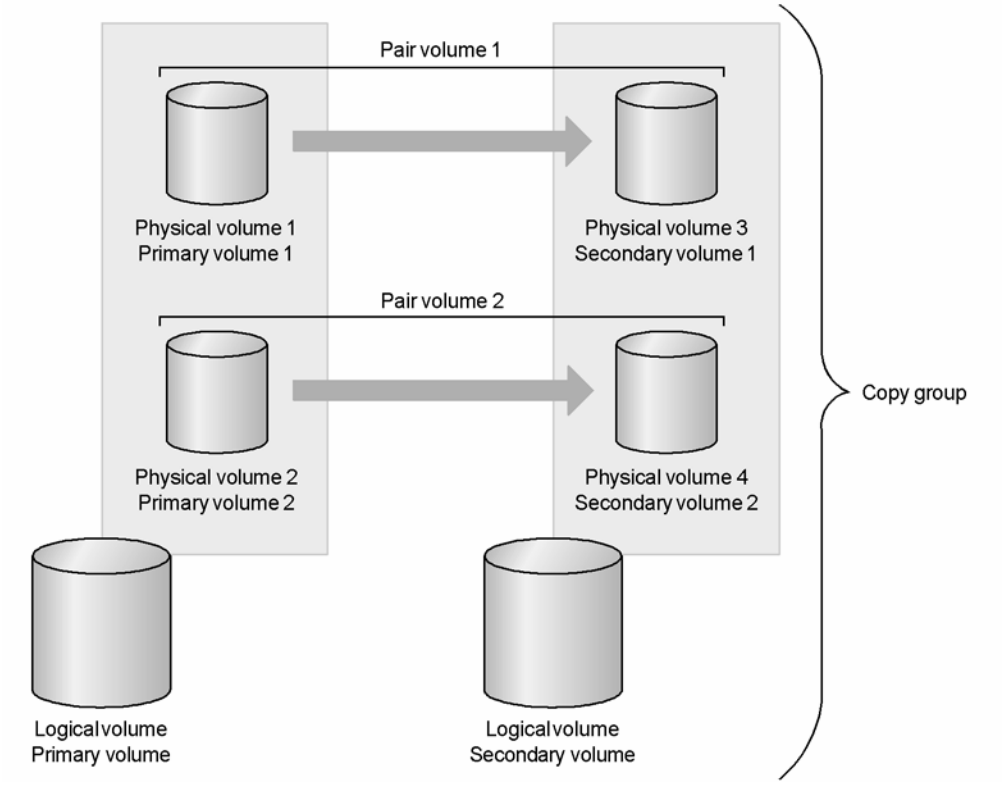



**Figure 1.1 Copy Group Consisting of More Than One Pair Volume**

If the logical volume that contains the data you want to back up consists of more than one physical volume, each of them is paired with its own secondary volume. By making more than one pair volume into a copy group, the entire logical volume that you want to back up can be synchronized or divided.

The name of a copy group consists of a dev_group (CCI group name) and a dev_name (CCI paired logical volume name). For example, when dev_group is VG01 and dev_name is dev01, the copy group name must be VG01,dev01.

***Note:*** For further information on CCI, please refer to the CCI manual for the applicable subsystem(s) (e.g., *Hitachi Lightning 9900™ V Series and Lightning 9900™ Command Control Interface (CCI) User and Reference Guide*, MK-90RD011).

## 1.3 Protection Services Functions

Protection Services has commands for carrying out the following functions:

- **Detecting resources**

  Protection Services provides a command that detects configuration information for database and file systems, as well as disk management information for RAID devices, and registers the detected information in the dictionary map file. The command can also display the information registered in the dictionary map file.

- **Backing up**

  Protection Services provides two backup commands. One backup command uses the volume duplication function of the storage subsystem to perform high-speed disk copy. The other backup command backs up data from the secondary volume to tape in collaboration with the backup management product.

- **Restoring**

  Protection Services provides a command that uses the volume duplication functions to restore a database or file system from a backup.

- **Clustering**

  Protection Services allows you to create failover-type cluster systems on several operating systems by using cluster software for these operating systems. With a file server or database server in a cluster configuration, Protection Services can continue to perform backups without interruption even if an error occurs.

- **Extended commands**

  Normal backup operations often involve executing several commands in combination to perform a complex task. For example, if you want to perform a tape backup, you execute a backup command based on disk copying and then continue by executing a command to back up data from the secondary volume to a tape. Protection Services provides scripts that automatically execute a series of commands. These scripts are called extended commands. Extended commands make it easier for you to perform backup tasks that use Protection Services commands.

## 1.4 Protection Services Components

The HiCommand Protection Services product includes the following software components:

- **Protection Services Copy Controller** (required, described in this document)
- **Protection Services for SQL Server** (optional, described in this document)
- **Protection Services for Exchange Server** (optional, described in this document)
- **Protection Services for Oracle** (optional, ***not*** described in this document)

  ***Note:*** Please refer to the *HiCommand Protection Services for Oracle User's Guide*, 3020-3-D54-30(E) for information on installing and using Protection Services for Oracle.

## 1.5 Protection Services System Requirements

This section describes the programs required to configure a system that uses Protection Services and describes related programs.

### 1.5.1 Host Requirements

**OS.** Protection Services programs can run on the following operating systems:

- Sun Solaris versions 7, 8, and 9
- HP-UX versions 11.0 and 11i (HP-UX 11.11). The following software patch module provided by HP is required:
  - For v11.0: PHKL_20973 (fix 64 bit VX_FREEZE ioctl returning EINVAL), or later
  - For v11i: PHCO_27913 (s700-800 11.11 LVM commands cumulative patch) or later
- Microsoft Windows (SQL Server and Exchange Server):
  - Windows 2000 Server Service Pack 2 OR Service Pack 3 OR Service Pack 4
  - Windows 2000 Advanced Server Service Pack 2 OR Service Pack 3 OR Service Pack 4
  - Windows Server 2003, Standard Edition
  - Windows Server 2003, Enterprise Edition

**Server hardware.**

- For Windows: PC/AT compatible machines
- For Solaris: SUN SPARCstation or SUN SPARCserver
- For HP-UX: For details on the applicable hardware modules, see the Release Notes for the prerequisite HP-UX version.

**File systems.** Protection Services supports the following file systems:

- For Solaris: VERITAS VxFS 3.4 or later, or Standard HFS
- For Windows: NTFS

  ***Note:*** Only basic disk is supported. Dynamic disk is not supported.

  ***Note:*** The disk on the target system should be mounted as drive character. This version does not support the system configuration that mounts the disk to the directory.

**Required applications.** In the host for which you want to install Protection Services, the following applications must be installed and set up:

- CCI (Command Control Interface)
  - For 9900V and 9900: version 01-09-03/02 or later
  - For 9500V and 9200: version 01-10-03/02 or later

  For information on CCI installation and configuration, please refer to the CCI manual for the applicable subsystem(s) (e.g., *Hitachi Lightning 9900™ V Series and Lightning 9900™ Command Control Interface (CCI) User and Reference Guide*, MK-90RD011).
- Logical volume manager:
  - In Solaris: VERITAS Volume Manager (VxVM) version 3.1.1, 3.2p2, or 3.5
  - In HP-UX: LVM (Logical Volume Manager) of the operating system
  - In Windows: logical disk manager of the operating system
- Protection Services for Exchange Server uses CDOEXM (Collaboration Data Object For Exchange Management). Microsoft Exchange system management tool must be installed to install the files necessary for executing commands.

**Database management systems.** Protection Services supports the following DBMSs:

- For SQL Server and Exchange Server:
  - Microsoft (R) SQL Server 2000 Standard Edition, Service Pack 2 or later
    Microsoft (R) SQL Server 2000 Enterprise Edition, Service Pack 2 or later

    ***Note:*** The distributed database environment and distribution database are not supported.

    ***Note:*** Service Pack 2 or later is required for Exchange Server.

    ***Note:*** Service Pack 2 or later is required for SQL Server when configuring multiple databases in one instance. Otherwise, Service Pack 2 or later is recommended.

**Backup management software.** When backing up the data on a secondary volume to tape:

- For Windows 2000 Server or Windows 2000 Advanced Server:
  - VERITAS NetBackup 3.4 or 4.5
  - VERITAS Backup Exec 8.6 or 9.0
- For Windows Server 2003, Standard Edition or Windows Server 2003, Enterprise Edition:
  - VERITAS Backup Exec 9.0
- For Solaris and HP-UX:
  - VERITAS NetBackup 3.4 or 4.5

**Cluster software.** Protection Services supports the following cluster software:

- For Windows: Microsoft(R) Cluster Service
- For Solaris: VERITAS Cluster Server version 2.0 or 3.5
- For HP-UX: MC/ServiceGuard version 11.13 or 11.14

### 1.5.2 Storage Subsystem Requirements

Protection Services supports the following storage subsystems:

- Lightning 9900 V Series
- Lightning 9900 Series
- Thunder 9500V Series
- Thunder 9200 Series

Table 1.1 shows the volume replication functionality required to use Protection Services with the above storage subsystems.

**Table 1.1 Required Functions on the Storage Subsystem**

| Storage Subsystem | Required Functions |
|---|---|
| Lightning 9900 V Series<br>Lightning 9900 Series | ShadowImage<br>CCI |
| Thunder 9500 V Series | ShadowImage or QuickShadow<br>CCI |
| Thunder 9200 | ShadowImage<br>CCI |

***Note:*** For information on ShadowImage operations, please refer to the ShadowImage manual for the applicable subsystem(s) (e.g., *Hitachi Lightning 9900™ V Series ShadowImage User's Guide*, MK-92RD110).

***Note:*** For information on 9500V QuickShadow operations, please refer to the *Hitachi Thunder 9500™ V Series QuickShadow User's Guide* (MK-93DF666).

***Note:*** For information on CCI operations, please refer to the CCI manual for the applicable subsystem(s) (e.g., *Hitachi Lightning 9900™ V Series and Lightning 9900™ Command Control Interface (CCI) User and Reference Guide*, MK-90RD011).

### 1.5.3 Notes on Volume Configuration

Protection Services backs up or restores data by mirroring physical volumes in the storage subsystem. Therefore, note the following points about the configuration of logical volumes:

- In Windows, the volume containing the database to be backed up should be left as a basic disk. Do not upgrade the volume to a dynamic disk.
- When you use the logical volume manager to configure logical volumes, you can use Protection Services only when making physical volumes into a single logical volume. You cannot use Protection Services when dividing a physical volume into logical volumes. When a logical volume contains more than one physical volume, a snapshot operation is performed for each physical volume.
- Do not use any functions that let you freely expand or reduce the capacity of a logical volume. If you use such functions, Protection Services will not perform backup and restoration correctly. This is because the number of physical volumes that make up the logical volume changes according to the change in capacity of the logical volume. Protection Services checks whether the configuration of logical volumes has been changed and, if changed, restoration terminates abnormally.
- If the volumes to be processed by Protection Services contain any LDEV, for which other than the normal mode is specified for the access level by using Open LDEV Guard, neither a backup nor a restoration is performed.
- Protection Services will un-mount and mount the mount point of target volume in backing up or restoring file system and database objects. Note the following requirements for constructing the mount point of volume:
  - In Windows:

    Maximum characters: 128 characters

    Usable characters: All characters that can be used for a folder name in Windows, except space, multibyte character, and single-byte kana.
  - In UNIX:

    Maximum characters: 255 characters

    Usable characters: All characters that can be used for a directory name in each UNIX platform.

Protection Services uses the pair volumes defined by CCI to back up or restore a file system or database object. When you create a pair volume by using CCI, abide by the following rules:

- A copy group must consist of pair volumes for the same application. When a copy group consists of more than one pair volume and there are pair volumes for different applications in the copy group, an unexpected backup or restoration may be performed.
- Both of the volumes that make up a pair volume must be contained in the same physical device. Protection Services does not allow you to configure a pair volume in more than one physical device.
- When the primary volume and the secondary volume are in the pair status, do not restart the server. If a mount operation is performed while the server is restarting, the primary volume and secondary volume might not be mounted correctly and a data inconsistency might occur.
- If there are multiple generations of backups (secondary volume), all the volumes might be mounted when the backup server restarts. Before executing the Protection Services command, unmount the volumes that are not to be used for backup or restoration by using the disk management functionality of the operating system.
- Protection Services operates pair volumes for ShadowImage and QuickShadow only.
- When you want to mix the pair volumes for ShadowImage and TrueCopy, the system configurations shown in Figure 1.2 and can be used. In the configuration shown in Figure 1.2, when you restore the pair volume for ShadowImage by using Protection Services, the status of the pair volume for TrueCopy must be set to SMPL or PSUS (SSUS). In the configuration shown in, when you back up or restore the pair volume for ShadowImage by using Protection Services, the status of the pair volume for TrueCopy must be set to SMPL or PSUS (SSUS).

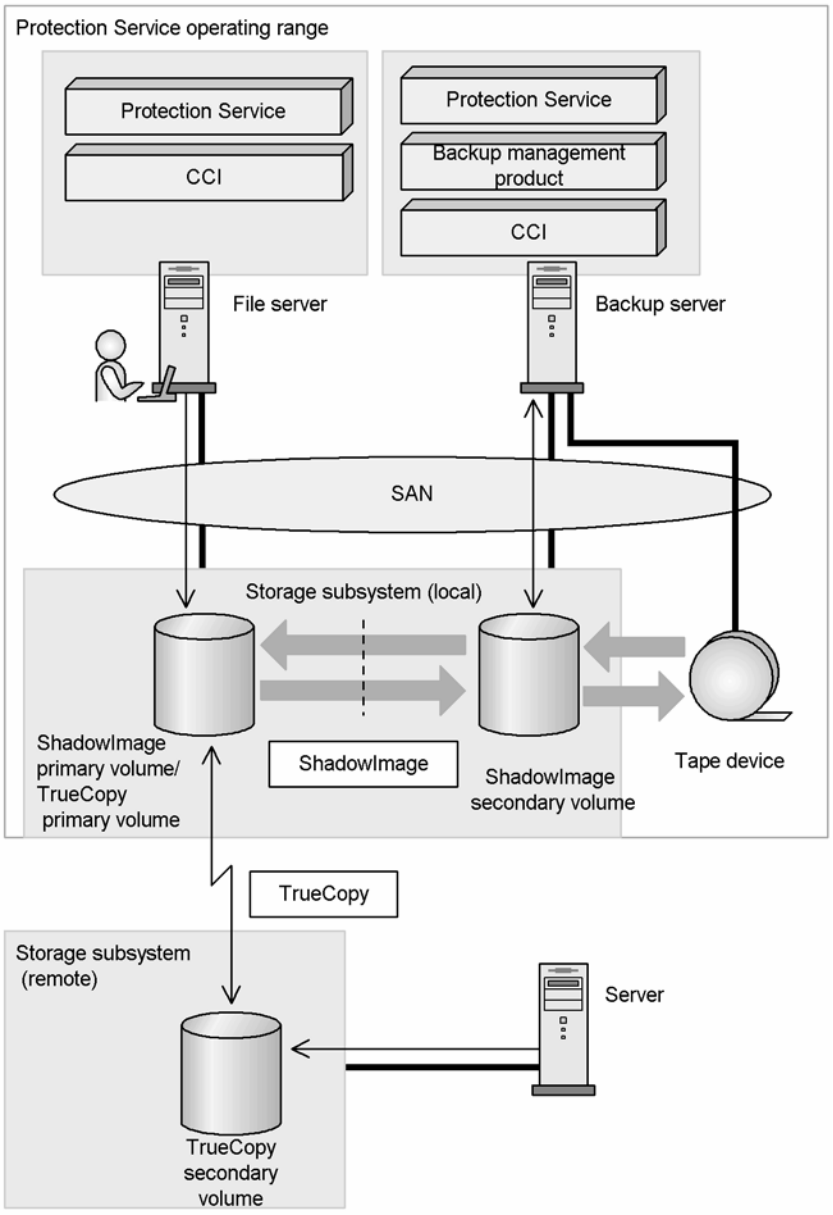



**Figure 1.2 ShadowImage and TrueCopy System Configuration (Shared P-VOL/P-VOL)**

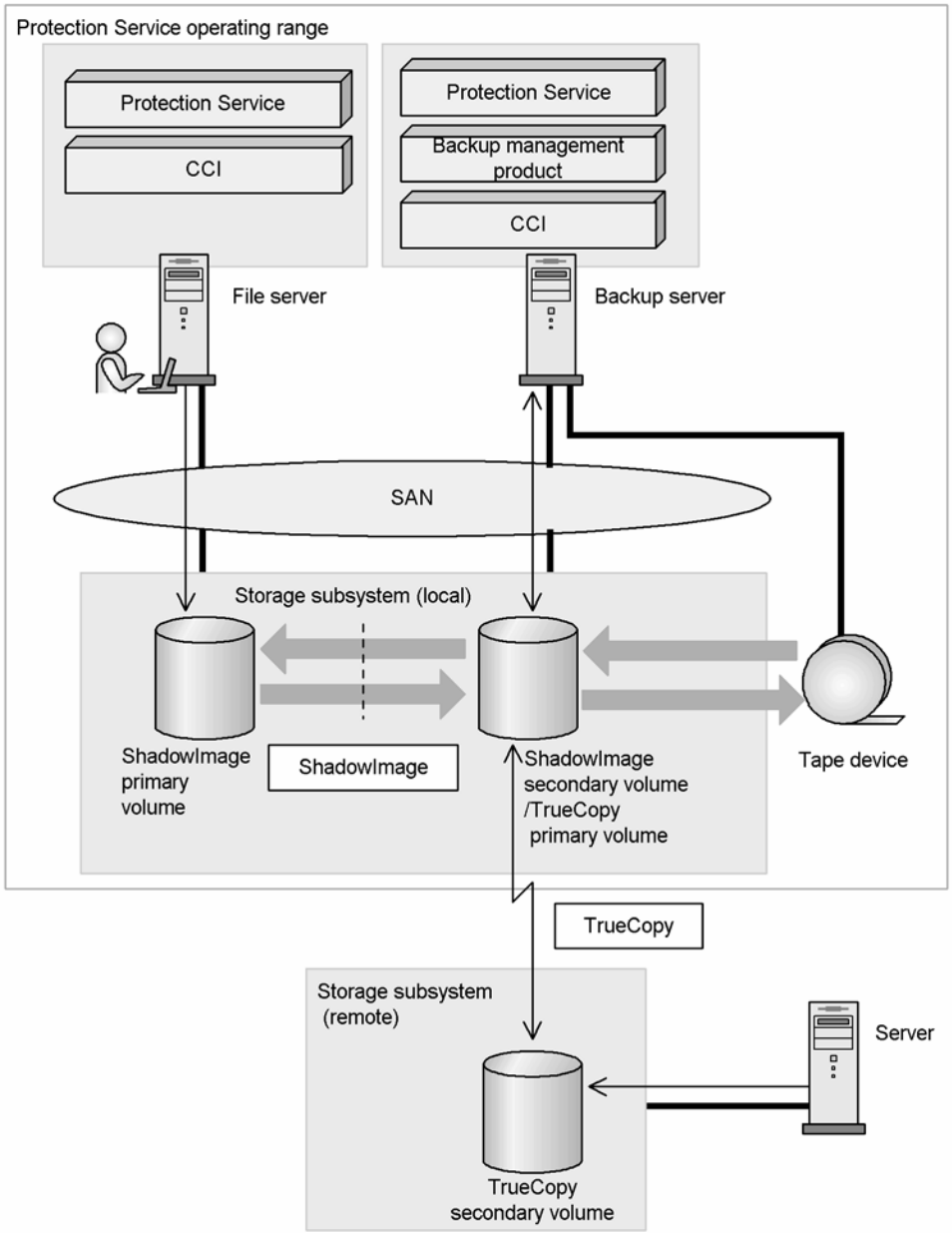



**Figure 1.3 ShadowImage and TrueCopy System Configuration (Shared S-VOL/P-VOL)**

***Note:*** For information on TrueCopy operations, please refer to the TrueCopy manual for the applicable subsystem(s) (e.g., *Hitachi Lightning 9900™ V Series TrueCopy User and Reference Guide*, MK-92RD108).

### 1.5.4 Notes on Using an Exchange Server Database

Protection Services for Exchange Server supports the following Exchange database products:

- Exchange 2000 Enterprise Server
- Exchange 2000 Server
- Exchange Server 2003 Enterprise Edition
- Exchange Server 2003 Standard Edition

Protection Services for Exchange Server is backed up and restored in units of physical volumes, so the configuration of objects of an Exchange database has the following conditions:

- The cold backup mode can back up the information store data files (***.edb** and ***.stm**), checkpoint file (***.chk**), and transaction log file (***.log**). The online backup mode can only back up the information store data files (***.edb** and ***.stm**). The files to be backed up must all be placed on a RAID volume defined as a pair.
  - When taking a backup with cold backup mode, you can place a check point file (***.chk**) in a physical volume where there are database files (***.edb** or ***.stm**) and transaction log files (***.log**). You can also place a check point file (***.chk**) in an another physical volume.
  - When taking a backup with online backup mode, you cannot place a check point file (***.chk**) in a physical volume where there are database files (***.edb** or ***.stm**). If you place these files in the same physical volume, you cannot take a backup with online backup mode. You can place a check point file (***.chk**) in a physical volume containing transaction log files (***.log**).
- Place a storage group in a physical volume upon considering that it is going to be backed up in a unit of physical volume. When more than one storage groups are placed in one physical volume, the storage groups cannot be backed up individually.
- Place the transaction log files and information-store data files in separate physical volumes. Data cannot be backed up if they are placed in the same physical volume.
- When there are information-store data files of different storage groups, place the data files in different physical volumes. The data files can be placed in the same physical volume but, in such a case, each desired data file must be specified at backup.
- Do not use the following characters when setting a name for a storage group:
  **= ; \ /**
- Files to consist of storage groups to be backed up or restored must be placed in a mount point directory which adheres to the following requirements:

  Maximum characters: 128 characters

  Usable characters: All characters that can be used for a folder name in Windows, except space, multibyte character, and single-byte kana.

- The following operations change the information pertaining to the Exchange Server on the Active Directory. Therefore, if you perform any of the following operations, you will no longer be able to restore (**drmexgrestore**) backup data acquired before these operations.
  - Modification of the paths of the information store, log, system files.
  - Addition or deletion of storage groups.
  - Modification of the storage group name.
  - Addition of an information store to a storage group.
  - Deletion of an information store from a storage group.

  If you have performed any of the above operations, you will need to back up the Active Directory and the Exchange database again. To perform a backup for the Active Directory, follow the instructions given in documentation provided by Microsoft.
- Do not use the circulation log when recovering a database by roll-forward.
- The following operations change the database name. Therefore, if you perform any of the following operations, you will no longer be able to restore and recover (**drmexgrestore -recovery**) backup data acquired before these operations.
  - Repairing information store using the **ESEUTIL** utility (**ESEUTIL /p**).
  - Defragmentation using the **ESEUTIL** utility (**ESEUTIL /d**).

  If you have performed any of the above operations, you will need to execute the drmexgbackup command, and back up the Exchange database again.
- When a restore by disk resynchronization and recovery (**drmexgrestore -resync -recovery**) is performed in a cluster environment, the KAVX1710-E message will be output, and the command may terminate abnormally. This message is output when a system attendant or information store on an Exchange cluster resource depends on a physical volume disk resource stored in a storage group or information store to be backed up. In this case, after changing the cluster settings so that the system attendant or information store no longer depends on the physical disk resource, execute the command again. For more information on changing the cluster resource settings, see the Windows manual.
- The restoration storage group for Exchange Server 2003 cannot be backed up. The files and folders that make up the restoration storage group must be placed on a different file system from the storage groups to be backed up.
- Protection Services for Exchange Server does not support VSS (Volume Shadow Copy Service).

### 1.5.5 Notes on Using an SQL Server Database

Protection Services for SQL Server supports the following SQL Server database products:

- SQL Server 2000 Enterprise Edition
- SQL Server 2000 Standard Edition

Protection Services for SQL Server is backed up and restored in units of physical volumes, so the object configuration of a SQL Server database requires the following:

- Configure the data files that comprise one instance on one disk drive. Do not place data files that comprise multiple instances on one disk drive.
- Store the following directory and file on a physical volume that does not contain data files (***.mdf** and ***.ndf**).
  - Storage directory for metadata
  - Backup data of the transaction log

Roll-forward recovery processing can be performed if the above directory and file are placed on separate volumes. This is because, even if a restoration is performed, the metadata and transaction log file cannot return to the status they were in when the backup was performed.

Backup processing for Protection Services checks whether these requirements are satisfied. If they are not satisfied, backup processing will terminate abnormally.

- Do not use the following characters when naming a database: **\ / : , ; * ? < > |**
- The databases to be backed up in Protection Services are the **master** database, the **model** database, and the **msdb** database. The **distribution** database is not backed up.
- In a configuration that contains multiple databases for one instance, the other databases also stop when you back up one database. Therefore, back up a database when the database load is low.

## 1.6 Protection Services-Cooperative Software

With Protection Services, you can further enhance system functionality by linking with backup management and cluster software, and automating tape backups. This section describes the software products that can be linked to Protection Services.

- **Backup management software**

  Using Protection Services, you can control backup management software automatically, and back up data replicated on secondary volumes within a storage system to a tape device. The following backup management products can be used with Protection Services:

  - VERITAS NetBackup
  - VERITAS Backup Exec

- **Cluster software**

  Protection Services comes with functionality that allows you to automatically control clusters, so that you can take advantage of high-availability systems based on cluster configurations. Since you need to take a database offline to perform a cold backup or restoration, when the database is taken offline while the cluster resources that monitor the DBMS are still online, a failover will probably occur. This usually results in the need to control cluster resources manually. However, when data is backed up in the cold backup mode or restored with Protection Services, cluster resources that monitor the DBMS are automatically taken offline, and then put back online once the processing finishes. The following cluster software products can be used with Protection Services.

  - For Solaris: VERITAS Cluster Server
  - For HP-UX: MC/ServiceGuard
  - For Windows: Microsoft Cluster Service

## 1.7 Protection Services System Configurations

This section describes the primary configuration patterns used for systems based on Protection Services. The following shows the major system configurations:

- System configuration when backing up and restoring data between volumes
- System configuration when storing backed up data to tape, and restoring the data from tape
- System configuration when restoring data on a host that differs from the one used for backup
- System configuration when using an SQL Server log-shipping functionality

### 1.7.1 Configuration for Backing Up and Restoring Data Between Volumes

The smallest possible configuration for a system using Protection Services is one that consists of a primary volume and a secondary volume, where data is backed up and restored between the two. This can be accomplished with only one server. Protection Services is added to the file/database server, and the backup and restoration commands are executed from the server

Figure 1.4 shows an example of a system configured to back up and restore data between volumes.

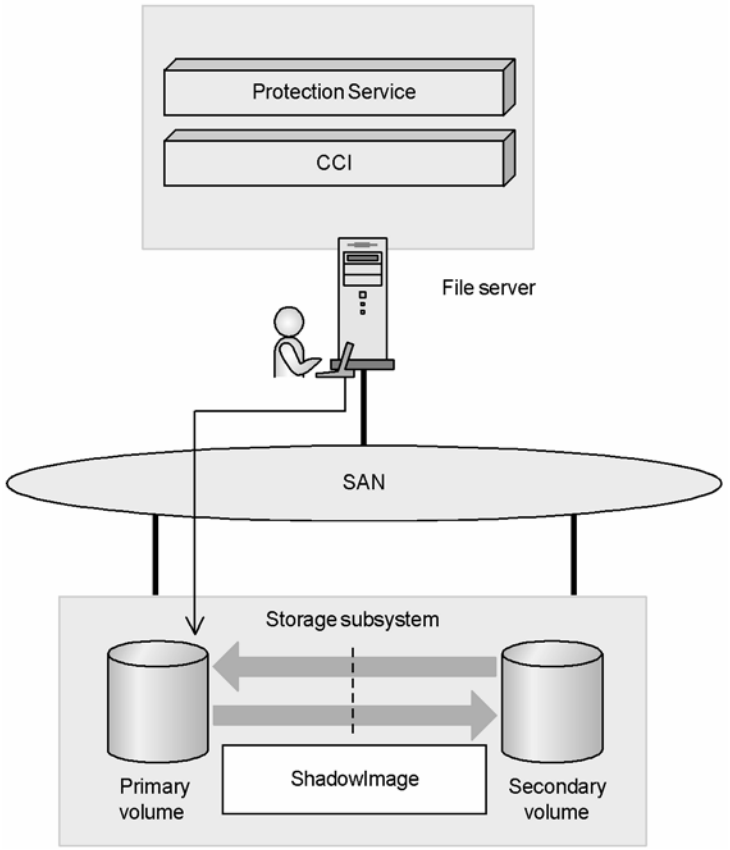



**Figure 1.4 System Configured to Back Up and Restore Data Between Volumes**

### 1.7.2 Configuration for Backing Up and Restoring Data to/from Tape

The configuration needed to store on tape data backed up using Protection Services consists of both a file server that manages the primary volume, and a backup server connected to the tape device. Protection Services needs to be installed on both the file server and backup server; commands for the primary volume are executed from the file server, and commands for the secondary volume are executed from the backup server.

Figure 1.5 shows an example of a system configured to store backed-up data to tape.

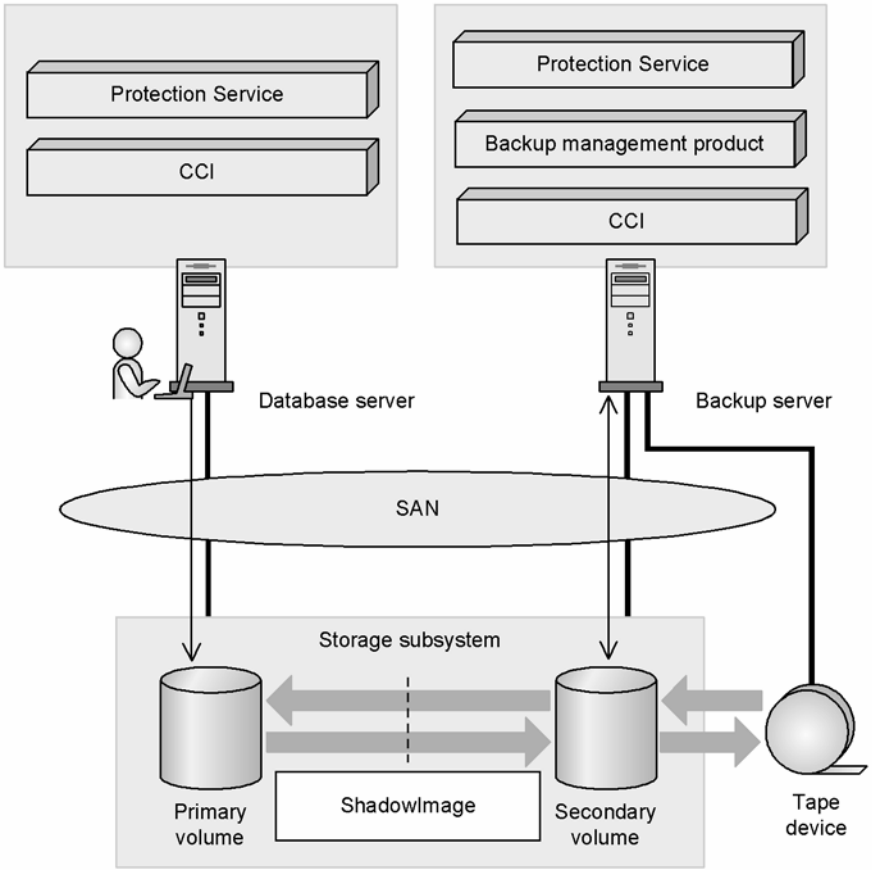



**Figure 1.5 System Configured to Back Up Data to Tape**

### 1.7.3 Configuration for Restoring Data on a Different Host (SQL Server only)

For using Protection Services to restore data on a host that differs from the one used for backup, the required configuration consists of two database servers: database server 1 for backup, and database server 2 for restoration. Protection Services needs to be installed on both database servers. Backup commands are executed on database server 1, and restoration commands are executed on database server 2.

Figure 1.6 shows an example of a system configured to restore data on a host that differs from the one used for backup.

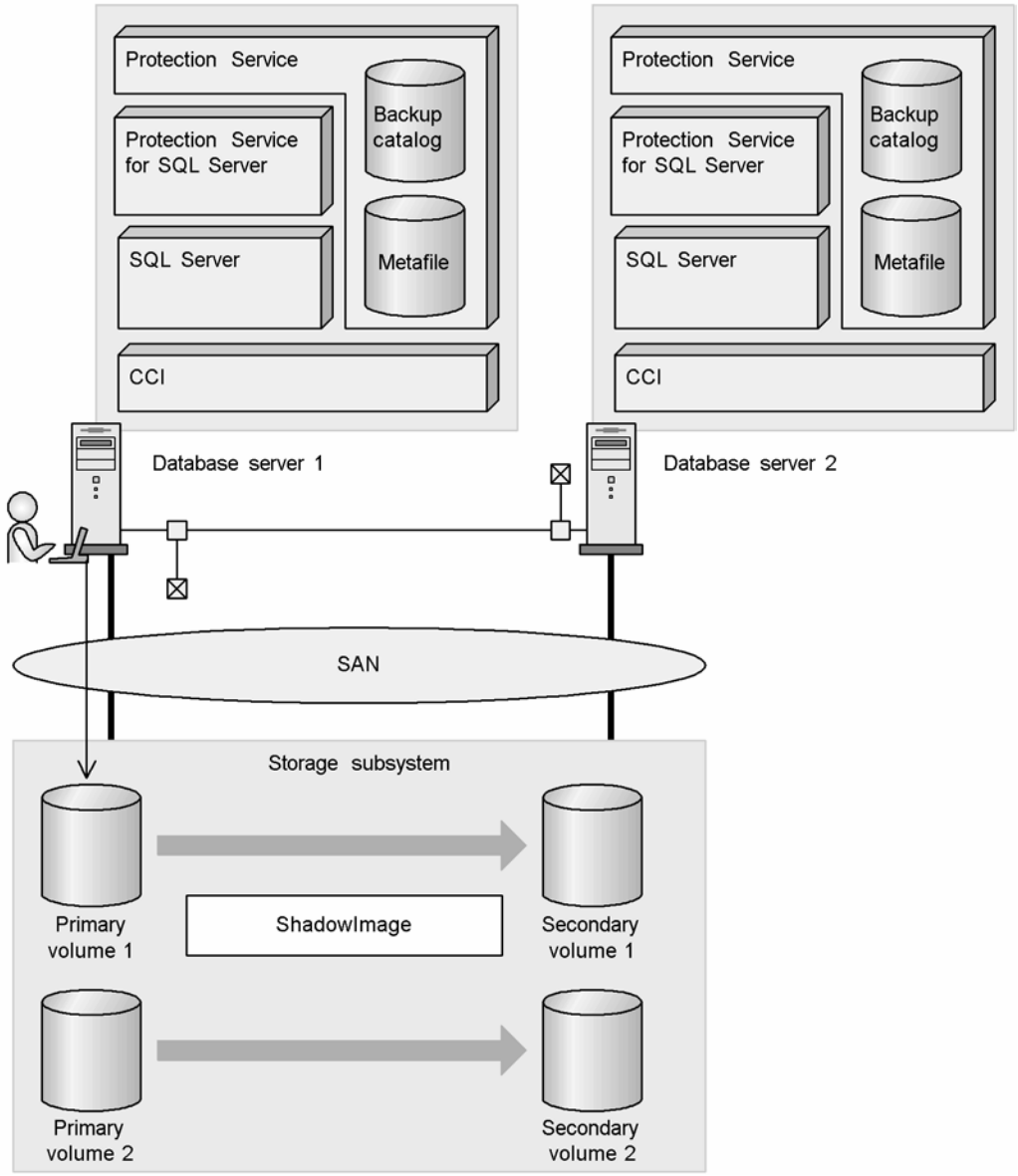



**Figure 1.6 System Configured to Restore Data on a Different Host**

### 1.7.4 Configuration for Using the SQL Server Log-Shipping Functionality

For using the SQL Server log-shipping functionality with Protection Services, the required configuration consists of a source server that distributes log files and a destination server to which the log files are distributed. Protection Services needs to be installed on both the source server and the destination server.

Figure 1.7 shows an example of a system configured to use the SQL Server log-shipping functionality.

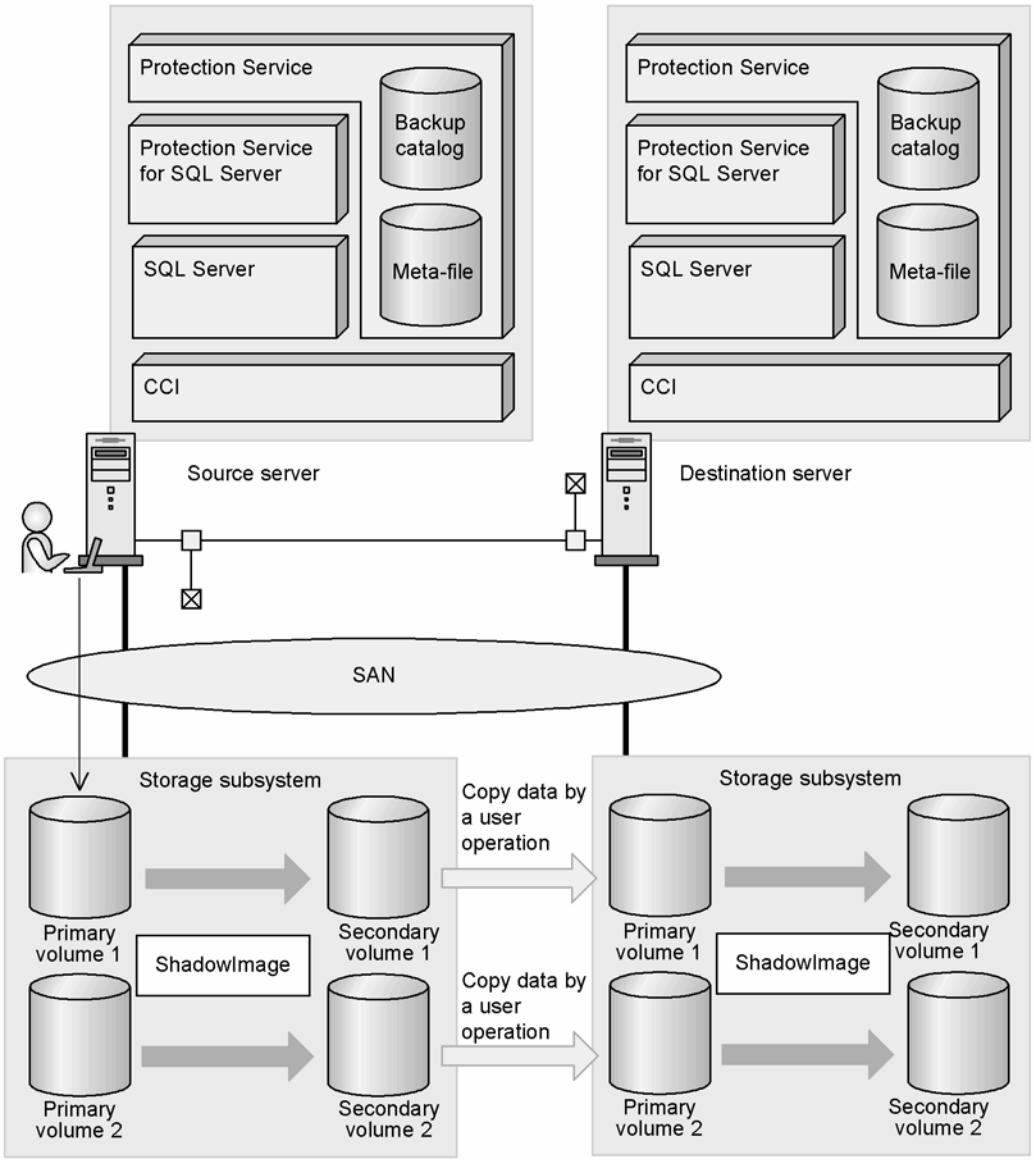



**Figure 1.7 System Configured to Use the SQL Server Log-Shipping Functionality**

# Chapter 2 Creating an Environment for Protection Services

This chapter gives an overview of environment setup and describes setup procedures for Protection Services.

2.1 Overview of environment setup

2.2 Setting up the environment for prerequisite products

2.3 Installing Protection Services

2.4 Setting environment variables (in UNIX)

2.5 Setting up linkage with a backup management product

2.6 Setting up linkage with CCI

2.7 Setting up operation of Protection Services

2.8 Setting up a cluster environment

2.9 Creating the dictionary map file

2.10 Backing up the operating environment of Protection Services

2.11 Uninstalling Protection Services

## 2.1 Overview of Environment Setup

To install Protection Services, you set up the environment in the following steps:

1. Set up the environment for products that are prerequisites for Protection Services.
2. Install Protection Services.
3. Set up the environment for Protection Services.
4. Set up the environment for the cluster system.
5. Check the environment setup.
6. Specify settings to avoid problems.

The environment setup tasks on the file/database server differ from those on the backup server. Table 2.1 shows the tasks needed for each kind of server.

**Table 2.1 Environment Setup Tasks for the Servers**

| Task | | File/Database Server | Backup Server |
|---|---|---|---|
| Set up the environment for prerequisite products | ShadowImage | Not needed * | Not needed * |
| | CCI | Needed | Needed |
| | Volume Manager (in UNIX only) | Needed | Needed |
| | Backup management product | Not needed | Needed |
| Install Protection Services | Protection Services – Copy Controller | Needed | Needed |
| | Protection Services for SQL Server<br>Protection Services for Exchange Server<br>Protection Services for Oracle | Needed | Not needed |
| Set up the environment for Protection Services | Set environment variables | Needed | Needed |
| | Set up the environment for the backup management product | Not needed | Needed |
| | Customize the RAID configuration definition file | Needed | Needed |
| | Customize the common parameter definition file | Needed | Needed |
| Set up a cluster configuration | Customize the common parameter definition file | Needed | Needed |
| | Create the Protection Services database | Needed | Needed |
| Check the environment setup | Create the dictionary map file | Needed | Needed |
| Specify settings to avoid problems | Protect the operating environment of Protection Services | Needed | Needed |

* ***Note:*** Environment setup for ShadowImage is not needed because it is performed on the storage subsystem side.

## 2.2 Setting up the Environment for Prerequisite Products

Table 2.2 shows the products that are prerequisites for Protection Services and whether environment setup is needed for the product.

**Table 2.2 Prerequisite Products and Environment Setup Requirements**

| Prerequisite Product | File/Database Server | Backup Server |
|---|---|---|
| ShadowImage | Not needed * | Not needed * |
| CCI | Needed | Needed |
| Volume Manager | Needed | Needed |
| Backup management product | Not needed | Needed |

* ***Note:*** Environment setup for ShadowImage is not needed because it is performed on the storage subsystem side.

This section covers the setup for Protection Services only. For details about installation and environment setup of another product, see the documentation for the product.

### 2.2.1 Setting Up CCI

To back up data by using Protection Services, you need to create a CCI configuration definition file (**horcm*n*.conf**) for each instance, to match the intended usage. (In **horcm*n*.conf**, ***n*** is the instance number.)

In Protection Services, a pair of a primary volume and secondary volume is managed as a copy group. A copy group is defined by a combination of **dev_group** and **dev_name** specified in a CCI configuration definition file.

Protection Services does not allow duplication of copy group names on the same server. If more than one CCI instance is activated, make sure that the combination of **dev_group** and **dev_name** is unique among all the CCI configuration definition files.

This section describes how to create configuration definition files for the following operations:

- To hold multiple generations of backups
- To back up more than one primary volume at one time
- To back up multiple generations of pair volumes at one time

***Note:*** For further information on creating a CCI configuration definition file, please refer to the CCI manual for the applicable subsystem(s) (e.g., *Hitachi Lightning 9900™ V Series and Lightning 9900™ Command Control Interface (CCI) User and Reference Guide*, MK-90RD011).

***(1) To hold multiple generations of backups*** (see Figure 2.1)

To hold multiple generations of a secondary volume (containing backup data):

(a) Define a pair volume that is made up of one primary volume and multiple generations of a secondary volume.

(b) Specify an **MU#** (pair identifier) for each pair.

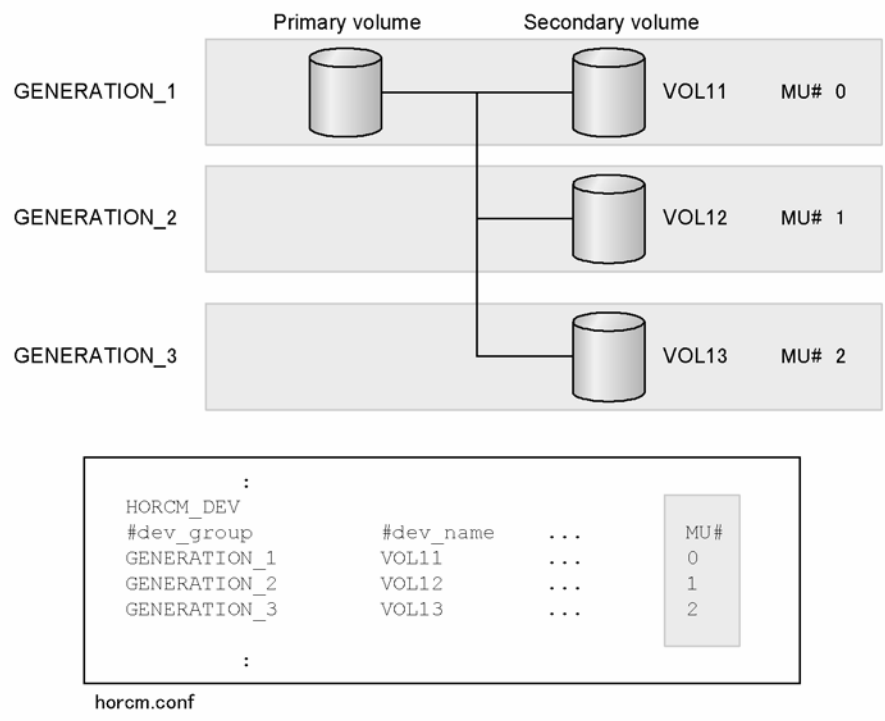



**Figure 2.1 Example Configuration: Multiple Generations of Backups**

***(2) To back up more than one primary volume at one time*** (see Figure 2.2)

To back up more than one primary volume at one time, specify the same **dev_group** name for all the paired volumes you want to back up.

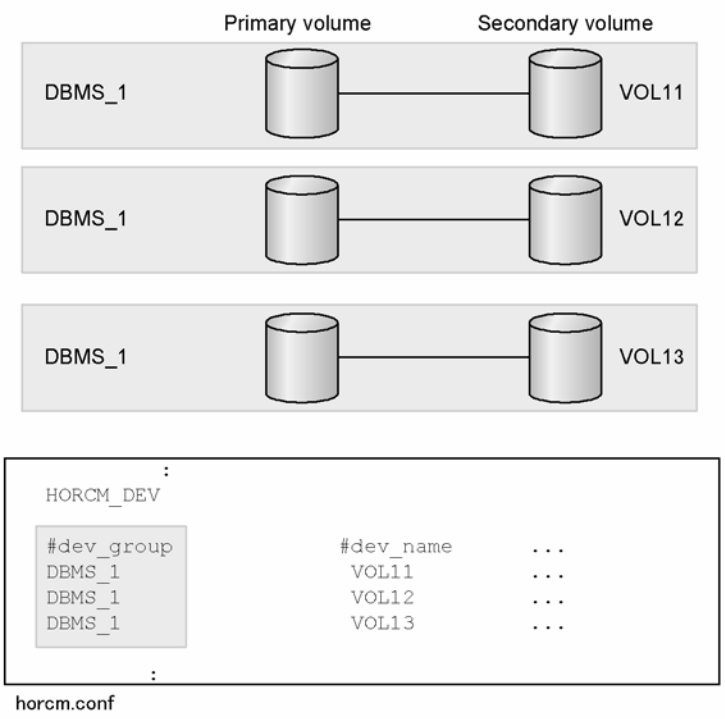
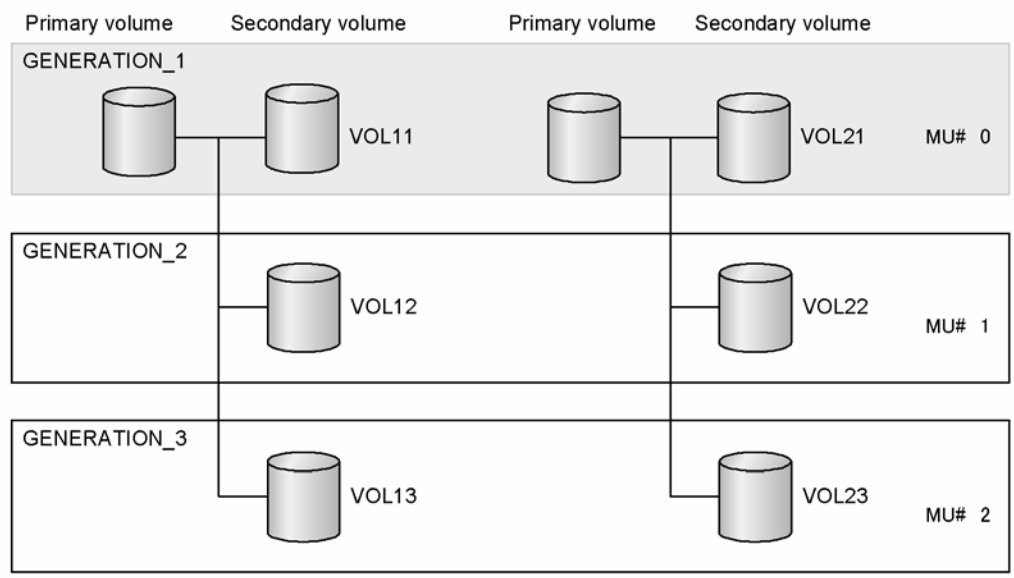



**Figure 2.2 Example Configuration: Backing Up Multiple P-VOLs**

***(3) To back up multiple generations of pair volumes at one time*** (see Figure 2.3)

To perform a backup with (1) and (2) above combined, specify the same **dev_group** name for the pair volume that has the same **MU#**.




```
          :
HORCM_DEV
#dev_group          #dev_name     ...        MU#
GENERATION_1        VOL11         ...        0
GENERATION_2        VOL12         ...        1
GENERATION_3        VOL13         ...        2
GENERATION_1        VOL21         ...        0
GENERATION_2        VOL22         ...        1
GENERATION_3        VOL23         ...        2
          :
```

**Figure 2.3 Example Configuration: Backing Up Multiple Generations of Pair Volumes**

To check whether the CCI configuration definition files you created by using the above procedures are valid, test whether the CCI instances can be activated. For details on how to activate CCI, see the CCI documentation. After you make sure that the CCI instances can be activated correctly, install Protection Services.

## 2.3 Installing Protection Services

After you finish environment setup for the products that are prerequisites for Protection Services, install Protection Services. This section describes the procedures for installing Protection Services.

Before you start installation, make sure that:

- You are logged in as a root user (administrator privileges).
- All programs are inactive (ended).

Install the Protection Services programs in the following order:

1. Protection Services - Copy Controller
2. Protection Services for SQL Server, Exchange Server, and/or Oracle

***Note:*** If an unexpected error such as insufficient disk space occurs, uninstall and then reinstall the HiCommand Protection Services software.

### 2.3.1 Installing Protection Services in the Solaris Environment

If you want to install Protection Services - Copy Controller by updating its version, in the **/var/sadm/install/admin/default** configuration definition file provided by the **pkgadd** program, change the **instance=unique** to **instance=nocheck**.

To install Protection Services - Copy Controller in the Solaris environment:

1. Insert the installation CD-ROM of Protection Services - Copy Controller into a CD-ROM drive. The CD-ROM is automatically mounted to **/cdrom/*volume-label***.
2. Use the **pkgadd** command to install Protection Services - Copy Controller. Enter the command as follows: **PROMPT> pkgadd -d /cdrom/*volume-label* HPTM**
3. When the **Input license key** message appears, enter the license key. The **Input license key** message does not appear when you overwrite Protection Services on the machine where Protection Services 1.4 has been installed.
4. When the installation confirmation message appears, enter **y**.

   After the **pkgadd** command finishes the installation, the command line prompt appears.

Protection Services - Copy Controller is stored in the following directories. You cannot change these directories.

- **/opt/drm**
- **/var/opt/drm**

When you want to display or update the registered license information, execute the **drmlicense** command.

### 2.3.2 Installing Protection Services in the HP-UX Environment

#### (1) Installing Protection Services - Copy Controller

To install Protection Services - Copy Controller in the HP-UX environment:

1. Insert the installation CD-ROM of Protection Services - Copy Controller into a CD-ROM drive, and mount the drive to any directory. For example, to mount it to **/sd_cdrom**, enter the following command:

   **PROMPT> pfs_mount *CD-ROM-device-special-file-name*/sd_cdrom**

2. Use the **swinstall** command to install Protection Services - Copy Controller. If you are installing Protection Services - Copy Controller for the first time, enter the command as follows: **PROMPT> swinstall -x ask=true -s /sd_cdrom HPTM**

   When you upgrade Protection Services, enter the following command:
   **PROMPT> swinstall -x ask=true -x reinstall=true -s /sd_cdrom HPTM**

3. When the **Input license key** message appears, enter the license key. The **Input license key** message does not appear when you overwrite Protection Services on the machine where Protection Services 1.4 has been installed.

   After the **swinstall** command finishes the installation, the command line prompt appears.

Protection Services is stored in the following directories. You cannot change these directories.

- **/opt/drm**
- **/var/opt/drm**

When you want to display or update the registered license information, execute the **drmlicense** command.

### 2.3.3 Installing Protection Services for SQL Server or Exchange Server

Perform the following tasks to install Protection Services for SQL Server or Exchange Server:

1. Install Protection Services - Copy Controller
2. Install Protection Services for SQL Server or Exchange Server
3. Set up the database (SQL Server only)

**(1) Installing Protection Services - Copy Controller**

To install Protection Services - Copy Controller in the Windows environment:

1. Insert the installation CD-ROM of Protection Services - Copy Controller into the CD-ROM drive. This example assumes that the **x:** drive is the CD-ROM drive.
2. Run the **setup.exe** file on the CD-ROM (select **Start**, select **Run**, enter **x:\setup.exe**, and select **OK**). The **Welcome** dialog box appears.
3. Click the **Next** button. The **License key** dialog box appears. This dialog box does not appear when you overwrite Protection Services on a machine on which Protection Services 1.4 has already been installed.
4. Enter the license key, and click the **Next** button. A dialog box prompting you to enter user information appears.
5. Enter the user name and company name, and click the **Next** button. A dialog box prompting you to confirm the installation destination appears.
6. Change the installation destination from the default, and click the **Next** button. If you change the installation destination directory, do not specify a directory where another product is installed. A dialog box prompting you to select the setup type appears.
7. Select the setup type, and click the **Next** button.
8. Enter the name of the program folder, and click the **Next** button. A dialog box appears, prompting you for confirmation before file copying starts.
9. Ensure that the information you specified is correct, and click the **Next** button. Installation starts. Wait until a message reporting that installation has finished is displayed.

   ***Note:*** If CCI is not installed in **C:\HORCM**, a dialog box prompting you to change the setup file appears.
10. Click the **Finish** button. When the installation finishes, the Protection Services – Copy Controller installation directory will be added to the **PATH** environment variable.

When you want to display or update the registered license information, execute the **drmlicense** command.

**(2) Installing Protection Services for SQL Server or Exchange Server**

To install Protection Services for SQL Server or Exchange Server (Windows environment):

1. Insert the installation CD-ROM of Protection Services for SQL Server or Exchange Server into the CD-ROM drive. This example assumes that the **x:** drive is the CD-ROM drive.
2. Run the **setup.exe** file on the CD-ROM (select **Start**, select **Run**, enter **x:\setup.exe**, and select **OK**). The **Welcome** dialog box appears.
3. Click the **Next** button. The **License key** dialog box appears. This dialog box does not appear when you overwrite Protection Services on a machine on which Protection Services 1.4 has already been installed.
4. Enter the license key, and click the **Next** button. A dialog box prompting you to select the setup type appears.
5. Select the setup type, and click the **Next** button.
6. Enter the name of the program folder, and click the **Next** button. A dialog box appears, prompting you for confirmation before file copying starts.
7. Ensure that the information you specified is correct, and click the **Next** button. Installation starts. Wait until a message reporting that installation has finished is displayed.
8. Click the **Finish** button.

When you want to display or update the registered license information, execute the **drmlicense** command.

**(3) Setting up the SQL Server database**

To set up the SQL Server database, use the **drmsqlinit** command to register the information about SQL Server. Register the following items according to the output messages:

- Storage directory for the Virtual Device Interface (VDI) metafiles
- VDI generation timeout period
- Storage directory for the UNDO log files
- Storage directory for the backup files (for transaction logs)

## 2.4 Setting Environment Variables in UNIX

Environment variables need to be set. In Windows, they are set automatically after installation. The environment variables you need to set are as follows:

- **PATH**
- **MANPATH**

### 2.4.1 PATH Environment Variable

In the PATH environment variable, add the following path to set the path to the commands:
**/opt/drm/bin/**

If you are using the Bourne shell, enter the following commands:
**PROMPT> PATH=/opt/drm/bin:$PATH**
**PROMPT> export PATH**

### 2.4.2 MANPATH Environment Variable

In the **MANPATH** environment variable, add the following path to set the path to the manuals: **/opt/drm/man/**

When using the Bourne shell, enter as follows:
**PROMPT> MANPATH=/opt/drm/man:$MANPATH**
**PROMPT> export MANPATH**

## 2.5 Setting Up Linkage with a Backup Management Product

This section describes how to set up linkage with a backup management product. You need to register parameters and create a configuration definition file.

### 2.5.1 Registering Parameters

Use the **drmtapeinit** command to register the information for linkage with a backup management product. Register the following items according to the output messages:

- Name of the backup management product
- Number of days to store the backup record used for tape backup

The *storage term of the backup records for tape backups* must be longer than the storage term of the media used by the backup management product (see Table 2.3). If the storage term of the backup records is shorter than the storage term of the media, after the storage term of a backup record expires, the backup associated with the backup record cannot be restored, even when the backup still remains on tape.

**Table 2.3 Storage Term of Media and Restorability**

| Storage Term of Media and Storage Term of Backup Records | Restorability |
|---|---|
| When the storage term of media is less than the storage term of backup records registered by **drmtapeinit** | Restoration using the **drmtaperestore** command or the **drmmediarestore** command is impossible. |
| When the storage term of media is greater than or equals the storage term of backup records registered by **drmtapeinit** | Restoration using the **drmtaperestore** command or the **drmmediarestore** command is possible. |

### 2.5.2 Creating Configuration Definition Files

Change the name of the definition file according to the backup management product you use, as follows:

- VERITAS NetBackup: **NBU.dat**
- VERITAS Backup Exec 8.6: **BENT.dat**
- VERITAS Backup Exec 9.0: **BEWS.dat**

The sample definition files are stored in the following locations:

- VERITAS NetBackup (for UNIX): **/opt/drm/conf/tape/NBU_sample.dat**
- VERITAS NetBackup (for Windows): ***Protection-Services-installation-directory*\conf\tape\NBU_sample.dat**
- VERITAS Backup Exec 8.6: ***Protection-Services-installation-directory*\conf\tape\BENT_sample.dat**
- VERITAS Backup Exec 9.0: ***Protection-Services-installation-directory*\conf\tape\BEWS_sample.dat**

***(1) Configuration parameters***. The parameters contained in the configuration files are in the order shown in Table 2.4 and Table 2.5.

**Table 2.4 Configuration File Parameters for Tape Backup (VERITAS NetBackup)**

| Parameter | Description |
|---|---|
| INST_PATH | Specify the absolute path in which VERITAS NetBackup is installed (within 1,024 bytes). |
| MOUNT_POINT | Specify the absolute path of the mount point of the volume that was backed up (within 255 bytes).<br>To back up a raw volume in UNIX, specify the special device file name for the secondary volume to be backed up. The following shows examples of the special device file names.<br>In Solaris (VERITAS Volume Manager):<br>Primary volume file name: **/dev/vx/dsk/dg01/vol-1**<br>Secondary volume file name: **/dev/vx/dsk/S*nn*dg01/vol-1**<br>In HP-UX (LVM):<br>Primary volume file name: **/dev/vg01/lvol1**<br>Secondary volume file name: **/dev/S*nn*vg01/lvol1**<br>For ***nn*** in the secondary volume file name, specify the backup generation number.<br>If the value of this parameter is set to default, the **CLASS** and **SCHEDULE** values will be used. |
| CLASS | Specify the class name used to back up the data stored in the path specified by **MOUNT_POINT** (within 255 bytes). |
| SCHEDULE | Specify the schedule name used to back up the data stored in the path specified by **MOUNT_POINT** (within 255 bytes). |
| PARALLEL_COUNT | Specify this when executing the following in parallel: backing up of data to tape, and restoring data from tape. Specify the number of backup processes to be executed in parallel: from 1 to 999. If you specify a non-numeric characters, or a number outside this range, execution will be performed sequentially, not in parallel. To execute backups in parallel, you need to set up VERITAS NetBackup. |

**Table 2.5 Configuration File Parameters for Tape Backup (VERITAS Backup Exec)**

| Parameter | Description |
|---|---|
| INST_PATH | Specify the absolute path in which VERITAS Backup Exec is installed (within 1,024 bytes). |
| MOUNT_POINT | Specify the absolute path of the mount point of the volume to be backed up (within 255 bytes). If the value of this parameter is set to default, the value specified by **SCRIPT_FILE** will be used for all directories. |
| SCRIPT_FILE | Specify the name of the backup job script file to be used to back up the data stored in the path specified by **MOUNT_POINT** (within 1,024 bytes). * |

* ***Note:*** The following shows the script keywords of VERITAS Backup Exec that are available for Protection Services. The portions in italics can be replaced with any value.

```
JOB_TYPE=Backup
JOB_NAME=testback
OVERWRITE_JOB=YES
MEDIA_NAME=DSK000001
MEDIA_SET=TAPEMEDIA_SET
APPEND=YES
APPEND_NO_OVERWRITE=YES
RUN_IMMEDIATE=YES
PATH1=
SUBDIRS1=
```

Parameters other than **INST_PATH** can be specified multiple times for a mount point. However, note the following:

- Always leave the line before the **MOUNT_POINT** line blank.
- Specify the configuration definition parameters in the order listed in the table above.
- When setting the **MOUNT_POINT** parameter to default, specify this parameter as the last entry.
- To specify the number of backup jobs to be executed in parallel, create a class definition for parallel execution as a definition method for VERITAS NetBackup.
- Depending on the created class definition, specify a mount point for each class name in this configuration definition file.

### *(2) Configuration file examples*

- Using VERITAS NetBackup in UNIX systems (**NBU.dat**):

```
INST_PATH=/usr/openv/netbackup

MOUNT_POINT=/disk03
CLASS=backup2
SCHEDULE=schedule2

MOUNT_POINT=default
CLASS=backup1
SCHEDULE=schedule1

PARALLEL_COUNT=2
```

- Using VERITAS NetBackup in Windows systems (**NBU.dat**):

```
INST_PATH=C:\Program Files\VERITAS\NetBackup

MOUNT_POINT=F:
CLASS=backup2
SCHEDULE=schedule2

MOUNT_POINT=G:
CLASS=backup1
SCHEDULE=schedule1

MOUNT_POINT=default
CLASS=backup1
SCHEDULE=schedule3

PARALLEL COUNT=2
```

- Using VERITAS Backup Exec (**BENT.dat***):

```
INST_PATH=C:\Program Files\VERITAS\Backup Exec\NT

MOUNT_POINT=E:\
SCRIPT_FILE=C:\BENT\E_Drive.txt

MOUNT_POINT=default
SCRIPT_FILE=C:\BENT\backup1.txt
```

* ***Note:*** If **BEWS.dat** is used, in the above entries replace **BENT** by **BEWS**.

## 2.6 Setting Up Linkage with CCI

In Protection Services, the CCI **HORCC_MRCF** environment variable is always set to **1**. Therefore, you do not need to set **HORCC_MRCF** when using any Protection Services command.

For the CCI settings, specify parameters in the **DEFAULT.dat** configuration definition file.

The location of the **DEFAULT.dat** configuration definition file differs depending on the operating system:

- In UNIX: **/opt/drm/conf/raid**
- In Windows: ***Protection-Services-installation-directory*\conf\raid**

If the **DEFAULT.dat** configuration definition file has an error or does not exist, the Protection Services commands will terminate abnormally. If you have deleted this configuration definition file by mistake, reinstall Protection Services.

### 2.6.1 Setting Up Instance Numbers

The setting of the CCI **HORCMINST** environment variable depends on the number of instances for CCI. You need to specify a **HORCMINST** parameter in the **DEFAULT.dat** file (see Table 2.6), for each CCI instance managed by Protection Services, per server.

**Table 2.6 Parameter in DEFAULT.dat for Instance Number**

| Parameter | Description | Default |
|---|---|---|
| HORCMINST | In this parameter, specify the number of the instance that manages the primary and secondary volumes to be backed up. The values of **HORCMINST** parameters are also set in **HORCMINST** environment variables.<br>The value of each **HORCMINST** parameter must be within the specifiable range of CCI.<br>The CCI instances specified in the **HORCMINST** parameters must be set in the CCI configuration file in advance so that the CCI instances can be activated.<br>Also, the instances at remote servers with which the CCI instances specified in the **HORCMINST** parameters communicate must be activated in advance. If they are not activated, the Protection Services command will fail. | 0 |

***Note:*** For further information on the CCI **HORCMINST** environment variable, please refer to the CCI manual for the applicable subsystem(s) (e.g., *Hitachi Lightning 9900™ V Series and Lightning 9900™ Command Control Interface (CCI) User and Reference Guide*, MK-90RD011).

### 2.6.2 Setting Up the Parameters for Checking the Status of a Pair

Protection Services determines whether a backup or restoration has finished by checking the status of the volume pair. By specifying parameters for the retry count and retry interval, you can set the retry count and retry interval for checking the pair status.

By default, Protection Services checks the pair status every five seconds, up to 120 times. This default setting assumes that a backup or restoration will finish in 10 minutes (5 seconds × 120 = 600 seconds = 10 minutes). If a volume is always being updated, a backup or restoration may be unable to finish in 10 minutes. In such a case, the backup or restoration command will terminate abnormally due to a timeout. To prevent the command from terminating abnormally due to a timeout, you must change the default setting (see Table 2.7).

**Table 2.7 Parameters in DEFAULT.dat for Retry Count and Retry Interval**

| Parameter | Description | Default (range) |
|---|---|---|
| RETRY_TIME | Specify the maximum retry count for checking the status of a pair. If you specify 0, Protection Services continues to retry checking until it can check the status. | 120 (0 to 3600) |
| RETRY_WAIT | Specify the number of seconds as the retry interval for checking the status of a pair. | 5 (0 to 3600) |

If the **RETRY_WAIT** parameter is small, the CPU load increases. Set the appropriate value, considering the CPU load. The **RETRY_WAIT** parameter varies depending on the storage subsystem. See Table 2.8 to set the appropriate value.

**Table 2.8 Values in the RETRY_WAIT Parameter Set for Storage Subsystems**

| Storage Subsystem | Description | Recommended Value |
|---|---|---|
| Thunder 9200<br>Thunder 9500V | A certain amount of time will elapse before the paired status changes. A wait time of at least one minute is needed. | 60 seconds |
| Lightning 9900<br>Lightning 9900V | For a pair status to change, a wait time of at least one second is needed. | 1 second |

Depending on the purpose of the processing, you can set the retry count and retry interval for checking the pair status. If you want to set the retry count and retry interval for a specific purpose, add the appropriate parameter in **DEFAULT.dat**. If you do not specify any purpose-specific parameters, the values of **RETRY_TIME** and **RETRY_WAIT** are used. Table 2.9 shows the parameters you can add.

**Table 2.9 Parameters in DEFAULT.dat for Retry Count and Pair Status Check Interval**

| Parameter | Description | Default (Range) |
|---|---|---|
| RESYNC_RETRY _TIME | Specifies the maximum number of times a retry can be performed for checking whether pair creation has finished.<br>Specify this parameter to check the pair status after paircreate or pairresync is executed for backup or resynchronization.<br>If you specify 0, Protection Services continues to retry checking until it can check the status. | Value of RETRY_TIME (0 to 3600) |
| RESYNC_RETRY _WAIT | Specifies the retry interval for checking whether pair creation has finished. You can specify a value in units of 10 milliseconds.<br>Specify this parameter to check the pair status after paircreate or pairresync is executed for backup or resynchronization. | Value of RETRY_WAIT (0 to 360000) |
| SPLIT_RETRY _TIME | Specifies the maximum number of times a retry can be performed for checking whether pair splitting has finished.<br>Specify this parameter to check the pair status after pairsplit is executed for backup or restoration.<br>If you specify 0, Protection Services continues to retry checking until it can check the status. | Value of RETRY_TIME (0 to 3600) |
| SPLIT_RETRY _WAIT | Specifies the retry interval for checking whether pair splitting has finished. You can specify a value in units of 10 milliseconds.<br>Specify this parameter to check the pair status after pairsplit is executed for backup or restoration. | Value of RETRY_WAIT (0 to 360000) |
| RESTORE _RETRY_TIME | Specifies the maximum number of times a retry can be performed for checking whether pair creation (from the secondary to the primary) has finished.<br>Specify this parameter to check the pair status after pairresync -restore is executed for restoration.<br>If you specify 0, Protection Services continues to retry checking until it can check the pair status. | Value of RETRY_TIME (0 to 3600) |
| RESTORE _RETRY_WAIT | Specifies the retry interval for checking whether pair creation (from the secondary to the primary) has finished. You can specify a value in units of 10 milliseconds.<br>Specify this parameter to check the pair status after pairresync -restore is executed for restoration. | Value of RETRY_WAIT (0 to 360000) |
| BUSY _RETRY_TIME | Specifies the maximum number of times a retry can be performed for checking the pair status if the CCI command is busy.<br>Specify this parameter to check the pair status if the CCI command was busy.<br>If you specify 0, Protection Services continues to retry checking until it can check the status. | Value of RETRY_TIME (0 to 3600) |
| BUSY _RETRY_WAIT | Specifies the retry interval for checking the pair status when the CCI command is busy. You can specify a value in units of 10 milliseconds.<br>Specify this parameter to check the pair status if the CCI command was busy. | Value of RETRY_WAIT (0 to 360000) |
| RESTORE_DELAY _RETRY_TIME | Maximum number of retry-count for checking the practicable of pairresync.<br>Specify this parameter for checking the status of pair is ready to execute the “pairresync -restore” in Restore. If 0 is specified, retry until status check is clear. | Value of RETRY_TIME (0 - 3600) |
| RESTORE_DELAY _RETRY_WAIT | Maximum number of retry-interval for checking the practicable of pairresync (10 msec)<br>Specify this parameter for checking the status of pair is ready to execute the “pairresync -restore” in Restore. | Value of RETRY_WAIT (0 - 360000) |

### 2.6.3 Setting Up the Track Size for Copying Data

You can change the track size for copying data that is to be resynchronized at backup or restoration (see Table 2.10). For example, you may want to change the track size for copying data in the following cases:

- When the priority of I/O for the primary volume is higher than the priority of data copying
- When the priority of data copying is higher in order to finish copying faster

For details on the values that can be specified as the track size, see the CCI documentation.

**Table 2.10 Parameter in DEFAULT.dat for Track Size for Copying Data**

| Parameter | Description | Default (Range) |
|---|---|---|
| COPY_SIZE | In this parameter, specify the track size for copying data. Specify a larger value to finish copying faster. | CCI default (1 to 15) |

When you execute a command, you can use the **DRM_COPY_SIZE** environment variable to change the track size. The change is also applied to the **COPY_SIZE** parameter.

## 2.7 Setting Up Operation of Protection Services

Protection Services operation is set in the **init.conf** environment configuration file. The location of the **init.conf** file differs depending on the operating system:

- In UNIX: **/opt/drm/conf/init.conf**
- In Windows: ***Protection-Services-installation-directory*\conf\init.conf**

If the **init.conf** environment configuration file has an error or does not exist, the Protection Services commands will use the defaults. If you have deleted this environment configuration file by mistake, reinstall Protection Services.

### 2.7.1 Setting Up the Parameters for Checking the Status of Cluster Resources

When Protection Services performs a cold backup or restoration in a cluster configuration, Protection Services can place the cluster resources online or offline. The retry operation checks whether the cluster resource is placed online or offline. If you want to change the retry count and retry interval for checking the status of the cluster resource, change the parameters shown in Table 2.11.

**Table 2.11 Parameters in init.conf for Checking the Status of Cluster Resources**

| Parameter | Description | Default (Range) |
|---|---|---|
| CLU_RETRY_TIME | In this parameter, specify the maximum retry count for checking the status of cluster resources. If you specify 0, Protection Services continues to retry checking until it can check the status. | 0 (0 to 3600) |
| CLU_RETRY_WAIT | In this parameter, specify the number of seconds as the retry interval for checking the status of cluster resources. | VCS: 1 or 2 (0 to 3600)<br>MCSG: 0 (0 to 3600)<br>MSCS: 1 (0 to 3600) |

### 2.7.2 Setting up the Parameters for Checking the Status of a Process

When Protection Services performs a cold backup or restoration in a cluster configuration, Protection Services activates or deactivates the service of the DBMS product to be backed up or restored. When Protection Services activates or deactivates the service, Protection Services checks the active/inactive status of the process. If you want to change the retry count and retry interval for checking the status of a process, change the parameters shown in Table 2.12.

**Table 2.12 Parameters in init.conf for Checking the Status of a Process**

| Parameter | Description | Default (Range) |
|---|---|---|
| SVC_RETRY_TIME | In this parameter, specify the maximum retry count for checking the status of a process. If you specify 0, Protection Services continues to retry checking until it can check the status. | 0 (0 to 3600) |
| SVC_RETRY_WAIT | In this parameter, specify the number of seconds as the retry interval for checking the status of a process. | 10 (0 to 3600) |

### 2.7.3 Setting Up the Backup Option (SQL Server only)

You can skip the confirmation of the SQL Server database status to shorten the time required for backup when the **drmsqlbackup** command is executed. When you want to shorten the time required for backup, change the following parameter:

**Table 2.13 Parameters in init.conf (Backup Option)**

| Parameter | Description | Default |
|---|---|---|
| SQL_QUICK_BACKUP | You can set this parameter to skip the confirmation of the SQL Server database status and shorten the time required for backup when the **drmsqlbackup** command is executed. | No setting (range = 1) |

In addition to changing the parameter, check the following conditions to shorten the time required for backup:

- Make sure that the database to be backed up is online. If the database to be backed up is not online, an error occurs when a snapshot backup is performed.
- Make sure that the CCI instance that manages the copy group to be operated is running. If the CCI instance is not running, an error occurs when the CCI command is issued.
- The previous backup information has been deleted. Use the **drmsqlcat** command to confirm whether or not the backup information has been deleted. To delete the backup information, use the **drmresync** command.
- The status of the copy group to be operated is **PVOL_PAIR**. Use the CCI **pairdisplay** command to confirm the status of the copy group.
- Make sure that the Quick Split option of the RAID device is on. If the Quick Split option of the RAID device is not on, the SQL Server database staticization is canceled in the PVOL_COPY status. The database staticization means that only the disk writing operation is temporarily stopped without stopping the SQL Server database updates. When the database staticization is canceled, the backup data of the secondary volume might fail.

### 2.7.4 Setting Up the Dictionary Map Synchronous Option

The execution time of a backup command can be shortened by updating the dictionary map asynchronously. To shorten the execution time of a backup command, set the parameter shown in Table 2.14.

**Table 2.14 Parameter of init.conf (Dictionary Map synchronous option)**

| Parameter | Description | Values | Default |
|---|---|---|---|
| DRM_DB_SYNC | It sets up whether renewal of a dictionary map is synchronized.<br>When YES is specified, the dictionary map is written in syncronous.<br>When NO is specified, it is asynchronous and a dictionary map is written in. | (YES \| NO) | YES |

## 2.8 Setting Up a Cluster Environment

In Windows, Protection Services allows you to put a file or database server in a cluster configuration so that the standby server can substitute for the active server if an error occurs. The environment setup differs according to the system configuration.

### 2.8.1 Using a Cluster Configuration in the Active-Passive Type

To set up the environment when using a cluster configuration in the Active-Passive type:

1. Change the locations of the dictionary map file and backup catalog.

   In the **init.conf** environment configuration files of Protection Services on the active and standby servers respectively, add the **DRM_DB_PATH=*directory-in-shared-disk*;*virtual-server-name*** entry. When editing the files, note the following points:

   - Add the entry to the last line of the **init.conf** file.
   - After ***directory-in-shared-disk*;*virtual-server-name***, always place a line feed code.
   - Specify a shared disk that is not to be backed up. Do not specify a shared disk that is part of a pair volume that is to be backed up.

   The following shows an example entry:

```
:
:
DRM_DB_PATH=H:\PTM;VHOST
```

2. Place the dictionary map file and backup catalog on the shared disk. On the active server, execute the **drmdbsetup** utility, as shown below.

   **PROMPT> set DRM_HOSTNAME=VHOST**
   **PROMPT> *Protection-Services-installation-directory*\bin\util\drmdbsetup -i**

   When the dictionary map file and backup catalog are created, the following message appears: **All data files were created.**

3. In the cluster system, register the shared disk as a cluster resource.

   For details on how to register a shared disk in the cluster system, see the documentation for the cluster product used in the cluster system.

   ***Note for SQL Server:*** In one cluster resource, register the service resource of one SQL Server instance only. When you register multiple SQL Server instances in one cluster source, backup and restoration cannot be performed correctly.

### 2.8.2 Using a Cluster Configuration in the Active-Active Type

To set up the environment when using a cluster configuration in the Active-Active type:

1. Set the locations of the dictionary map file and backup catalog.

   In the **init.conf** configuration definition files of Protection Services on the active and standby servers respectively, add a **DRM_DB_PATH=*directory-in-shared-disk*;*virtual-server-name*** entry for each virtual server. When editing the files, note the following points:

   - Add the entry to the last line of the **init.conf** file.
   - In ***directory-in-shared-disk***, specify a cluster resource of ***virtual-server-name***.
   - Specify a shared disk that is different from the volume to be backed up. Do not specify a shared disk that is part of a pair volume that is to be backed up.
   - After ***directory-in-shared-disk*;*virtual-server-name***, always place a line feed code.

   The following shows example entries:

```
:
:
DRM_DB_PATH=H:\PTM;VHOST1
DRM_DB_PATH=I:\PTM;VHOST2
```

2. Create the dictionary map file and backup catalog on each shared disk.

   On a server that can reference each shared disk, execute the **drmdbsetup** utility, as shown below.

   On a server that can reference the H drive, execute:

   **PROMPT> set DRM_HOSTNAME=VHOST1**
   **PROMPT> *Protection-Services-installation-directory*\bin\util\drmdbsetup -i**

   On a server that can reference the I drive, execute:

   **PROMPT> set DRM_HOSTNAME=VHOST2**
   **PROMPT> *Protection-Services-installation-directory*\bin\util\drmdbsetup -i**

   When the dictionary map file and backup catalog are created, the following message appears: **All data files were created.**

3. In the cluster system, register the shared disk that contains the dictionary map file and backup catalog as a cluster resource.

   For details on how to register a shared disk in the cluster system, see the documentation for the cluster product used in the cluster system.

   ***Note for SQL Server:*** In one cluster resource, register the service resource of one SQL Server instance only. When you register multiple SQL Server instances in one cluster source, backup and restoration cannot be performed correctly.

## 2.9 Creating the Dictionary Map File

After you finish all the environment setups, create the dictionary map file. By creating this file, you can check whether the environment has been set up correctly.

To create the dictionary map file:

1. For Copy Controller: Execute the **drmfsdisplay** command with the **-refresh** option specified as follows: **PROMPT> drmfsdisplay -refresh**

   For SQL Server: Execute the **drmsqldisplay** command with the **-refresh** option specified as follows: **PROMPT> drmsqldisplay -refresh**

   For Exchange Server: Execute the **drmexgdisplay** command with the **-refresh** option specified as follows: **PROMPT> drmexgdisplay -refresh**

2. When the following message appears, the environment has been set up correctly:

   **KAVX0023-I Dictionary map file was updated.**

   If this message does not appear, check the environment settings according to the error messages, if any.

## 2.10 Backing Up the Operating Environment of Protection Services

If you regularly back up the operating environment of Protection Services (the directories that contain Protection Services data and user-created files), you can restore the operating environment if a system error occurs.

When Protection Services is not used, use a tape backup product or another backup tool to back up the following directories and files regularly:

- All files under the **/opt/drm** directory (in Unix)
- All files under the **/var/opt/drm** directory (in Unix)
- All files under the ***Protection-Services-installation-directory*** (in Windows)
- The directory that contains the dictionary map file
- Definition files created after installing Protection Services

## 2.11 Uninstalling Protection Services

This section describes the procedures for uninstalling Protection Services. Before you start uninstallation, make sure that:

- You are logged in as a root user (administrator privileges).
- All programs are inactive.

To uninstall Protection Services programs in the following order. Note that this order differs from the installation order.

1. Uninstall Protection Services for SQL Server, Exchange Server, or Oracle.
2. Uninstall Protection Services - Copy Controller, and delete the settings related to Protection Services.

Table 2.15 shows the tasks needed for the file/database server and backup server.

**Table 2.15 Environment Setup Tasks for Servers (Uninstalling Protection Services)**

| Task | | File/Database Server | Backup Server |
|---|---|---|---|
| Uninstall Protection Services | Protection Services – Copy Controller | Needed | Needed |
| | Protection Services for SQL Server<br>Protection Services for Exchange Server<br>Protection Services for Oracle | Needed | Not needed |
| Delete the settings related to Protection Services | Delete environment variables | Needed | Needed |
| | Delete user-defined files | Needed | Needed |

### 2.11.1 Uninstalling Protection Services in Solaris

To uninstall Protection Services - Copy Controller:

1. Use the **ps** command to check whether there are Protection Services - Copy Controller commands that are currently running. Enter the following command:
   **PROMPT> ps -ef | grep drm**

   The processes whose names begin with **drm** are those of Protection Services. When processes are running, wait until all of them terminate.

2. Use the **pkgrm** command to uninstall Protection Services - Copy Controller. Enter the following command: **PROMPT> pkgrm HPTM**

3. The following messages appear, one at a time. Respond with **y** to both of them.

   **Do you want to remove this package?**
   **Do you want to continue removal of this package [y,n,?]**

   After uninstallation of Protection Services - Copy Controller has finished, the command prompt appears.

4. Delete user files. The **pkgrm** command does not delete the definition files, log files, and other files created by users after installation. To delete these files, delete the following **drm** directories:
   **/opt/drm**
   **/var/opt/drm**

### 2.11.2 Uninstalling Protection Services in HP-UX

To uninstall Protection Services - Copy Controller:

1. Use the **ps** command to check whether there are Protection Services - Copy Controller commands that are currently running. Enter the following command:

   **PROMPT> ps -ef | grep drm**

   The processes whose names begin with **drm** are those of Protection Services. When processes are running, wait until all of them terminate.

2. Use the **swremove** command to uninstall Protection Services - Copy Controller. Enter the command as follows:

   **PROMPT> swremove HPTM**

   After Protection Services is uninstalled, the command line prompt appears.

3. Delete the user files. The **pkgrm** command does not delete the definition files and log files that the users created after installation. To delete these files, delete the following drm directories:

   **/opt/drm**

   **/var/opt/drm**

### 2.11.3 Uninstalling Protection Services in Windows

To uninstall Protection Services for SQL Server or Exchange Server:

1. Open the **Add/Remove Programs** control panel (select **Start**, select **Settings**, select **Control Panel**, and double-click on **Add/Remove Programs**).
2. In the **Currently installed programs** list, select the desired HiCommand Protection Services program (SQL Server or Exchange Server), and then click the **Remove** button.
3. A dialog box appears to verify that you want to delete Protection Services. Click the **Delete** button, and then the **Next** button.
4. A dialog box confirming deletion of the selected Protection Services component appears. Click **OK** to start uninstallation. After uninstallation finishes, close the dialog box.
5. Delete any user files that were created after installation (e.g., definition files, log files).

To uninstall Protection Services - Copy Controller:

1. Open the **Add/Remove Programs** control panel (select **Start**, select **Settings**, select **Control Panel**, and double-click on **Add/Remove Programs**).
2. In the **Currently installed programs** list, select **Protection Services – Copy Controller**, and then click the **Change or Remove Programs** button.
3. When the panel asking you to confirm deletion of Protection Services appears, select **Delete**, and then select **Next**.
4. When the panel confirming deletion of Protection Services appears, select **OK** to start uninstallation.
5. After uninstallation finishes, close the dialog box.
6. Delete any user files that were created after installation (e.g., definition files or log files).
7. Delete the Protection Services - Copy Controller installation folder from the PATH system environment variable. For details on how to change environment variables, see the Windows help.

# Chapter 3 Using Extended Commands

This chapter describes the extended commands that Protection Services provides.

3.1 Overview of extended commands

3.2 System configuration examples

3.3 Preparations for executing extended commands

3.4 Procedures of extended commands

3.5 Examples of using extended commands (in UNIX)

3.6 Examples of using extended commands (in Windows)

3.9 Log files for extended commands

3.10 Extended command specifications

## 3.1 Overview of Extended Commands

An extended command is used to reduce the effort required to perform data protection operations such as backup or restoration. You can use extended commands to automatically perform backup and restoration, without needing to specify further complicated operations.

For example, use Protection Services commands to back up data to tape. In this case, you must interactively execute commands having the following functions:

1. Unlock the secondary volume.
2. Mount the secondary volume.
3. Unmount the secondary volume.
4. Lock the secondary volume.
5. Back up data to the secondary volume.
6. Check the execution results of the backup.
7. Export the backup record to a temporary file.
8. Lock the primary volume.
9. Transfer a temporary file to the backup server.
10. Import the backup record from the temporary file.
11. Check the execution results of the import.
12. Back up the data of the secondary volume to a tape.
13. Check the execution results of the tape backup.
14. Unlock the primary volume.

For all the above commands, specifying the resource information to be operated on and the information related to backup can be complicated.

The above information is pre-defined in an extended command. You can use a tool such as operation management software to automatically execute extended commands. Therefore, you can perform backup without needing to specify detailed operations, thereby reducing the effort required for data protection operations. By using HiCommand Policy Manager as operation management software, you can integrate and manage storage subsystem operations. For information on HiCommand Policy Manager, please contact your Hitachi Data Systems account team.

### 3.1.1 List of Extended Commands

Table 3.1 lists and describes the extended commands of Protection Services. Table 3.2 lists and describes the extended commands of Protection Services for SQL Server.

Extended commands are installed in the following directory:

In UNIX: **/opt/drm/script/bin**

In Windows: ***Protection-Services-installation-directory*\script\bin**

**Table 3.1 Extended Commands for Copy Controller**

| Extended Command Name | General Explanation | Section |
|---|---|---|
| EX_DRM_BACKUPID_SET | Generates a backup ID file. | 3.10.1 |
| EX_DRM_CACHE_PURGE | Clears the cache of the secondary volume (for Windows). | 3.10.2 |
| EX_DRM_CG_DEF_CHECK | Checks the contents of the copy group list file. | 3.10.3 |
| EX_DRM_DB_EXPORT | Exports a backup record to a file. | 3.10.4 |
| EX_DRM_DB_IMPORT | Imports a backup record from a file. | 3.10.5 |
| EX_DRM_FS_BACKUP | Backs up the file system. (Copy Controller only) | 3.10.6 |
| EX_DRM_FS_DEF_CHECK | Checks the contents of an operation definition file. (Copy Controller only) | 3.10.7 |
| EX_DRM_FS_RESTORE | Restores the file system in the primary volume. (Copy Controller only) | 3.10.8 |
| EX_DRM_FTP_GET | Gets a backup record file from the backup server. | 3.10.9 |
| EX_DRM_FTP_PUT | Transfers a backup record file to the backup server. | 3.10.10 |
| EX_DRM_HOST_DEF_CHECK | Checks the contents of the host environment settings file. | 3.10.11 |
| EX_DRM_RESYNC | Resynchronizes the copy group. | 3.10.12 |
| EX_DRM_TAPE_BACKUP | Backs up the data of the secondary volume to a tape. | 3.10.13 |
| EX_DRM_TAPE_RESTORE | Performs a restoration from a tape to the secondary volume. | 3.10.14 |

**Table 3.2 Extended Commands for SQL Server**

| Extended Command Name | General Explanation | Section |
|---|---|---|
| EX_DRM_SQL_BACKUP | Backs up the SQL Server database. | 3.11.1 |
| EX_DRM_SQL_DEF_CHECK | Checks the contents of the operation definition file. | 3.11.2 |
| EX_DRM_SQL_RESTORE | Restores the SQL Server database in the primary volume. | 3.11.3 |
| EX_DRM_SQL_TLOG_BACKUP | Backs up the transaction log of SQL Server. | 3.11.4 |
| EX_DRM_SQLFILE_EXTRACT | Deploys the latest SQL Server metafile to the folder to be backed up to a tape. | 3.11.5 |
| EX_DRM_SQLFILE_PACK | Backs up the SQL Server metafiles. | 3.11.6 |

**Table 3.3 Extended Commands for Exchange Server**

| Extended Command Name | General Explanation | Section |
|---|---|---|
| EX_DRM_EXG_BACKUP | Backs up the Exchange Server database. | 3.12.1 |
| EX_DRM_EXG_DEF_CHECK | Checks the contents of the operation definition file. | 3.12.2 |
| EX_DRM_EXG_VERIFY | Verifies the consistency of the Exchange database. | 3.12.3 |

### 3.1.2 Before Executing Extended Commands

You must be familiar with the information described in this section in order to use extended commands. The topics are grouped as follows:

- Execution permission for extended commands
- Automatic execution of extended commands
- Operation IDs
- Definition files used by extended commands
- FTP service

***(1) Execution permission for extended commands***

You must have system administrator permission to execute the extended commands.

***(2) Automatic execution of extended commands***

A backup or restoration process that uses extended commands may be performed across more than one server. Since it is difficult to execute extended commands at each of physically remote servers, you need to perform remote execution of the extended commands. If you want to repeat execution of extended commands, you need to set up automatic execution.

In such a case, install the operation management software that meets the following requirements:

- The software can be started by specifying the file name in VBScript (Microsoft Visual Basic Scripting Edition) and shell script programs (batch files).
- Operations such as repeat executions of programs and evaluating conditions can automatically be executed according to a predefined execution order and schedule.

We recommend that you use operation management software to make a process of executing extended commands more simple. By using HiCommand Policy Manager as operation management software, you can integrate and manage storage subsystem operations. For information on HiCommand Policy Manager, please contact your Hitachi Data Systems account team.

### *(3) Operation IDs*

An operation ID is a unique character string given to each resource that will be the processing target of an extended command. An operation ID is specified as an argument of an extended command. For the operation ID, specify a unique name among all the servers that are used for extended commands.

The following shows an example of specifying an operation ID:
***server-name-of-operation-target*** + ***resource-name-to-be-operated***

An operation ID can have up to 64 ASCII characters except the following special characters that cannot be used in a file name: \ / : . * ? " < > |

If you use operation management software, you can predefine programs that use extended commands, and can use the name of the programs as operation IDs.

In a UNIX environment, operation IDs are case sensitive. In a Windows environment, operation IDs are not case sensitive.

### *(4) Definition files used by extended commands*

The extended command definition files manage various kinds of information on the environment for executing extended commands. Before executing extended commands, you need to use a text editor to create the extended command definition files and store them in each server where the extended commands will be executed. Create the following files according to the configuration of the system where extended commands will be executed:

- Operation definition file

  This file defines information about the storage destination of file system files, target storage groups, and temporary files. Create it in association with the operation ID. When you specify the operation ID as an argument of an extended command, the system references the information in the operation definition file corresponding to the operation ID.

- Host environment settings file

  A host environment settings file defines information about a host and log files. Create a host environment settings file for each host.

For details on how to create the above definition files, see section 3.3.

### *(5) FTP service*

When you execute extended commands, temporary files containing information required for data backup or restoration are generated. When you execute extended commands on a system running a database server and a backup server, these temporary files are transferred between the database server and the backup server by the FTP service.

Before using the FTP service, set a FTP server on the backup server.

### 3.1.3 Notes on Executing the Extended Commands

You use the MS-DOS prompt or operation management software to start extended commands.

If you want to use operation management software to control extended commands, start them by using the program execution definition functionality of the software. When you use this functionality, specify extended command names as the names of programs to be executed.

If you want to start an extended command by using the MS-DOS prompt in the Windows environment, take either of the following actions so that **cscript.exe** starts the extended commands:

- Change the host parameter, and then execute the extended commands:

  From the MS-DOS prompt, enter the following command. Once you change the host parameter, you do not need to change it any longer.

  **cscript //H:Cscript**

- Specify the **cscript** command so that it executes an extended command.

  Execute the **cscript** command in the following format:

  **cscript** ***name-of-the-extended-command-you-want-to-execute***

In the Windows default settings, **wscript.exe** starts an extended command and a pop-up dialog box appears. The dialog box displays the execution results of the command. Therefore, note that an extended command cannot execute automatically.

You cannot specify the same operation ID for multiple extended commands and execute these commands in parallel.* Doing so will cause the extended commands to terminate abnormally, or the backup catalog that is the target of the extended commands may be destroyed.

**** For SQL Server:*** The EX_DRM_SQL_TLOG_BACKUP can specify the same operation ID as other extended commands and execute extended commands in parallel.

## 3.2 System Configuration Examples

This section describes three major system configurations for executing extended commands:

- System configuration for backing up and restoring data between volumes
- System configuration for performing a tape backup and restoration
- System configuration when the file/database server is in a cluster configuration

### 3.2.1 System Configuration: Backing Up and Restoring Data Between Volumes

When there is only one server, use the extended commands to back up data from the primary volume to the secondary volume. To restore data from the secondary volume to the primary volume, use the commands provided by Protection Services. Install Protection Services onto the file/database server, and execute the extended commands from the file/database server.

Figure 3.1 shows a system configuration for backing up and restoring data between volumes.

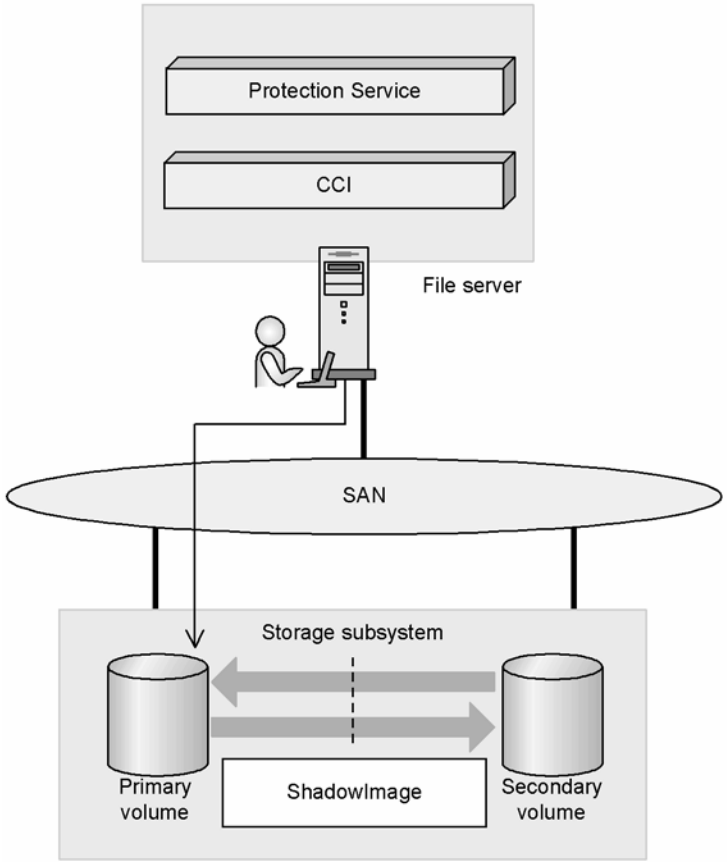



**Figure 3.1 System Configuration for Backing Up and Restoring Data Between Volumes**

### 3.2.2 System Configuration: Performing Tape Backups and Restorations

In the system configuration that has a file/database server and a backup server connected to a tape device, you can back up data to a tape and can restore data from a backup tape.

To store backup data to a tape, use the extended commands. To restore backup data from a tape, use the Protection Services commands.

Figure 3.2 shows a system configuration for performing a tape backup and restoration. In this example, the backup server serves as an FTP server. Protection Services is installed on the database server and backup server. For the primary volume, extended commands are executed from the database server. For the secondary volume, extended commands are executed from the backup server.

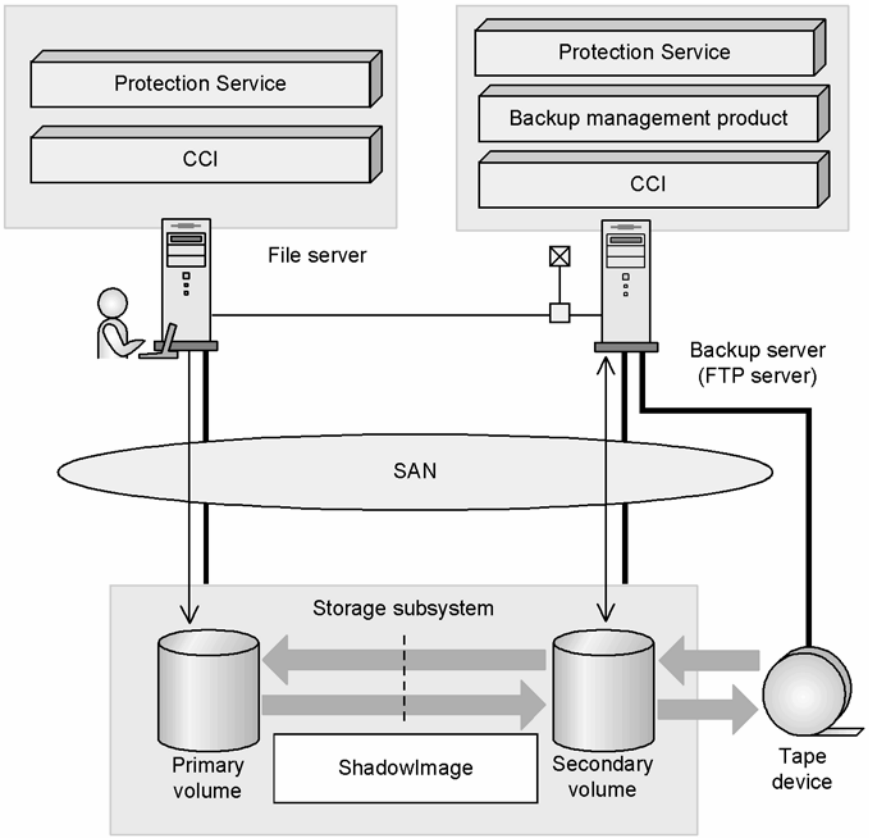



**Figure 3.2 System Configuration for Performing a Tape Backup and Restoration**

### 3.2.3 System Configuration: File/Database Server in a Cluster Configuration

In Windows, when Protection Services is used in an environment where the file/database server has a cluster failover configuration, if an error occurs on the active server, the standby server can substitute for the active server. In a multi-server system where the database server has a cluster configuration, you can back up data to a tape and can restore data from its backup tape.

To store backup data to a tape, use the extended commands. To restore backup data from a tape, use the Protection Services commands.

Figure 3.3 shows a system configuration when a file server is in a cluster configuration. Mount point directories **M:**, **N:**, and **D:** have been created in **File Server A** and **File Server B**, respectively, and **Virtual Server C** has been set in each mount point directory, respectively.

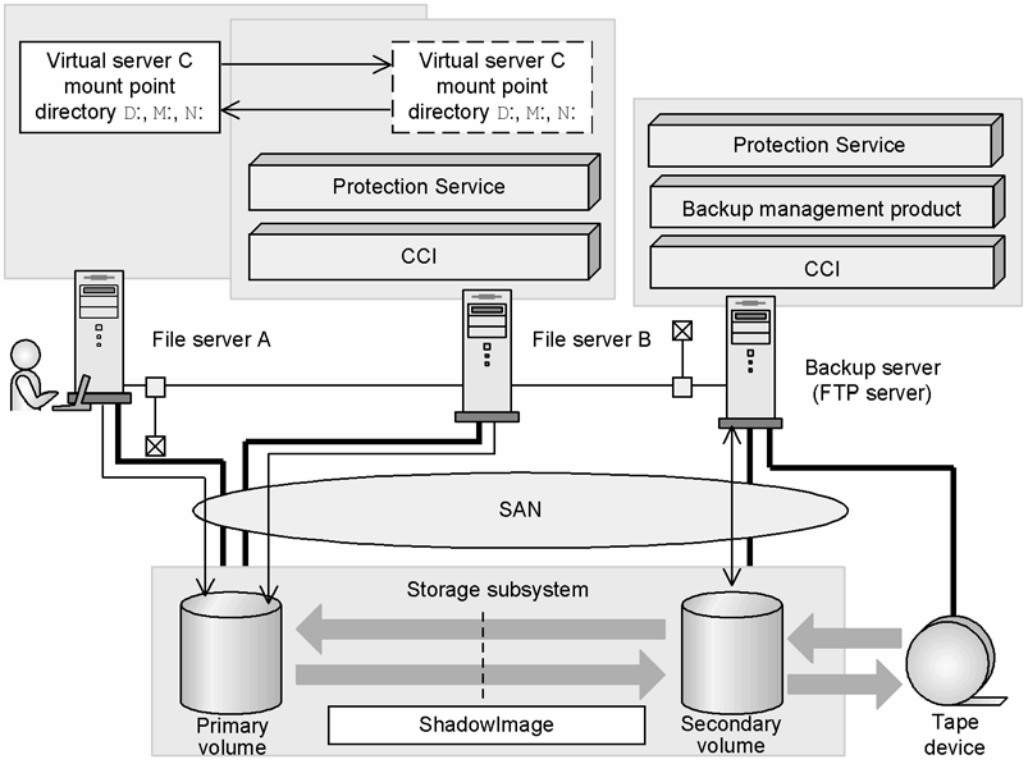



**Figure 3.3 System Configuration: File Server in a Cluster Configuration**

Figure 3.4 shows a system configuration when a database server is in a cluster configuration. In this example, the virtual server C is set for the SQL Server instance **INSTANCE_1**.

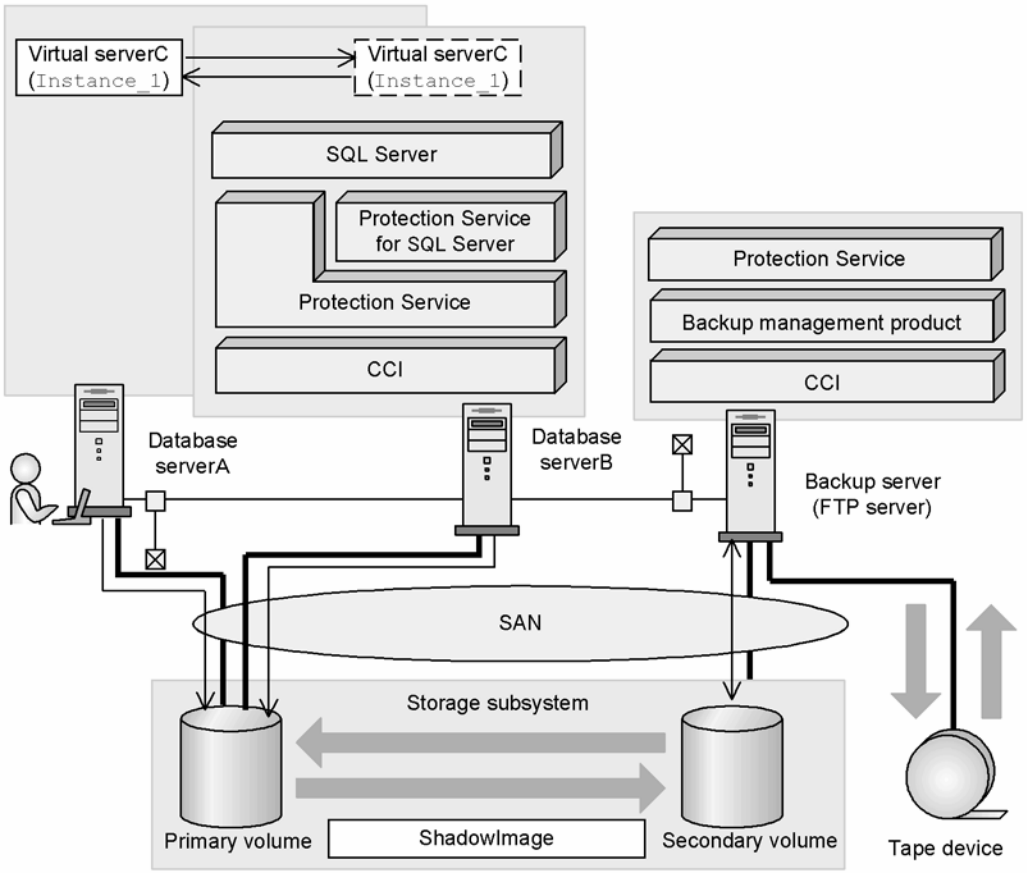



**Figure 3.4 System Configuration: SQL Server in a Cluster Configuration**

Figure 3.5 shows a system configuration when a database server is in a cluster configuration. In this example, the virtual server C is set for the storage group **STORAGE_1**.

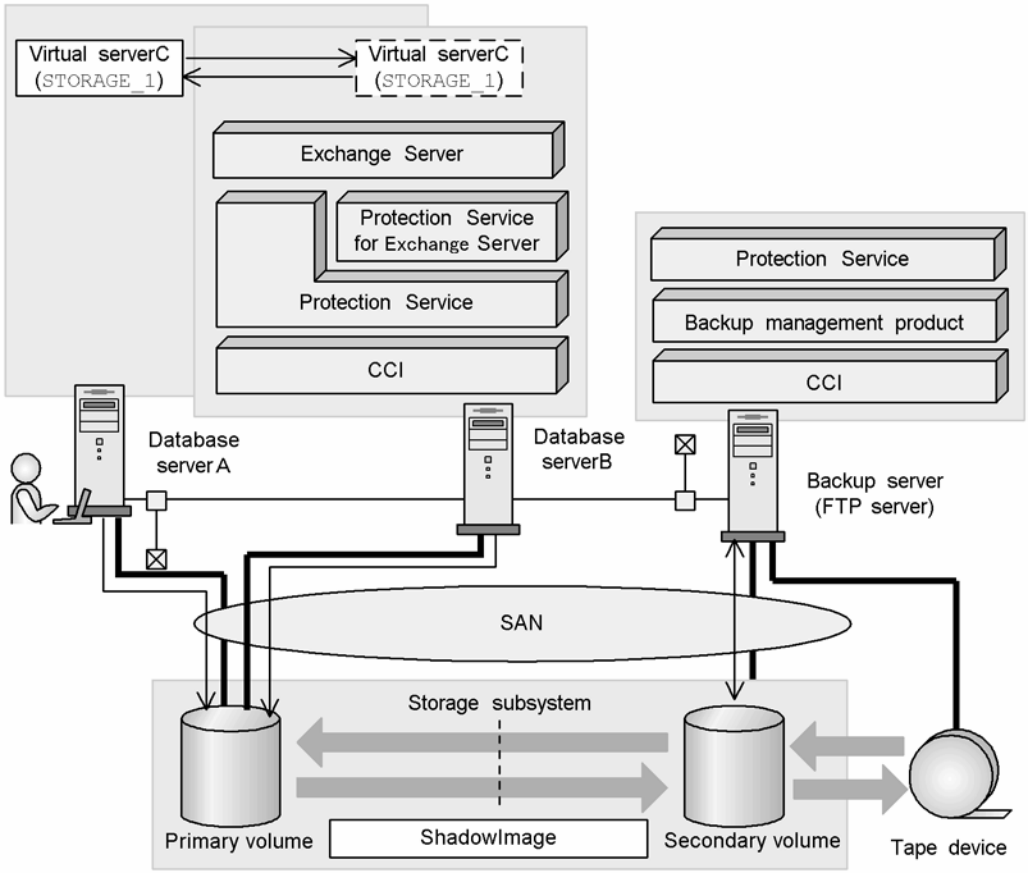



**Figure 3.5 System Configuration: Exchange Server in a Cluster Configuration**

In the preceding system configurations, suppose the backup server serves as an FTP server, and the standby file/database server contains the same programs as those installed in the active file server. Protection Services is installed on the file/database servers and backup server. For the primary volume, extended commands are executed from the file/database server. For the secondary volume, extended commands are executed from the backup server.

## 3.3 Preparations for Executing Extended Commands

Before executing extended commands, Protection Services and program products that are prerequisites for Protection Services need to be installed and set up. For details on the installation and setup, see Chapter 2.

The preparations for executing extended commands are as follows:

- Create VDI metafile storage directory (SQL Server)
- Create a temporary directory (folder) for extended commands
- Set up the operating environment for Protection Services
- Create an operation definition file
- Create a host environment settings file
- Check the FTP service (in a system configuration for tape backups)

The preparation tasks on a file or database server are different from the preparation tasks on a backup server. Table 3.4 shows the preparation tasks for each server:

**Table 3.4 Preparation Tasks for Servers for Extended Commands**

| Tasks | | File Server | Database Server | Backup Server |
|---|---|---|---|---|
| Create a VDI metafile storage directory (SQL Server) | | Needed | Needed | Needed |
| Create a temporary directory (folder) for extended commands | | Needed | Needed | Needed |
| Set up the operating environment for Protection Services | Set up SQL Server information | -- | Needed | Not needed |
| | Create a dictionary map file | Needed | Needed | Not needed |
| | Set up information about the backup management product | Not needed | Not needed | Needed |
| Create a mount point directory list file (Copy Controller only) | | Needed | Needed | Not needed |
| Create an operation definition file | | Needed | Needed | Needed |
| Create a host environment settings file | | Needed | Needed | Needed |
| Create a copy group list file | | Needed | Needed | Needed |
| Check the FTP service (in a system configuration for tape backups) | | Not needed | Needed | Needed for Copy Controller<br>Not needed for database products |

### 3.3.1 Creating VDI Metafile Storage Directories (SQL Server)

After a backup or restoration is performed, the following files are generated:

- SQL Server metafile
- Transaction log file
- Undo log file

You need to create a VDI metafile storage directory in a database server and a backup server respectively. The same name for VDI metafile storage directories must be specified on the database server and the backup server. To identify multiple database server instances on the backup server, specify the following name:
***desired-directory\target-server-name\target-instance-name***

### 3.3.2 Creating a Temporary Directory for Extended Commands

When an extended command is executed, the following temporary files are created:

- SQL Server metafile
- Backup ID file
- Backup record file

The FTP service transfers these temporary files between servers. To use the FTP service, you must create temporary directories for storing the copies of the temporary files for each server (i.e., file/database server, backup server) before you execute extended commands.

**In UNIX:**

Specify temporary directory names for a file server and a backup server respectively in the following format: ***desired-directory/operation-ID***

**In Windows – Copy Controller:**

Specify a temporary directory name for a file server in the following format:
***desired-directory\operation-ID***

When the file server is in a cluster configuration, on the shared disk, create a directory for storing temporary files for the file server.

Specify the following name to create a temporary directory for the backup server:
***home-directory-of-the-FTP-site\operation-ID***

Internet Information Services (IIS) sets the home directory of the FTP site.

**In Windows – SQL Server:**

Create a temporary folder of the database server for each instance. Specify the following name: ***desired-directory\instance-name***

In the ***desired-directory***, specify a directory other than the VDI metafile storage directory.

When the database server is in a cluster configuration, on the shared disk, create a directory for storing temporary files for the database server.

You also create a temporary folder for the backup server in the home directory of the FTP site. This folder name must match the value specified in the **BK_DATA_FILE_DIR** operation definition file. Specify the following name:
***home-directory-of-the-FTP-site\database-server-name\instance-name***

Internet Information Services (IIS) sets the home directory of the FTP site.

**In Windows – Exchange Server:**

You create the temporary folder for the database server in the extended commands installation folder. This folder name must match the value specified in the **DB_DATA_FILE_DIR** operation definition file.

When the database server is in a cluster configuration, on the shared disk, create a directory for storing temporary files for the database server.

You also create a temporary folder for the backup server in the home directory of the FTP site. This folder name must match the value specified in the **BK_DATA_FILE_DIR** operation definition file. Specify the following name:
***home-directory-of-the -FTP-site\target-server-name***

Internet Information Services (IIS) sets the home directory of the FTP site.

### 3.3.3 Setting the Operating Environment for Executing Extended Commands

To set the operating environment of Protection Services for executing extended commands:

1. Set the information about the database server.

   **SQL Server:** Execute the **drmsqlinit** command on the SQL Server instance to be operated. Register the following items depending on the output message:

   - VDI metafile storage directory (register the directory created in section 3.3.1)
   - VDI-generation timeout
   - UNDO log file directory
   - Transaction log backup file directory

2. Create a dictionary map file.

   **Copy Controller:** Execute the **drmfsdisplay** command with the **-refresh** option.

   **SQL Server:** Execute the **drmsqldisplay** command with the **-refresh** option.

   **Exchange Server:** Execute the **drmexgdisplay** command with the **-refresh** option.

3. Set the information about the backup management product. Execute the **drmtapeinit** command. Register the following items depending on the output message:

   - Name of the backup management product
   - Number of days for which to store the backup catalog for tape backups

### 3.3.4 Creating an Operation Definition File (for UNIX)

Create an operation definition file according to the configuration of the system using extended commands. After creating the extended command definition files, store them in the following directory of each server where extended commands will be executed:

**/opt/drm/script/conf/**

***(1) Locations of operation definition files***

Create two identical operation definition files for each target mount point or file. Place one operation definition file on the file server and the other on the backup server. Figure 3.6 shows the locations of operation definition files.

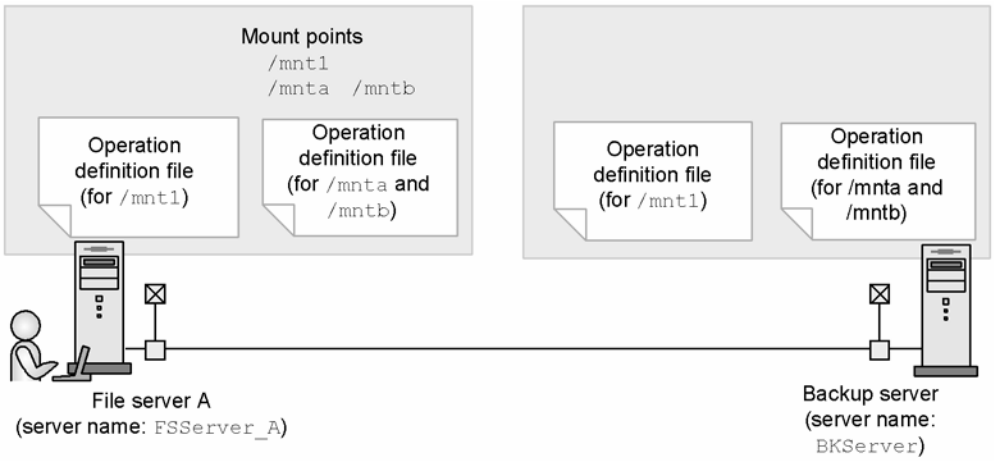



**Figure 3.6 Locations of Operation Definition Files (UNIX)**

File server A (server name: **FSServer_A**) has three mount points **/mnt1**, **/mnta**, and **/mntb**. This example assumes that mount points **/mnta** and **/mntb** have been defined to be processed in batch mode in the **app.txt** mount point directory list file.

In this case, on file server A, you would place an operation definition file for **/mnt1** and an operation definition file for the mount point directories specified in **app.txt** (**/mnta** and **/mntb**). On the backup server (server name: **BKServer**), you would place an operation definition file for **/mnt1**, **/mnta**, and **/mntb**.

### *(2) Format of operation definition files*

An operation definition file is created, for each operation ID that uniquely identifies the processing target, with a name in the following format:

**/opt/drm/script/conf/*_operation-ID*.dat**

Table 3.5 shows the entries of an operation definition file, their contents, and the maximum value length (in bytes). Specification of these entries is required.

**Table 3.5 Example: Contents of Entries in an Operation Definition File (UNIX)**

| Specification Item | Information to be Specified | Maximum No. of Characters |
|---|---|---|
| BACKUP_OBJECT | Specify a character string identifying the type of the backup object. Specify FILESYSTEM. | 32 |
| DB_SERVER_NAME | Specify the file system name. | 128 |
| INSTANCE_NAME | Specify the mount point directory name or mount point directory list file name. | 128 |
| TARGET_NAME | Specify the file name or directory name to be backed up.<br>This entry is valid only when backup is performed, and cannot be used when restoration is performed.<br>You can specify multiple file names or directories, separated by commas.<br>If you omit this value, backup is executed for each mount point. | 1,024 |
| DB_DATA_FILE_DIR *1 | Specify a temporary directory for the extended commands on the file server. Specify a directory that actually exists even if you do not use a backup server. *2 | 128 |
| BK_DATA_FILE_DIR *1 | Specify a temporary directory for extended commands on the backup server. *2<br>If you are not using a backup server, specify -. | 128 |
| SET_DRM_HOSTNAME | Specify a value of 0. | 1 |

***Notes:***

1. Do not specify the value in the DB_DATA_FILE_DIR entry and BK_DATA_FILE_DIR entry.
2. Specify the absolute path for the directory name. Do not specify the relative path or shared name. The directory names are case sensitive.

### *(3) Operation definition file creation procedure*

This section describes the procedure for creating an operation definition file when a tape backup is performed, based on the example system configuration shown in Figure 3.6 above.

This example assumes the following conditions:

- File server A (server name: **FSServer_A**) has three mount point directories **/mnt1**, **/mnta**, and **/mntb**.
- Mount points **/mnta** and **/mntb** have been set to be processed in batch mode in the **APP.txt** mount point directory list file.
- The storage directories for extended command temporary files listed in Table 3.6 have been created in file server A and the backup server (server name: **BKServer**).

In this example, you create an operation definition file for each of the operation IDs listed in Table 3.7.

**Table 3.6 Storage Directories for Extended Command Temporary Files (UNIX)**

| Server Name | Storage Directories |
|---|---|
| FSServer_A | /var/opt/drm_FS_tmp/Operation_A<br>/var/opt/drm_FS_tmp/Operation_B |
| BKServer | /var/opt/drm_bk_tmp/Operation_A<br>/var/opt/drm_bk_tmp/Operation_B |

**Table 3.7 Operation IDs for which an Operation Definition File is Created (UNIX)**

| Operation ID | Target File Server | Target Mount Point or File |
|---|---|---|
| Operation_A | File server A | Entire **/mnt1** |
| Operation_B | File server A | Mount point directories specified in **app.txt** (**/mnta** and **/mntb**) |

To create an operation definition file:

1. Create an operation definition file on file server A and set the required items. Create two files with the following file names:

   **/opt/drm/script/conf/_Operation_A.dat**

   **/opt/drm/script/conf/_Operation_B.dat**

   Specification example of **/opt/drm/script/conf/_Operation_A.dat**:

```
BACKUP_OBJECT=FILESYSTEM
DB_SERVER_NAME=FSServer_A
INSTANCE_NAME=/mnt1
TARGET_NAME=
DB_DATA_FILE_DIR=/var/opt/drm_FS_tmp/Operation_A
BK_DATA_FILE_DIR=/var/opt/drm_bk_tmp/Operation_A
SET_DRM_HOSTNAME=0
```

   Specification example of **/opt/drm/script/conf/_Operation_B.dat**:

```
BACKUP_OBJECT=FILESYSTEM
DB_SERVER_NAME=FSServer_A
INSTANCE_NAME=app
TARGET_NAME=
DB_DATA_FILE_DIR=/var/opt/drm_FS_tmp/Operation_B
BK_DATA_FILE_DIR=/var/opt/drm_bk_tmp/Operation_B
SET_DRM_HOSTNAME=0
```

2. On file server A, execute the check tool **EX_DRM_FS_DEF_CHECK** for operation definition files.

   **"EX_DRM_FS_DEF_CHECK" "operation-ID" -db**

   If an error occurs, correct the contents of the file, and execute the check tool again.

3. Copy the operation definition files created on file server A to the backup server. Copy the files to the following directory:

   **/opt/drm/script/conf/**

4. On the backup server, execute the check tool **EX_DRM_FS_DEF_CHECK** for operation definition files.

   **"EX_DRM_FS_DEF_CHECK" "operation-ID" -bk**

   If an error occurs, change the backup server configuration depending on the contents of the operation definition file, or change the contents of the operation definition file depending on the backup server configuration. When you change the backup server configuration, re-execute the checking tool. When you change the contents of the operation definition file, place the same file on the file server, and then re-execute the checking tool.

### 3.3.5 Creating an Operation Definition File (for Windows)

An operation definition file is created depending on the configuration of the system using extended commands. After you create the extended command definition files, store them in the following directory of each server where extended commands will be executed:

***Protection-Services-installation-directory*\script\conf**

#### *(1a) Locations of operation definition files (file servers)*

Create two identical operation definition files for each target mount point or file. Place one operation definition file on the file server and the other on the backup server. In a cluster configuration, the same operation definition file must be located on all the servers where the cluster resource (mount point or file) to be backed up is defined.

Figure 3.7 shows the locations of operation definition files for a sample system with two file servers and one backup server.

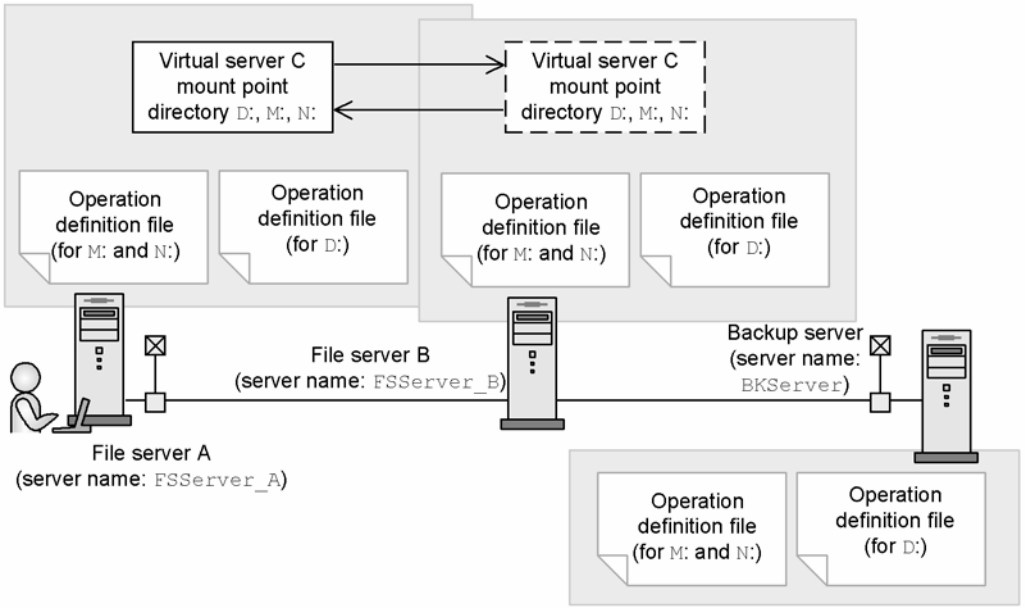



**Figure 3.7 Locations of Operation Definition Files (Windows, File Servers)**

In this example, the virtual server **VServer_C** is running on file server A (server name: **FSServer_A**) and file server B (server name: **FSServer_B**), which make up the cluster.

The three mount points **D:**, **M:**, and **N:** exist on file server A and file server B, and the virtual server C (server name: **VServer_C**) has been defined as a cluster resource. The mount points **M:** and **N:** are assumed to be set in the mount point directory target definition file **app.txt** so that the mount point directories are operated at one time.

In this example, on file servers A and B, place the operation definition file about **D:** and the operation definition file about mount point directories **M:** and **N:** specified in the **app.txt**. On the backup server (server name: **BKServer**), place the operation definition file about **D:** and the operation definition file about **M:** and **N:**.

### *(1b) Locations of operation definition files (SQL Server/Exchange Server)*

Create two identical operation definition files for one target instance/storage group. Place one operation definition file on the database server and the other on the backup server. In a cluster configuration, the same operation definition file must be located on all the servers where the cluster resource (instance or database/storage group) to be backed up is defined.

Figure 3.8 shows the locations of operation definition files for a sample system with two database servers and one backup server.

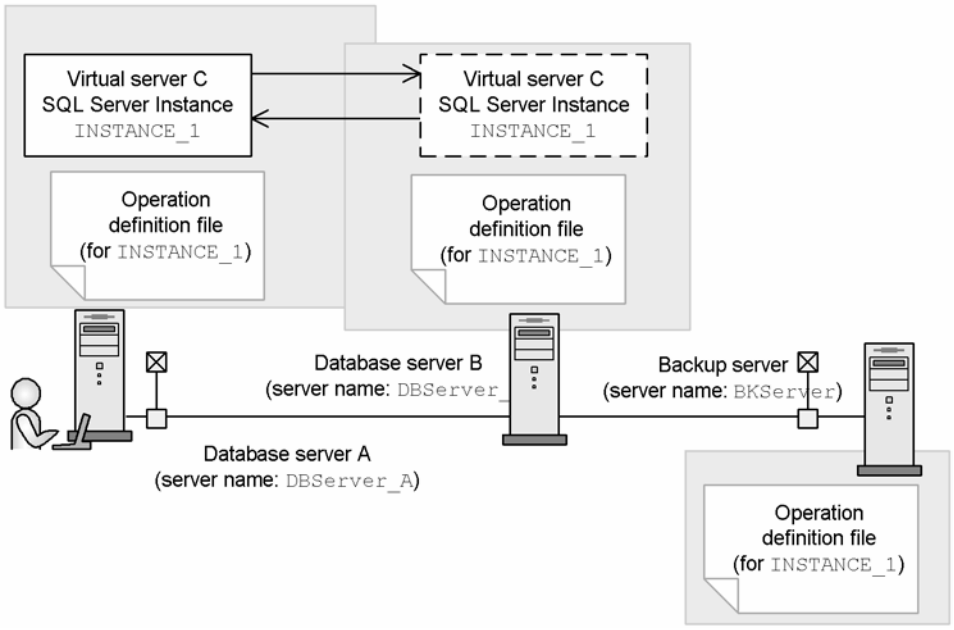



**Figure 3.8 Locations of Operation Definition Files (Windows, SQL Server shown)**

In this example, the virtual server (server name: **VServer_C**) is running on database server A (server name: **DBServer_A**) and database server B (server name: **DBServer_B**), which are making up the cluster.

The SQL Server instance **INSTANCE_1** exists on database A and database B, and virtual server C has been defined as a cluster resource.

In this example, the operation definition file for the instance **INSTANCE_1** is located on database server A, database server B, and the backup server (server name: **BKServer**) respectively.

### *(2) Format of operation definition files*

An operation definition file is created, for each operation ID that uniquely identifies the processing target, with a name in the following format:

***Protection Services-installation-directory*\script\conf_*operation-ID*.dat**

Table 3.8 shows the entries of an operation definition file, the contents of them, and the maximum value length (in bytes). Specifying the entries is always required.

**Table 3.8 Contents of Entries in an Operation Definition File (Windows) (continues on the next page)**

| Specification Item | Information to be Specified | Max. No. of Characters |
|---|---|---|
| BACKUP_OBJECT | Specify a character string identifying the type of the backup object.<br>For Copy Controller, specify **FILESYSTEM**.<br>For SQL Server, specify **MSSQL**.<br>For Exchange Server, specify **MSEXCHANGE**. | 32 |
| DB_SERVER_NAME | Specify the file/database server name. If the mount point (or file), instance, or storage group to be backed up is in a cluster configuration, specify the virtual server name. *2<br>This value must match the database server name specified in the **DRM_DB_PATH=*folder-on-the-shared-disk*;*virtual-server-name*** entry in the Protection Services environment settings file **init.conf**. | 128<br>63 for Exchange Server |
| INSTANCE_NAME | For Copy Controller: Specify the mount point directory name or mount point directory list file name.<br>For SQL Server: Specify an SQL Server instance name. When DEFAULT is specified, the SQL Server default instance name is used.<br>For Exchange Server: Specify hyphen (-).<br>If a space character is included, enclose the entry in the double-quotation **"**. | 128<br>1 for Exchange Server |
| TARGET_NAME | For Copy Controller: Specify the file name or the directory name you want to back up. This entry is valid only when backup is performed, and cannot be used when restoration is performed. If you omit this value, backup is executed for each mount point.<br>For SQL Server: Specify the names of databases you want to back up. This entry is valid only when backup is performed, and cannot be used when restoration is performed. If you omit this value, a backup is performed for each instance.<br>For Exchange Server: Specify the storage group name you want to back up. *3<br>If you omit this value, all storage groups in the server are targeted for backup.<br>If you specify more than one name, use a comma (,) to separate each name. If a space character is included, enclose the entry in the double-quotation **"**. | 1,024<br>259 for Exchange Server |
| AP_FILE_DIR *1 | For SQL Server: Specify the VDI metafile storage directory. This value must match the VDI metafile storage directory name that was registered by using the **drmsqlinit** command. | 128 |

**Table 3.8 Contents of Entries in an Operation Definition File (Windows) (continued)**

| Specification Item | Information to be Specified | Max. No. of Characters |
|---|---|---|
| DB_DATA_FILE_DIR *1 | Specify a temporary directory/folder for the extended commands, which should be created under the installation folder for the extended commands, on the file/database server. *4<br>This directory is used when the extended commands generate a temporary file. Specify a directory that actually exists, even when only one server is used. *4<br>If this folder is modified from ***Protection Services-installation-directory*\script\tmp**, specify this folder in the **SCR_TMP_DIR** value of the log collection tool (**drm_log.bat**). | 128 |
| BK_DATA_FILE_DIR *1 | Specify a temporary directory for extended commands on the backup server. *4<br>If you do not intend to use a backup server, specify a hyphen (**-**). | 128 |
| SET_DRM_HOSTNAME | For Copy Controller: Specify **0**.<br>For SQL Server, Exchange Server: Specify a database server configuration. When the database server has a cluster configuration, specify **1**. When the database server does not have a cluster configuration, specify **0**. | 1 |

***Notes:***

1. Do not specify the value in the AP_FILE_DIR entry in the DB_DATA_FILE_DIR entry or the BK_DATA_FILE_DIR entry.
2. For Exchange Server: You can also specify the virtual server name in the -hostname option of the extended command EX_DRM_EXG_BACKUP. If you specify the virtual server name in both DB_SERVER_NAME in the operation definition file and in the -hostname option, the value specified in the -hostname option has priority.
3. This specification is effective only if the target Exchange Server is an Exchange 2000 Enterprise Server or an Exchange 2003 Enterprise Edition server. If the target Exchange Server is not an Exchange 2000 Enterprise Server or an Exchange 2003 Enterprise Edition server, any items you specify are ineffective. If the server is an Exchange 2003 Enterprise Edition, do not specify the storage group for recovery.
4. Specify the folder name as an absolute path that includes the drive character. Do not include relative path expressions or shared name expressions in the folder name. When you specify a folder other than the root folder, do not suffix a slash (\) to the name. File names are not case sensitive.

### *(3) Creating an operation definition file in a cluster configuration (Copy Controller)*

The following gives an example of creating operation definition files for a system that has a cluster configuration when the file server is in a cluster configuration. This example assumes following conditions:

- A virtual server **VServer_C** is running on file server A (server name: **FSServer_A**) and file server B (server name: **FSServer_B**), which make up the cluster.
- The FTP service has been set on the backup server (server name: **BKServer**) and is running. The home directory of the FTP site is **C:\FTP_ROOT**.
- File server A is specified as an active server, and file server B is specified as a standby server. The shared disk **G:** is used.
- The three mount points **D:**, **M:**, and **N:** exist on file server A and file server B. The virtual server C (server name: **VServer_C**) has been defined as a cluster resource.
- The cluster resource in Table 3.9 has been registered in a cluster group **FSCG_1**.
- The mount points **M:** and **N:** have been set in the mount point directory target definition file **app.txt** so that the mount point directories are operated at one time.
- The storage directory for extended command temporary files is created on file server A, file server B, and the backup server (server name: **BKServer**)(see Table 3.10).

This example creates operation definition files corresponding to the operation IDs listed in Table 3.11.

**Table 3.9 Cluster Resources (Copy Controller)**

| Cluster Group Name | Virtual Server | Mount Point | Storage Drive Name for Extended Command Temporary Files |
|---|---|---|---|
| FSCG_1 | VServer_C | D: | G:\drm_FS_tmp\Operation_A |
| FSCG_1 | VServer_C | M:,N: | G:\drm_FS_tmp\Operation_B |

**Table 3.10 Storage Directories for Extended Command Temporary Files (Windows)**

| Server Name | Storage Directories for Extended Command Temporary Files (Cluster Configuration) |
|---|---|
| FSServer_A<br>FSServer_B | G:\drm_FS_tmp\Operation_A<br>G:\drm_FS_tmp\Operation_B |
| BKServer | C:\FTP_ROOT\Operation_A<br>C:\FTP_ROOT\Operation_B |

**Table 3.11 Operation IDs for which an Operation Definition File is Created (Windows)**

| Operation ID | Target file Server Name | Target Mount Point or File |
|---|---|---|
| Operation_A | VServer_C | Entire **D:** |
| Operation_B | VServer_C | Mount point directories specified in **app.txt** (**M:** and **N:**) |

To create an operation definition file for a cluster configuration (Copy Controller):

1. Create an operation definition file on the active server (file server A), and set the required items. Create the following two files.

   ***installation-destination-for-extended-commands*\conf_Operation_A.dat**
   ***installation-destination-for-extended-commands*\conf_Operation_B.dat**

   The value ***installation-destination-for-extended-commands*** indicates ***Protection Services-installation-destination*\script**.

   The following shows an example of writing the file ***installation-destination-for-extended-commands*\conf_Operation_A.dat**.

```
BACKUP_OBJECT=FILESYSTEM
DB_SERVER_NAME=VServer_C
INSTANCE_NAME=D:
TARGET_NAME=
DB_DATA_FILE_DIR=G:\drm_FS_tmp\Operation_A
BK_DATA_FILE_DIR=C:\FTP_ROOT\Operation_A
SET_DRM_HOSTNAME=1
```

   The following shows an example of writing the file ***installation-destination-for-extended-commands*\conf_Operation_B.dat**.

```
BACKUP_OBJECT=FILESYSTEM
DB_SERVER_NAME=VServer_C
INSTANCE_NAME=app.txt
TARGET_NAME=
DB_DATA_FILE_DIR=G:\drm_FS_tmp\Operation_B
BK_DATA_FILE_DIR=C:\FTP_ROOT\Operation_B
SET_DRM_HOSTNAME=0
```

2. On the active server (file server A), execute the check tool **EX_DRM_FS_DEF_CHECK** for operation definition files.

   **"EX_DRM_FS_DEF_CHECK" "operation-ID" -db**

   If an error occurs, correct the contents of the file and execute the check tool again.

3. Copy the operation definition files created on the active server (file server A) to the backup server. The copy destination is:

   ***installation-destination-for-extended-commands*\conf**

4. On the backup server, execute the check tool **EX_DRM_FS_DEF_CHECK** for operation definition files.

   **"EX_DRM_FS_DEF_CHECK" "operation-ID" -bk**

   If the error occurs, change the backup server configuration depending on the contents of the operation definition file, or change the contents of the operation definition file depending on the backup server configuration. When you change the backup server configuration, re-execute the checking tool. When you change the contents of the operation definition file, place the same file on the file server, and then re-execute the checking tool.

5. Copy the operation definition files created on the active server (file server A) to the standby server (file server B). The copy destination is:

   ***installation-destination-for-extended-commands*\conf**

### *(4) Creating an operation definition file in a cluster configuration (SQL Server)*

The following gives an example of creating an operation definition file for a system that has a cluster configuration. This example assumes following conditions:

- The virtual server (server name: **VServer_C**) is running on database server A (server name: **DBServer_A**) and database server B (server name: **DBServer_B**), which are making up the cluster.
- The SQL Server instance **INSTANCE_1** exists on database A and database B, and the virtual server C (server name: **VServer_C**) has been defined as a cluster resource.
- There is a cluster group **SQLCG_1** on database server A and database server B, and the cluster resource shown in Table 3.12 has been registered.
- The FTP service is set up and activated on the backup server (**BKServer**). The home directory of the FTP site is **C:\FTP_ROOT**.
- The database server A is specified as an active server and the database server B is specified as a standby server. The shared disk **G:** is used.
- The drmsqlinit command is executed for the **INSTANCE_1**.
- The value has been set in the **DRM_DB_PATH=*folder-on-the-shared-disk*;*virtual-server-name*** entry in the Protection Services environment settings file **init.conf**.
- The extended command temporary file storage directory and VDI metafile storage directory have been created on database server A, database server B, and the backup server (see Table 3.13). In this example, you create an operation definition file for the operation ID listed in Table 3.14.

**Table 3.12 Cluster Resource Example (SQL Server)**

| Cluster Group Name | Virtual Server | SQL Server Instance Name | Extended Command Temp. File Storage Folder |
|---|---|---|---|
| SQLCG_1 | VServer_C | INSTANCE_1 | G:\tmp\INSTANCE_1 |

**Table 3.13 Example: Storage Directories for Extended Command Temporary Files and VDI Metafiles**

| Server Name | Extended Command Temporary File Installation Folder | VDI Metafile Storage Directory |
|---|---|---|
| DBServer_A<br>DBServer_B | G:\tmp\INSTANCE_1 | G:\MSSQL\VServer_C\INSTANCE_1\META |
| BKServer | C:\FTP_ROOT\VServer_C\INSTANCE_1 | G:\MSSQL\VServer_C\INSTANCE_1\META |

**Table 3.14 Operation ID for which to Create an Operation Definition File (SQL Server)**

| Operation ID | Target Database Server | Target Instance and Database |
|---|---|---|
| Operation_A | VServer_C | Entire INSTANCE_1 |

To create an operation definition file for a cluster configuration (SQL Server):

1. Create an operation definition file on the active server (database server A), and set the required items. Create the file with the following name:

   ***Protection-Services-directory*\script**

   In the example ***extended-command-installation-directory*** indicates ***extended-command-installation-directory*\conf_Operation_A.dat**

   An example of specifying this file is:

```
BACKUP_OBJECT=MSSQL
DB_SERVER_NAME=VServer_C
INSTANCE_NAME=INSTANCE_1
TARGET_NAME=
AP_FILE_DIR=G:\MSSQL\VServer_C\INSTANCE_1\META
DB_DATA_FILE_DIR=G:\tmp\INSTANCE_1
BK_DATA_FILE_DIR=C:\FTP_ROOT\VServer_C\INSTANCE_1
SET_DRM_HOSTNAME=1
```

2. On the active server (database server A), execute the tool **EX_DRM_SQL_DEF_CHECK** for checking an operation definition file.

   **"EX_DRM_SQL_DEF_CHECK.wsf" -db -f *target-operation-definition-file***

   If the tool detects an error, correct the contents of the file, and execute the check tool again.

3. Copy the operation definition file created on the active server (database server A) to the backup server. The copy destination is:

   ***extended-command-installation-directory*\conf**

4. On the backup server, execute the tool **EX_DRM_SQL_DEF_CHECK** for checking an operation definition file.

   **"EX_DRM_SQL_DEF_CHECK.wsf" -bk -f *target-operation-definition-file***

   If the error occurs, change the backup server configuration depending on the contents of the operation definition file, or change the contents of the operation definition file depending on the backup server configuration. If you change the backup server configuration, re-execute the checking tool. If you change the contents of the operation definition file, place the same file on the database server, and then re-execute the checking tool.

5. Copy the operation definition file created on the active server (database server A) to the standby server (database server B). The copy destination is:
   ***extended-command-installation-directory*\conf**

### *(5) Creating an operation definition file in a cluster configuration (Exchange Server)*

The following gives an example of creating an operation definition file for a system that has a cluster configuration. This example assumes following conditions:

- The Exchange Server used in the system is an Exchange 2000 Enterprise Server.
- On database A (server name: **DBServer_A**) and database B (server name: **DBServer_B**) making up the cluster, the virtual server C (server name: **VServer_C**) is running.
- The storage group **STORAGE_1** exists on database A and database B, and the virtual server C **VServer_C** has been defined as a cluster resource.
- There is a cluster group **EXGCG_1** on database server A and database server B.
- The cluster resource in Table 3.15 has been registered in a cluster group **EXGCG_1**.
- The FTP service has been set up on a backup server (server name: **BKServer**) and has been started. The home directory of the FTP site is set as **C:\FTP_ROOT**.
- Database server A is specified as an active server, and database server B is specified as a standby server. The shared disk **G:** is used.
- The value has been set in the **DRM_DB_PATH=*folder-on-the-shared-disk*;*virtual-server-name*** entry in the Protection Services environment settings file **init.conf**.
- The extended command temporary file installation folder has been created on database server A, database server B, and the backup server (see Table 3.16). In this example, you create an operation definition file for the operation ID listed in Table 3.17.

**Table 3.15 Cluster Resource Example (Exchange Server)**

| Cluster Group Name | Virtual Server | Storage Group Name |
|---|---|---|
| EXGCG _1 | VServer_C | STORAGE_1 |

**Table 3.16 Example: Extended Command Temporary File Storage Directory and VDI Metafile Storage Directory**

| Server Name | Extended Command Temporary File Installation Folder |
|---|---|
| DBServer_A<br>DBServer_B | G:\temp |
| BKServer | C:\FTP_ROOT\VServer_C\- |

**Table 3.17 Operation ID for which to Create an Operation Definition File (Exchange Server)**

| Operation ID | Virtual Server | Target Storage Group |
|---|---|---|
| Operation_A | VServer_C | STORAGE_1 |

To create an operation definition file for a cluster configuration (Exchange Server):

1. Create an operation definition file on the active server (database server A) on which the virtual server **EVS_C** is running and set required items. Create the file with the following name:

   ***extended-command-installation-folder*\conf_Operation_A.dat**

   Note that ***extended-command-installation-folder*** indicates ***Protection-Services-installation-folder*\script**.

   An example of specifying this file is:

   ```
   BACKUP_OBJECT=MSEXCHANGE
   DB_SERVER_NAME=VServer_C
   INSTANCE_NAME=-
   TARGET_NAME=
   DB_DATA_FILE_DIR=G:\temp
   BK_DATA_FILE_DIR=C:\FTP_ROOT\VServer_C\-
   SET_DRM_HOSTNAME=1
   ```

2. On the active server (database server A), execute the check tool **EX_DRM_EXG_DEF_CHECK** for an operation definition file.

   **"EX_DRM_EXG_DEF_CHECK.wsf" -db -f "*target-operation-definition-file*"**

   If an error occurs, correct the contents of the file and execute the check tool again.

3. Copy the operation definition file created on the active server (database A) to the backup server. Copy the file to the following folder.

   ***installation-destination-for-extended-commands*\conf**

4. On the backup server, execute the check tool **EX_DRM_EXG_DEF_CHECK** for an operation definition file.

   **"EX_DRM_EXG_DEF_CHECK.wsf" -bk -f "*target-operation-definition-file*"**

   If the error occurs, change the backup server configuration depending on the contents of the operation definition file, or change the contents of the operation definition file depending on the backup server configuration. When you change the backup server configuration, re-execute the checking tool. When you change the contents of the operation definition file, place the same file on the database server, and then re-execute the checking tool.

5. Copy the operation definition file you created on the active server (database server A) into the standby server (database B). The copy destination is: ***extended-command-installation-folder*\conf**

### 3.3.6 Creating Host Environment Settings Files

Host environment settings files are created depending on the configuration of the system using extended commands. These files must be located on each server.

***(1) Format of host environment settings files***

Two operation definition files need to be created for one instance to be operated. One operation definition file is located on the database server and the other file is located on the backup server.

A host environment settings file is created with a name in the following format:

In UNIX: **/opt/drm/script/conf/host.dat**

In Windows: ***Protection-Services-installation-directory*\script\conf\host.dat**

Table 3.18 shows the entries of a host environment settings file, the values of them, and the maximum value lengths (in bytes).

**Table 3.18 Value of Entries in a Host Environment Settings File**

| Entry Name | Explanation | Max. Length (in bytes) |
|---|---|---|
| HOST_ROLE | Specifies a host type. Specify **DB** for a file/database server and **BK** for a backup server. | 2 |
| MAX_LOG_LINES | Specifies the maximum number of lines that the log file for scripts can contain. Specify an integer (range: from 1,000 to 100,000). | 6 |

***(2) Procedure for creating host environment settings files***

The following explains the procedure for creating a host environment settings file. In this example, the host environment settings file is created on each server (i.e., two file/database servers and one backup server connecting the tape device).

To create a host environment settings file:

1. Create a host environment settings file on the file/database servers A and B, and set the items you need. Create the file with the following name:
   ***extended-command-installation-folder*\conf\host.dat**

   An example of specifying this file is:
   ```
   HOST_ROLE=DB
   MAX_LOG_LINES=5000
   ```

   For database servers: In the example, ***extended-command-installation-directory*** indicates ***Protection-Services-installation-directory*\script**. Create the file with the following name: ***extended-command-installation-directory*\conf\host.dat**

2. On the file/database servers A and B, execute **EX_DRM_HOST_DEF_CHECK**, which is a tool for checking a host environment settings file.

   **"EX_DRM_HOST_DEF_CHECK" -db -f *host-environment-settings-file***
   or
   **"EX_DRM_HOST_DEF_CHECK.wsf" -db -f *host-environment-settings-file***

   If the tool detected an error, correct the contents of the file, and then re-execute the check tool.

3. Create a host environment settings file on the backup server, and set the items you need. Create the file with the following name:
   ***extended-command-installation-folder*\conf\host.dat**

   An example of specifying this file is:
   ```
   HOST_ROLE=BK
   MAX_LOG_LINES=5000
   ```

   For database servers: Create the file with the following name:
   ***extended-command-installation-directory*\conf\host.dat**

4. On the file/database servers A and B, execute **EX_DRM_HOST_DEF_CHECK**, which is a tool for checking a host environment settings file.

   **"EX_DRM_HOST_DEF_CHECK" -bk -f *host-environment-settings-file***
   or
   **"EX_DRM_HOST_DEF_CHECK.wsf" -bk -f *host-environment-settings-file***

### 3.3.7 Checking the FTP Service (for Tape Backups)

If you want to execute extended commands in a system configuration for tape backups, you must specify the settings for transmitting files between servers. With the FTP service starting, make sure that the following operations can be performed between the directory (folder) specified in the **DB_DATA_FILE_DIR** entry of the operation definition file and the directory (folder) specified in the **BK_DATA_FILE_DIR** entry:

- Logon to the FTP server from the database server to the backup server
- File transmission and reception using FTP

In the UNIX environment, when you change the FTP user who uses it at the time of execution of **EX_DRM_FTP_PUT.sh** or **EX_DRM_FTP_GET.sh**, delete the file created by the FTP user before change. The file to delete is a file stored in the directory set up as "**BK_DATA_FILE_DIR**" on a backup server.

## 3.4 Procedures of Extended Commands

The following sections explain the processing flow to be followed when you execute the following types of backup and restore operations using the extended commands.

3.4.1 Backing up a file system or database to a secondary volume

3.4.2 Restoring a file system or database to a primary volume

3.4.3 Backing up a file system or database to a tape (ordinary split operation)

3.4.4 Backing up a file system or database to a tape (ordinary paired operation)

3.4.5 Restoring a file system or database from its backup tape

### 3.4.1 Backing Up a File System or Database to a Secondary Volume

**(1) File system**

Figure 3.9 illustrates the procedure for backing up a file system to a secondary volume in a single-server system. Extended commands are executed on the file server.

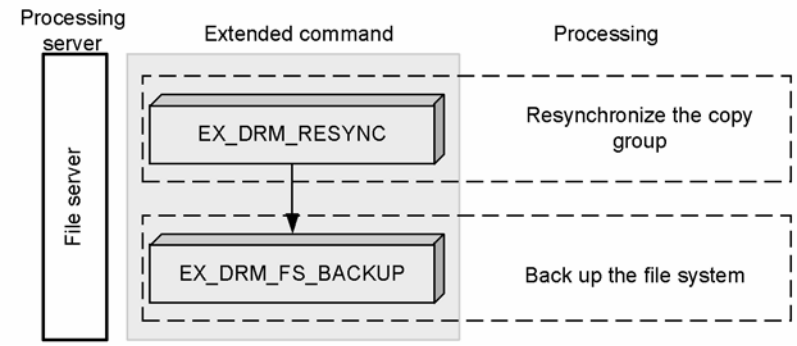



**Figure 3.9 Backing Up a File System to a Secondary Volume**

To back up a file system:

1. Resynchronize the copy groups. To enhance the speed of backup processing, execute **EX_DRM_RESYNC** to resynchronize the copy groups before you back up the file system to the secondary volume.
2. Back up the file system from the primary volume to the secondary volume by executing **EX_DRM_FS_BACKUP**.

### (2) SQL Server or Exchange Server database

Figure 3.10 illustrates the procedure for backing up an SQL Server or Exchange Server database to a secondary volume in a single-server system. Execute extended commands on the database server.

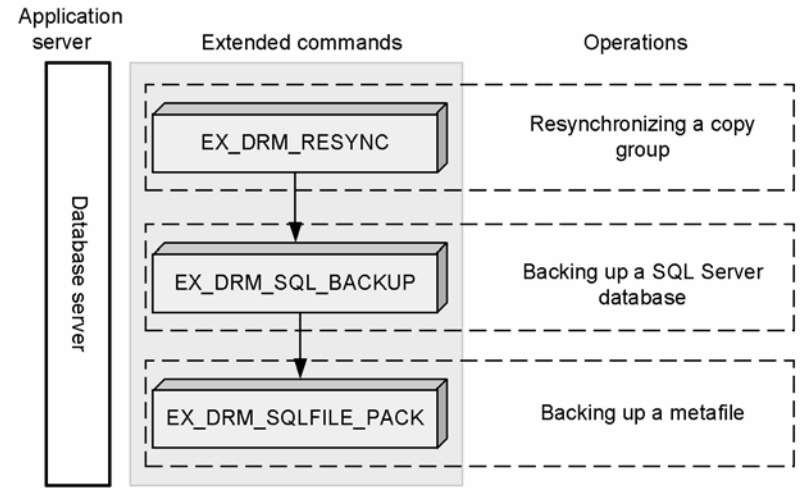



**Figure 3.10 Backing Up a Database to a Secondary Volume**

To back up an SQL Server or Exchange Server database:

1. Resynchronize the copy group. To enhance the speed of backup processing, execute **EX_DRM_RESYNC** to resynchronize the copy group before you back up the database to the secondary volume.
2. Back up the database from the primary volume to the secondary volume:

   For SQL Server, execute the **EX_DRM_SQL_BACKUP** extended command.

   For Exchange Server, execute the **EX_DRM_EXG_BACKUP** extended command.
3. ***SQL Server only:*** Back up the SQL Server metafile and backup ID file by executing the **EX_DRM_SQLFILE_PACK** extended command. This extended command deletes all the old files from the temporary folders for extended commands and backs up the files created by the **EX_DRM_SQL_BACKUP** extended command.

### 3.4.2 Restoring a File System or Database to a Primary Volume

#### (1) File system

Figure 3.11 illustrates the procedure for restoring a backup copy of the file system to the primary volume in a single-server system. Extended commands are executed on the file server.

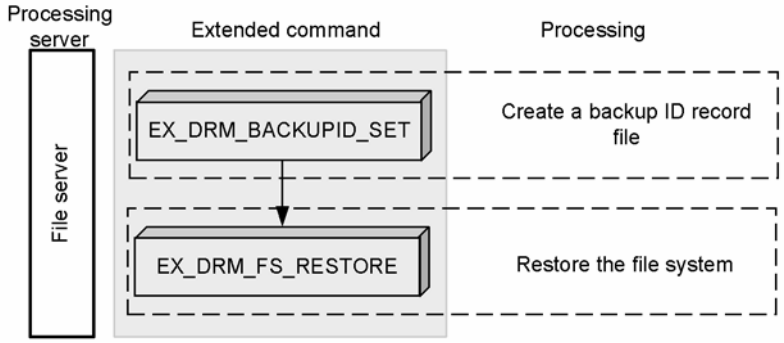



**Figure 3.11 Restoring a File System to a Primary Volume**

Before restoring a file system to a primary volume, you need to identify the backup ID to be used for restore processing. To identify the backup ID to be used for restore processing, execute the **drmfscat** command.

To restore the file system to the primary volume:

1. Create a backup ID record file by executing **EX_DRM_BACKUPID_SET**, specifying the backup ID.
2. Restore the file system to the primary volume by executing **EX_DRM_FS_RESTORE**.

**(2) SQL Server database**

Figure 3.12 illustrates the procedure for restoring an SQL Server database from its backup to the primary volume in a single-server system. Extended commands are executed on the database server.

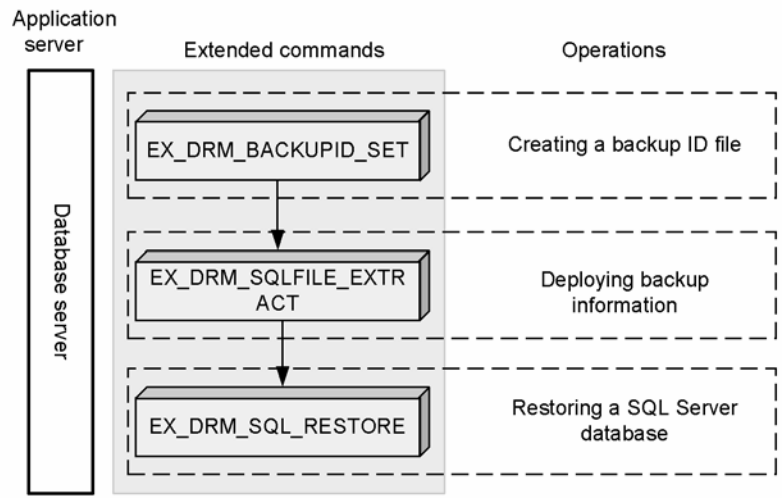



**Figure 3.12 Restoring an SQL Server Database to a Primary Volume**

Before restoring a database to a primary volume, you need to identify the backup ID to be used for restore processing. To identify the backup ID to be used for restoration, execute the **drmsqlcat** command.

To restore the SQL Server database to the primary volume:

1. Create a backup ID record file by executing **EX_DRM_BACKUPID_SET** with the backup ID specified.
2. Execute the **EX_DRM_SQLFILE_EXTRACT** extended command to deploy the backup information from the latest SQL Server metafile.
3. Restore the SQL Server database to the primary volume by executing the **EX_DRM_SQL_RESTORE** extended command.

To recover the database after restoration is complete, execute the **drmsqlrecover** command or the **drmsqlrecovertool** command.

### 3.4.3 Backing Up a File System or Database to Tape (Always-Split Mode)

#### (1) File system (always-split mode)

Figure 3.13 illustrates the procedure for backing up the file system to a tape with a multi-server system operating in the always-split mode. Data is backed up after the copy group is resynchronized. Extended commands are executed on the file server and backup server.

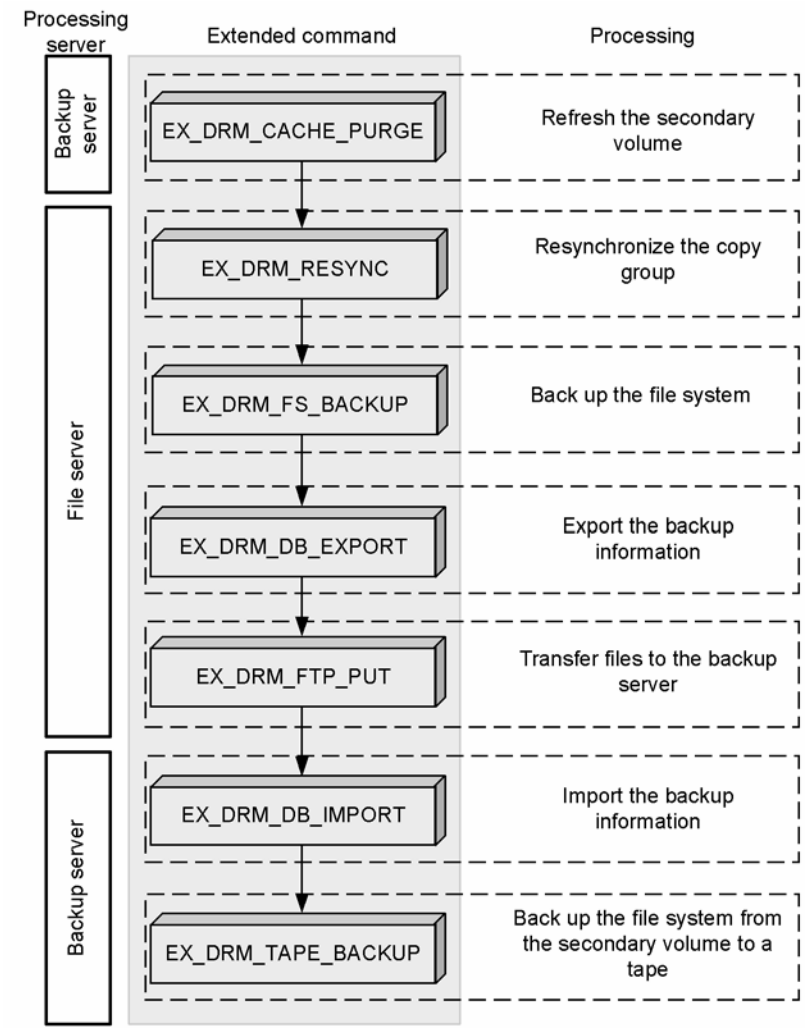



**Figure 3.13 Backing Up a File System to Tape (Always-Split Mode)**

To back up a file system to tape:

1. For Windows only, execute **EX_DRM_CACHE_PURGE** on the backup server to mount and then unmount the secondary volume and clear its cache. In UNIX, this operation is not required.
2. Resynchronize the copy groups by executing **EX_DRM_RESYNC** on the database server. Resynchronizing the copy groups before you back up the file system to the secondary volume enhances the speed of backup processing.
3. Back up the file system from the primary volume to the secondary volume by executing **EX_DRM_FS_BACKUP**.
4. Execute **EX_DRM_DB_EXPORT** to export the backup information generated by **EX_DRM_FS_BACKUP** to a temporary file.
5. Execute **EX_DRM_FTP_PUT** on the database server to transfer all backup record files to the backup server.
6. Execute **EX_DRM_DB_IMPORT** on the backup server to import the backup record file that was transferred from the database server, to the backup catalog on the backup server.
7. Execute **EX_DRM_TAPE_BACKUP** to back up the data of the secondary volume and the temporary file to a tape.

**(2) SQL Server database or Exchange Server database (cold backup) (always-split mode)**

Figure 3.14 illustrates the procedure for backing up a database to a tape with a multi-server system operating in always-split mode. Resynchronize the copy groups, and then back up the data. Execute extended commands on the database server and backup server.

***Note:*** This procedure performs a cold backup of an Exchange Server database. The procedure for performing an online backup of an Exchange Server database is given below.

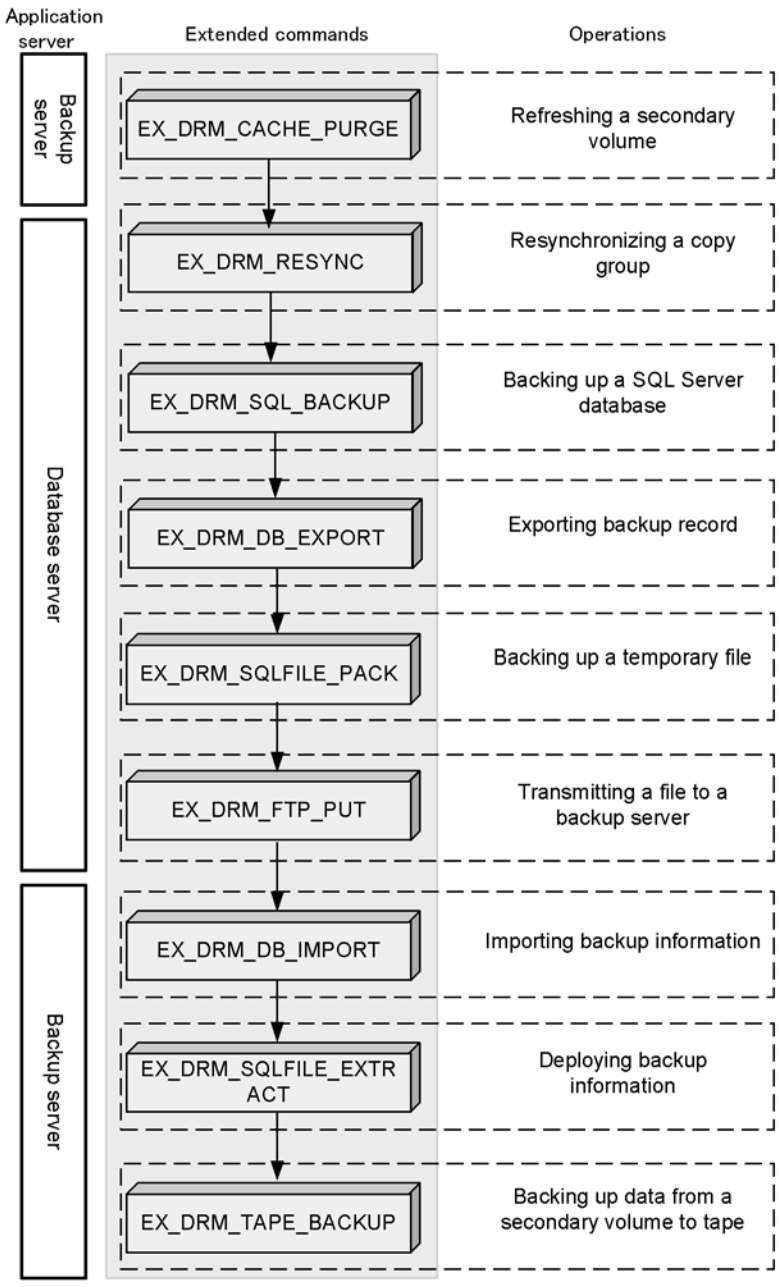



**Figure 3.14 Backing Up a Database to Tape (Always-Split Mode) (SQL Server shown)**

To back up an SQL Server or Exchange Server database (cold backup) to tape:

1. Execute **EX_DRM_CACHE_PURGE** on the backup server to mount and then unmount the secondary volume and clear its cache.
2. On the database server, execute the **EX_DRM_RESYNC** extended command to resynchronize the copy group. Resynchronizing the copy groups before you back up the database to the secondary volume enhances the speed of backup processing.
3. Back up the database from the primary volume to the secondary volume:

   For SQL Server, execute the **EX_DRM_SQL_BACKUP** extended command.

   For Exchange Server, execute the **EX_DRM_EXG_BACKUP** extended command.
4. Execute the **EX_DRM_DB_EXPORT** extended command to export the backup information generated by **EX_DRM_SQL_BACKUP** or **EX_DRM_EXG_BACKUP** to a temporary file.
5. ***SQL Server only:*** Execute the **EX_DRM_SQLFILE_PACK** extended command to back up the SQL Server metafile and backup ID file. This extended command deletes all the old files from the temporary folders for extended commands and backs up the files created by the **EX_DRM_SQL_BACKUP** extended command.
6. Execute the **EX_DRM_FTP_PUT** extended command to transfer all backup information files and all SQL Server metafiles to the backup server.
7. On the backup server, execute the **EX_DRM_DB_IMPORT** extended command to import the backup information file that was transferred from the database server to the backup catalog on the backup server.
8. ***SQL Server only:*** Execute the **EX_DRM_SQLFILE_EXTRACT** extended command to deploy the backup information from the latest SQL Server metafile.
9. Execute the **EX_DRM_TAPE_BACKUP** extended command to back up the data of the secondary volume and the temporary file to a tape.

**(3) Online backup of the Exchange Server database (always-split mode)**

In performing online backup of the Exchange database, you should verify the consistency of the Exchange database before backing up onto tape the data that was backed up to the secondary volume. Figure 3.15 shows the processing flow for online backup of the Exchange database.

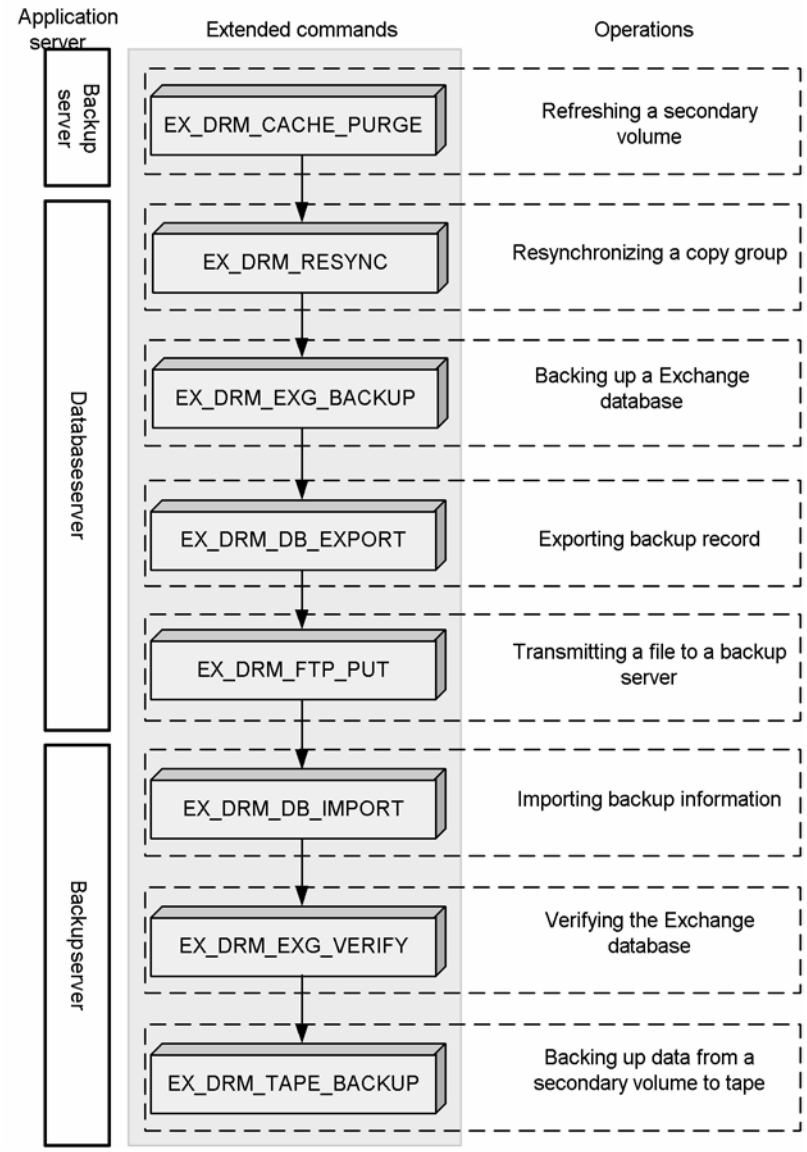



**Figure 3.15 Performing Online Backup of an Exchange DB to Tape (Always-Split Mode)**

To do online backup of the Exchange Server database onto tape (always-split mode):

1. Execute **EX_DRM_CACHE_PURGE** on the backup server, mount/dismount the secondary volume, and clear the cache.
2. Resynchronize the copy group by executing **EX_DRM_RESYNC** on the database server. You can accelerate the backup process by resynchronizing the copy group before backing up the Exchange database onto the secondary volume.
3. Back up the Exchange database from the primary volume to the secondary volume by executing **EX_DRM_EXG_BACKUP**.
4. Export the backup information generated by the **EX_DRM_EXG_BACKUP** command to a temporary file executing **EX_DRM_EXG_EXPORT**.
5. Transfer all backup information files to the backup server by executing **EX_DRM_FTP_PUT** on the database server.
6. Execute **EX_DRM_DB_IMPORT** on the backup server to import the backup information files transferred from the database server to the backup catalog for the backup server.
7. Verify the consistency of the Exchange database backed by the **EX_DRM_EXG_BACKUP** command by executing **EX_DRM_EXG_VERIFY**.
8. Execute **EX_DRM_TAPE_BACKUP** to back up onto tape the data and temporary files on the secondary volume.

### 3.4.4 Backing Up a File System or Database to Tape (Always-Paired Mode)

#### (1) File system (always-paired mode)

Figure 3.16 illustrates the procedure for backing up a file system to tape with a multi-server system operating in the always-paired mode. Extended commands are executed on the file server and backup server. In the always-paired mode, you do not need to resynchronize the copy group before the backup. In this example, the copy group is resynchronized and initialized after the tape backup completes.

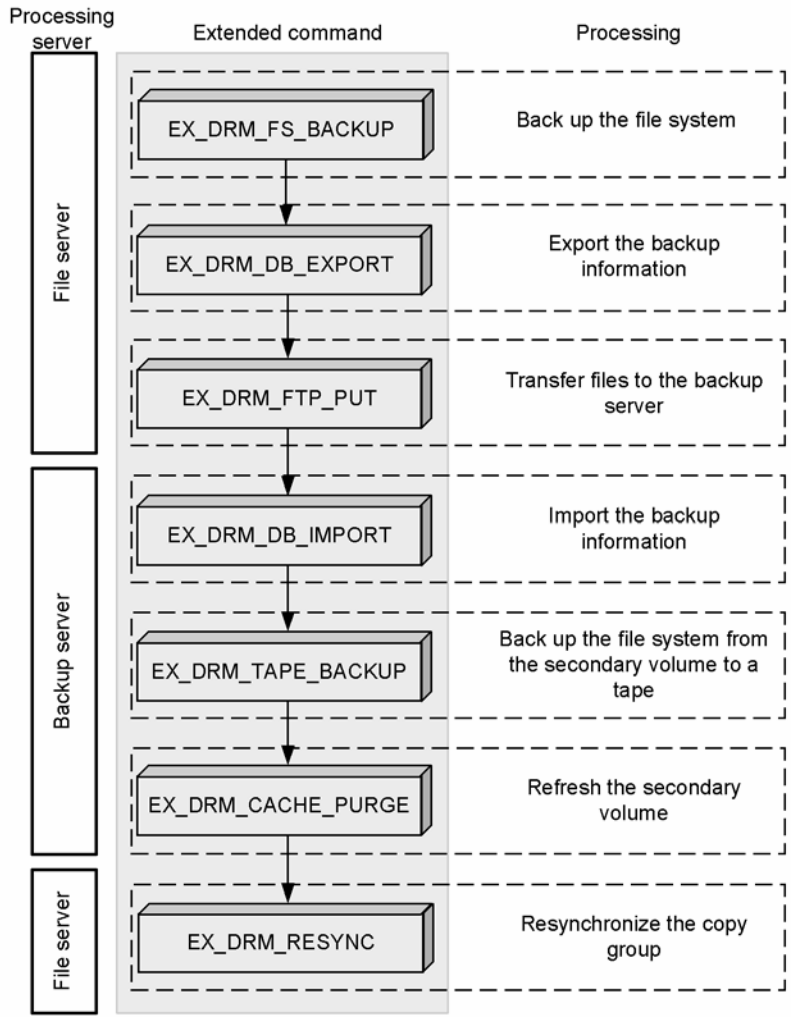



**Figure 3.16 Backing Up a File System to Tape (Always-Paired Mode)**

To back up a file system to a tape:

1. Back up a file system to the secondary volume by executing **EX_DRM_FS_BACKUP** on the database server. A backup ID record file that records the backup ID is generated.
2. Execute **EX_DRM_DB_EXPORT** to export the backup information generated by **EX_DRM_FS_BACKUP** to a temporary file.
3. Execute **EX_DRM_FTP_PUT** on the database server to transfer all backup record files to the backup server.
4. Execute **EX_DRM_DB_IMPORT** on the backup server to import the backup record file that was transferred from the database server, to the backup catalog on the backup server.
5. Execute **EX_DRM_TAPE_BACKUP** to back up the data of the secondary volume and the temporary file to a tape.
6. Clear the cache of the secondary volume (for Windows). In Windows, execute **EX_DRM_CACHE_PURGE** to mount and then unmount the secondary volume and clear its cache. In UNIX, this operation is not required.
7. Resynchronize the copy groups by executing **EX_DRM_RESYNC** on the database server.

**(2) SQL Server or Exchange Server database (cold backup) (always-paired mode)**

Figure 3.17 illustrates the procedure for backing up an SQL Server or Exchange Server database to tape with a multi-server system operating in the always-paired mode. Extended commands are executed on the database server and backup server. In the always-paired mode, you do not need to resynchronize the copy group before the backup. In this example, the copy group is resynchronized and initialized after the tape backup completes.

***Note:*** This procedure performs a cold backup of an Exchange Server database. The procedure for performing an online backup of an Exchange Server database is given below.

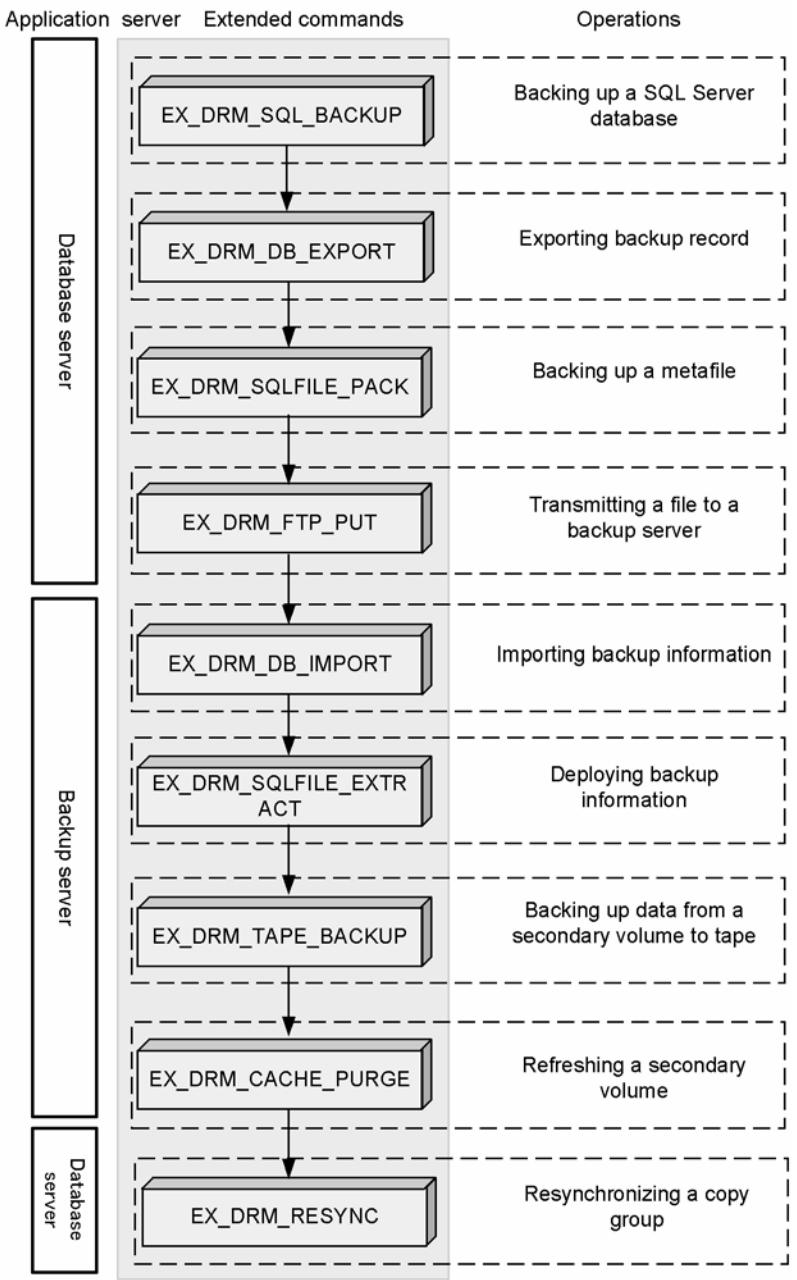



**Figure 3.17 Backing Up a Database to Tape (Always-Paired Mode) (SQL Server shown)**

To back up an SQL Server or Exchange Server database (cold backup) to tape:

1. On the database server, execute the following command to back up the database to the secondary volume:

   For SQL Server, execute the **EX_DRM_SQL_BACKUP** extended command. The backup ID file, in which the backup ID is recorded, and SQL Server metafile are generated.

   For Exchange Server, execute the **EX_DRM_EXG_BACKUP** extended command.

2. Execute the **EX_DRM_DB_EXPORT** extended command to export the backup information generated by **EX_DRM_SQL_BACKUP** or **EX_DRM_EXG_BACKUP** to a temporary file.

3. ***SQL Server only:*** Execute the **EX_DRM_SQLFILE_PACK** extended command to back up the SQL Server metafile and backup ID file. This extended command deletes all the old files from the temporary folders for extended commands and backs up the files created by the **EX_DRM_SQL_BACKUP** extended command.

4. Execute **EX_DRM_FTP_PUT** on the database server to transfer all backup information files to the backup server.

5. Execute **EX_DRM_DB_IMPORT** on the backup server to import the backup information file that was transferred from the database server, to the backup catalog on the backup server.

6. ***SQL Server only:*** Execute the **EX_DRM_SQLFILE_EXTRACT** extended command to deploy the backup information from the latest SQL Server metafile transmitted from the database server.

7. Execute the **EX_DRM_TAPE_BACKUP** extended command to back up the data and temporary files of the secondary volume to a tape.

8. Clear the cache of the secondary volume. On the backup server, execute the **EX_DRM_CACHE_PURGE** extended command to mount and then unmount the secondary volume and clear its cache.

9. Resynchronize the copy group. On the database server, execute the **EX_DRM_RESYNC** extended command to resynchronize the copy group.

**(3) Online backup of the Exchange Server database (always-paired mode)**

In performing online backup of the Exchange database, you should verify the consistency of the Exchange database before backing up onto tape the data that was backed up to the secondary volume. Figure 3.15 shows the processing flow for online backup of the Exchange database.

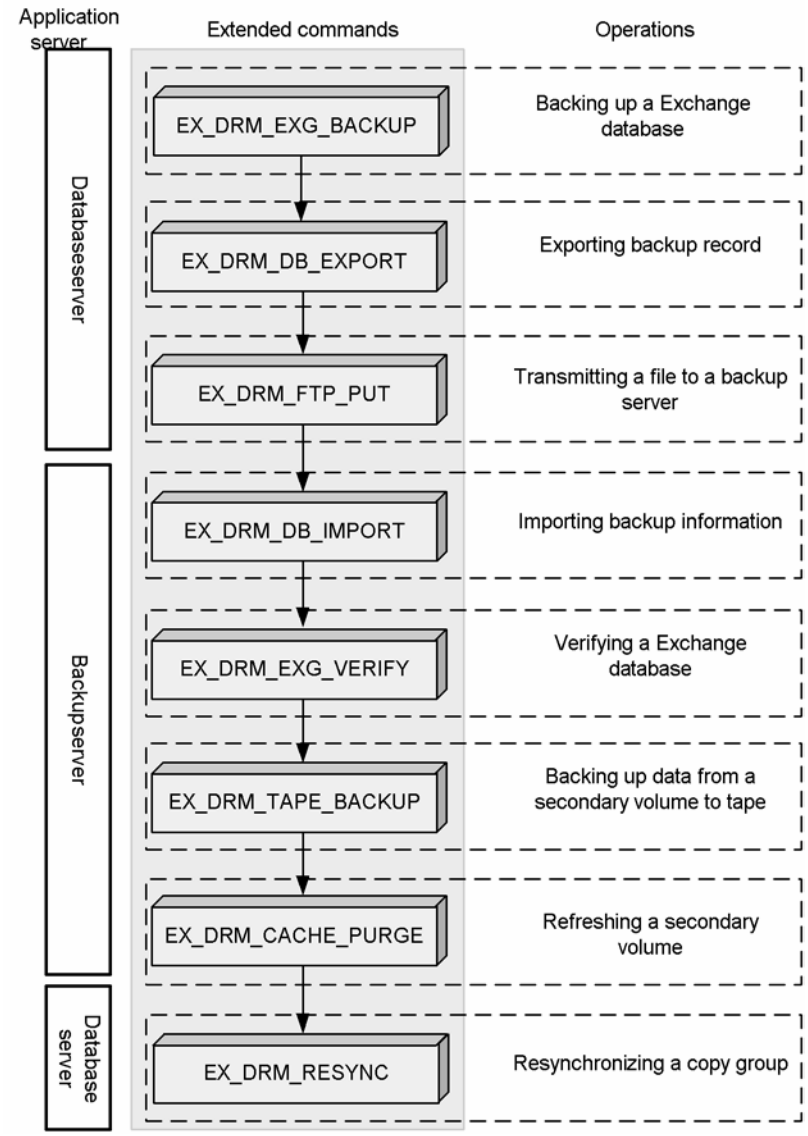



**Figure 3.18 Performing Online Backup of an Exchange DB to Tape (Always-Paired Mode)**

To do online backup of the Exchange Server database onto tape (always-paired mode):

1. Execute **EX_DRM_EXG_BACKUP** on the database server to back up the Exchange database onto the secondary volume. A backup ID record file that records the backup ID is generated.
2. Execute **EX_DRM_DB_EXPORT** to export the backup information generated by **EX_DRM_EXG_BACKUP** to a temporary file.
3. Execute **EX_DRM_FTP_PUT** on the database server to transfer all backup information files to a backup server.
4. Execute **EX_DRM_DB_IMPORT** on the backup server to import the backup information files transferred from the database server to the backup catalog for the backup server.
5. Execute **EX_DRM_EXG_VERIFY** to verify the consistency of the Exchange database backed by the **EX_DRM_EXG_BACKUP** command.
6. Execute **EX_DRM_TAPE_BACKUP** to back up onto tape the data and temporary files on the secondary volume.
7. Clear the cache of the secondary volume. Execute **EX_DRM_CACHE_PURGE**, mount the secondary volume, unmount the secondary volume, and clear the cache.
8. Execute **EX_DRM_RESYNC** on the database server to resynchronize the copy group.

### 3.4.5 Restoring a File System or Database from Tape

#### (1) File system

Figure 3.19 illustrates the procedure for restoring a file system from a tape in a multi-server system. Extended commands are executed on the file server and backup server.

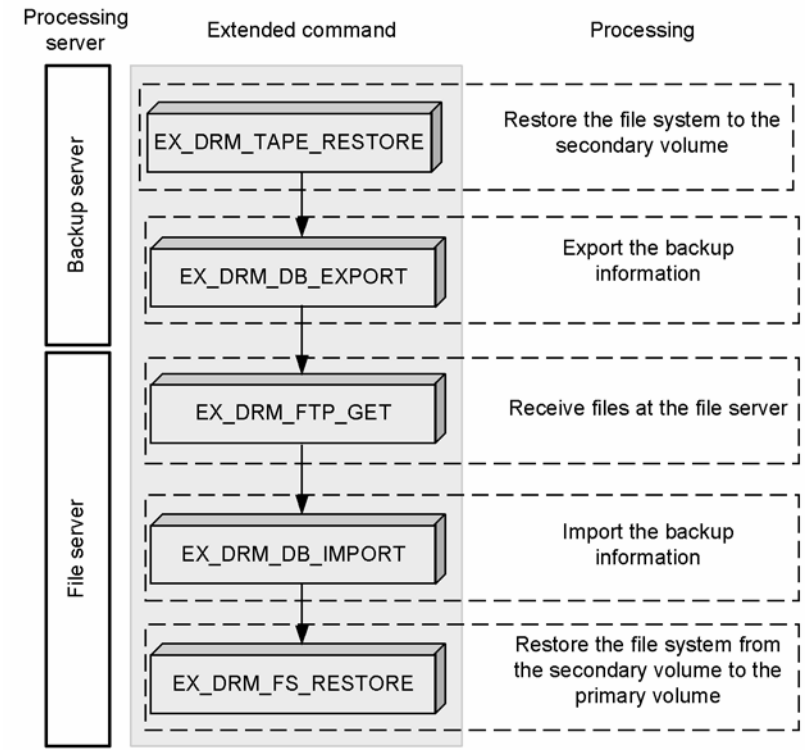



**Figure 3.19 Restoring a File System from Tape**

Before you restore a file system from a tape, you must identify the backup ID to be used for restore. To identify the backup ID to be used for restore, execute the **drmtapecat** command on the backup server.

To restore a file system from tape:

1. Execute **EX_DRM_TAPE_RESTORE** on the backup server to restore the file system that was backed up to a tape to the secondary volume.
2. Execute **EX_DRM_DB_EXPORT** on the backup server to export the backup information generated by **EX_DRM_TAPE_RESTORE** to a temporary file.
3. Execute **EX_DRM_FTP_GET** on the database server to receive all backup record files held on the backup server onto the database server. At this time, all old files on the database server are deleted.
4. Execute **EX_DRM_DB_IMPORT** to import the backup record file that was transferred from the backup server to the backup catalog on the database server.
5. Restore the file system from the secondary volume to the primary volume. Execute the **drmfsrestore** command to restore the file system to the primary volume.

### (2) SQL Server or Exchange Server database

Figure 3.20 illustrates the procedure for restoring an SQL Server or Exchange Server database from tape in a system consisting of a multi-server configuration. Execute extended commands on the database server and backup server.

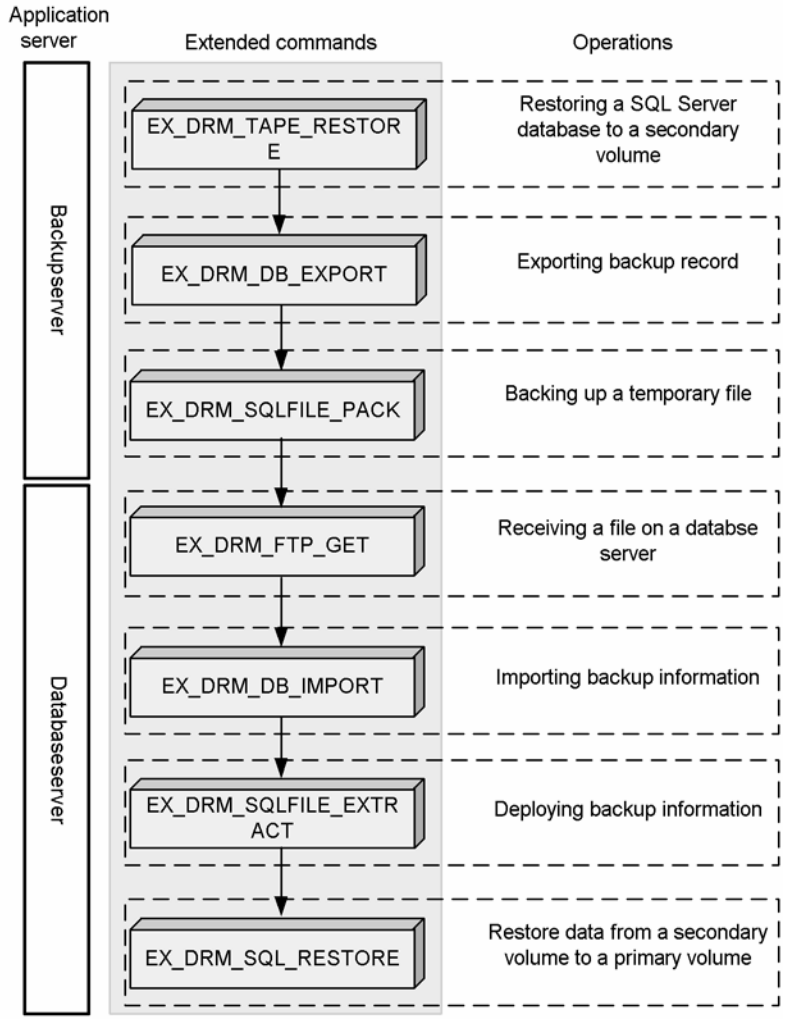



**Figure 3.20 Restoring a Database from Tape (SQL Server shown)**

Before you restore a database from tape, you must identify the backup ID to be used for restore. To identify the backup ID to be used for restore, execute the **drmtapecat** command on the backup server.

To restore an SQL Server or Exchange Server database from tape:

1. On the backup server, execute the **EX_DRM_TAPE_RESTORE** extended command to restore the database from tape to the secondary volume.
2. Execute **EX_DRM_DB_EXPORT** on the backup server to export the backup information generated by **EX_DRM_TAPE_RESTORE** to a temporary file.
3. ***SQL Server only:*** Execute the **EX_DRM_SQLFILE_PACK** extended command to back up the SQL Server metafile and backup ID file. This extended command deletes all the old files from the temporary folders for extended commands and backs up the files created by the **EX_DRM_SQL_BACKUP** extended command.
4. Execute EX_DRM_FTP_GET on the database server to receive all backup information files and SQL Server metafiles held on the backup server onto the database server. All old files on the database server are deleted.
5. Import the backup record from the file. Execute the **EX_DRM_DB_IMPORT** extended command to import the backup information file that was transferred from the backup server, to the backup catalog on the database server.
6. ***For SQL Server:*** Execute the **EX_DRM_SQLFILE_EXTRACT** extended command to deploy the backup information from the latest SQL Server metafile transferred from the backup server.

   ***For Exchange Server:*** Determine the backup ID used during the restore operation. Execute the **drmexgcat** command to determine the backup ID used to restore the Exchange database from the secondary volume to the primary volume.
7. ***For SQL Server:*** To restore the database from the secondary volume to the primary volume, execute the **EX_DRM_SQL_RESTORE** extended command. To perform recovery on the database after restoration, execute the **drmsqlrecover** command on the database server.

   ***For Exchange Server:*** To restore the database that was online backed up from the secondary volume to the primary volume, execute the **drmexgrestore** command with the **-recovery** option specified.

## 3.5 Examples of Using Extended Commands (Copy Controller in UNIX)

This section uses examples to illustrate how to use extended commands. The examples in this section assume the system configuration shown in Figure 3.21.

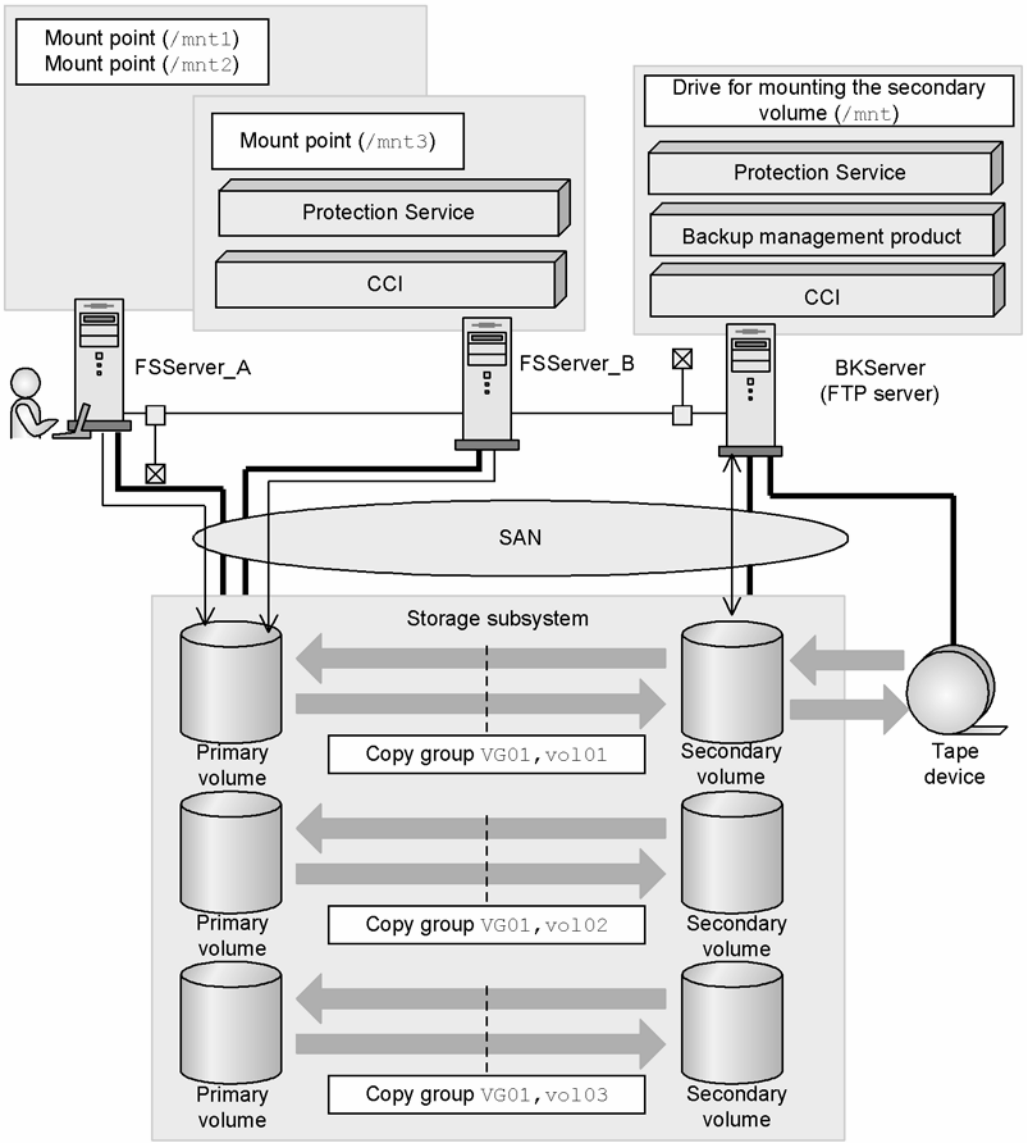



**Figure 3.21 System Configuration: Back Up and Restore a File System to Tape (UNIX)**

The examples in this section assume the following conditions:

- Command path **/opt/drm/script/bin** has been set in the PATH environment variable.
- There are two file servers (server names: **FSServer_A** and **FSServer_B**) and a backup server to which a tape device is connected (server name: **BKServer**).
- The primary volume and secondary volume are mirrored.
- The backup management product is installed on the backup server.
- The parameters of the backup management product have been registered by using the **drmtapeinit** command.
- The primary volume paired with the secondary volume to be backed up is not backed up until the backup of the secondary volume to tape is completed.
- **FSServer_A** has mount points **/mnt1** and **/mnt2**, while **FSServer_B** has mount point **/mnt3**.
- The mount point to be backed up is linked to the disk partition that has been mounted by VxFS.
- The mount point to be backed up is run in always-split mode.
- The secondary volume is not always mounted; it is mounted in the **/mnt** directory only during operation.
- At each file server and the backup server, the storage directories for extended command temporary files specified in the operation definition file have been created.

### 3.5.1 Example of Backing Up File Systems

This section gives an example of cold backup of file system to a tape. This example performs online backup of the mount point directory /mnt of the database server **DBServer_A** to the secondary volume and then backs up these groups from the secondary volume to a tape. It uses **Operation_A** as the operation ID that identifies the file system to be backed up. Note that you cannot perform any new backup until the backup data has been backed up to tape.

To back up file system:

1. Execute **EX_DRM_RESYNC** on the database server to resynchronize the copy groups. Resynchronizing the copy groups before you perform backup enhances the speed of backup processing. In this example, the copy group name is **VG01,vol01**.

   **DBServer_A > EX_DRM_RESYNC Operation_A -cg VG01,vol01 -copy_size 7**

2. Perform cold backup of file system to the secondary volume. To perform backup, execute **EX_DRM_FS_BACKUP**. Specify the operation ID **Operation_A** as the argument.

   **DBServer_A > EX_DRM_FS_BACKUP Operation_A**

3. Export the backup record to a temporary file. To back up data from the secondary volume to a tape, you must copy information about backup that was performed from the primary volume to the secondary volume. Copy this information to the backup server. Execute **EX_DRM_DB_EXPORT** to export information about backup to a temporary file. Temporary files are stored in a temporary directory for extended commands on the database server.

   **DBServer_A > EX_DRM_DB_EXPORT Operation_A**

4. Batch-transfer the temporary files from the database server to the backup server. To transfer the files, execute **EX_DRM_FTP_PUT** on the database server. In this example, the user ID used for logon to the FTP server is **admin** and the password is **password**. Temporary files are stored in a temporary directory for extended commands on the backup server.

   **DBServer_A > EX_DRM_FTP_PUT Operation_A -server BKServer**

5. Import the temporary files that were transferred from the database server, to the backup catalog on the backup server. To import the files, execute **EX_DRM_DB_IMPORT** on the backup server.

   **BKServer > EX_DRM_DB_IMPORT Operation_A**

6. Back up the data of the secondary volume to a tape. To back up the data, execute **EX_DRM_TAPE_BACKUP** on the backup server. In this example, the drive containing the secondary volume is **/mnt**.

   **BKServer > EX_DRM_TAPE_BACKUP Operation_A -exopt -mount_pt /mnt**

   When you execute backup, information about this backup is registered in the backup catalog with the new backup ID **0000000002**.

### 3.5.2 Example of Restoring a File System

This section gives an example of restoring data that was backed up to a tape and recovering file system. This example restores the data from the tape to the secondary volume, then resynchronizes the secondary volume to the primary volume, and restores the data. This example uses **Operation_A** as the operation ID that identifies the file system to be restored.

To restore file system:

1. Check the ID of the backup data to be used for restore. To check the ID, execute the **drmtapecat** command on the backup server.

```
BKServer >drmtapecat -hostname BKServer_A -l
BACKUP-ID ORIGINAL-ID HOSTNAME BACKUP-OBJECT INSTANCE SNAPSHOT TIME     EXPIRATION
TIME   BACKUP-MEDIA
0000000002 0000000001 BKServer_A FILESYSTEM  /mnt1   2003/08/01 19:42:15
2003/08/11 20:32:20  -
:
:
```

2. Restore the backed up data from the tape to the secondary volume. To restore the data, execute **EX_DRM_TAPE_RESTORE** on the backup server.

   **BKServer > EX_DRM_TAPE_RESTORE Operation_A -backup_id 0000000002**

3. Export backup information to a temporary file. To restore the data from the secondary volume to the primary volume, you must copy backup information about restore performed from the tape to the secondary volume. Copy this information to the file server. Execute **EX_DRM_DB_EXPORT** to export the backup information to a temporary file in the temporary directory for extended commands.

   **BKServer > EX_DRM_DB_EXPORT Operation_A**

4. Execute **EX_DRM_FTP_GET** on the fileserver to batch-receive the temporary files held on the backup server onto the file server. Temporary files are stored in a temporary directory for extended commands on the database server.

   **FSServer_A > EX_DRM_FTP_GET Operation_A -server BKServer**

5. Import the temporary files that were transferred from the backup server, to the backup catalog on the file server. To import the files, execute **EX_DRM_DB_IMPORT** on the file server.

   **FSServer_A >EX_DRM_DB_IMPORT Operation_A**

6. Restore the data of the secondary volume to the primary volume. Resynchronize the primary volume and secondary volume and then restore the data. To restore the data, execute the **drmfsrestore** command on the file server.

   **FSServer_A > drmfsrestore 0000000001 -resync**

### 3.5.3 Example of Restoring Data Between Volumes

This section gives an example of recovering file system when backup data is saved in the secondary volume. This example resynchronizes the secondary volume to the primary volume and then restores the data. This example uses **Operation_A** as the operation ID that identifies the file system to be restored.

To restore file system:

1. Check the ID of the backup data to be used for restore. To check the ID, execute the **drmfscat** command on the file server.

```
FSServer_A >drmfscat /mnt1
INSTANCE: /mnt1
BACKUP-ID: 0000000001 BACKUP-MODE: ON-LINE INSTANCE: /mnt1    ORIGINAL-ID:
0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FSServer_A
T FILE     FS         DG   DEVICE       COPY-GROUP
F -         /mnt1    -    Harddisk2   VG01,vol01
F -         -          -    -             VG01,vol01
:
```

2. Create a backup ID record file by executing **EX_DRM_BACKUPID_SET**, specifying the backup ID.

   **FSServer_A > EX_DRM_BACKUPID_SET Operation_A -backup_id 0000000001**

3. Restore the data of the secondary volume to the primary volume. Resynchronize the primary volume and secondary volume and then restore the data. To restore the data, execute the **drmfsrestore** command on the file server.

   **FSServer_A > drmfsrestore 0000000001 -resync -recovery**

## 3.6 Examples of Using Extended Commands (Copy Controller in Windows)

This section uses examples to illustrate how to use extended commands. The examples in this section assume the system configuration shown in Figure 3.22.

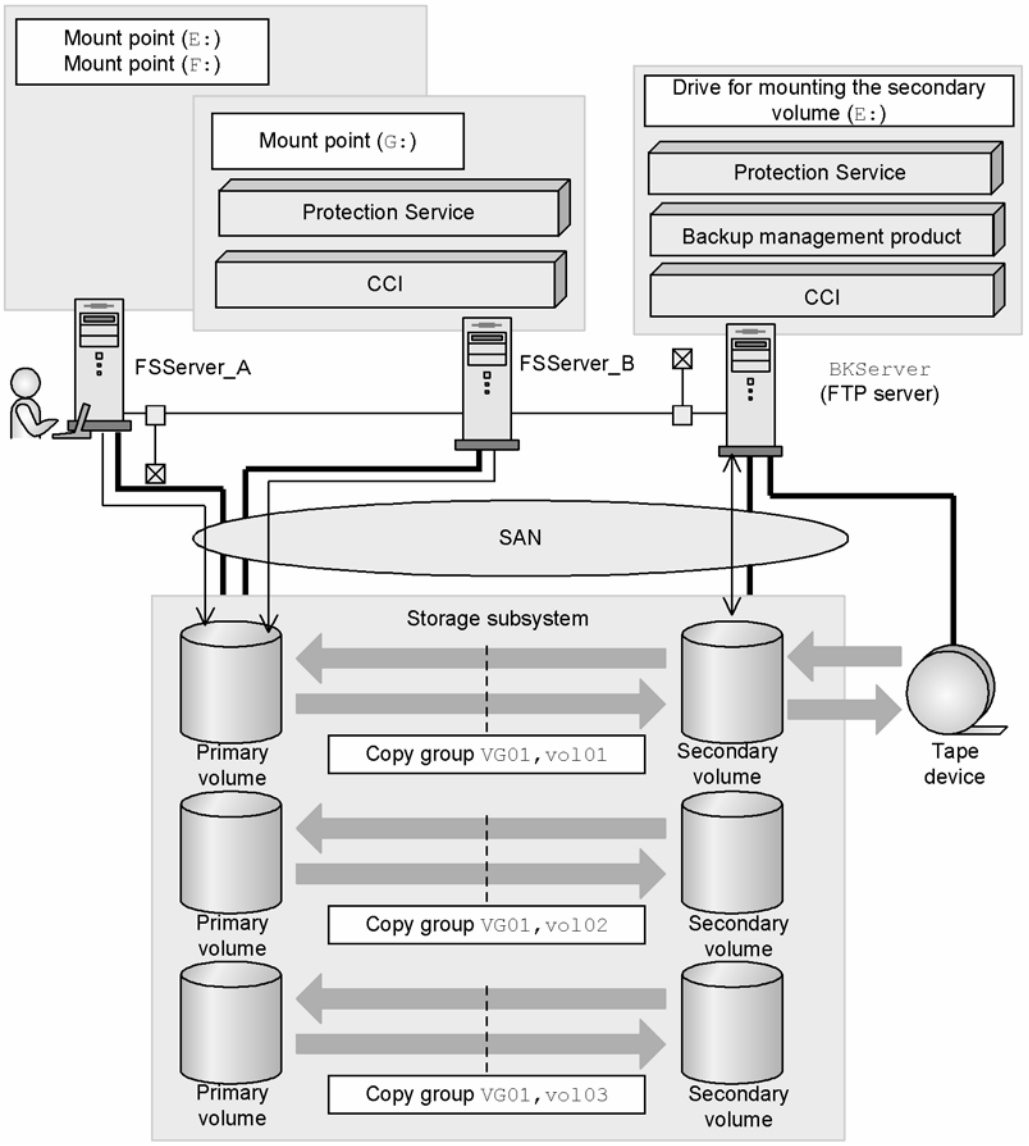



**Figure 3.22 System Configuration: Back Up and Restore a File System to Tape (Windows)**

The examples in this section assume the following conditions:

- The mount point to be backed up is NTFS-formatted.
- The primary volume and secondary volume are defined as a pair at the file server and the backup server.
- The backup management product is installed on the backup server.
- The parameters for the backup management product have been registered by using the **drmtapeinit** command.
- The FTP service is running on the backup server, and the OS logon user for each file server can log on to the FTP server and transmit files using FTP. The FTP user ID is **admin**, and the FTP user password is **password**.
- There are two file servers (server names: **FSServer_A** and **FSServer_B**) and a backup server to which a tape device is connected (server name: **BKServer**).
- The host parameters have been changed by executing the **cscript //H:Cscript** command from the command prompt.
- The primary volume paired with the secondary volume to be backed up is not backed up until the backup of the secondary volume to tape is completed.
- **FSServer_A** has mount points **E:** and **F:**, while **FSServer_B** has mount point **G:**.
- The mount point to be backed up is run in always-split mode.
- The secondary volume is not always mounted; it is mounted in the **E** drive (drive letter: **E:**) only during operation.
- At each file server and the backup server, the storage directories for extended command temporary files specified in the operation definition file have been created.

### 3.6.1 Example of Backing Up File Systems

This section gives an example of cold backup of a file system to a tape. This example performs online backup of the mount point directory **E:** of the file server **FSServer_A** to the secondary volume and then backs up this data from the secondary volume to a tape. The example uses **Operation_A** as the operation ID that identifies the file system to be backed up. Note that you cannot perform any new backup until the backup data has been backed up to tape.

To back up the file system:

1. Before starting the backup, clear the system cache for the backup server. To clear the system cache, execute **EX_DRM_CACHE_PURG** on the backup server and mount/unmount the secondary volume. In this example, the copy group name is **VG01,vol01**.

   **BKServer > EX_DRM_CACHE_PURGE Operation_A -cg VG01,vol01**

2. Execute **EX_DRM_RESYNC** on the file server to resynchronize the copy groups. Resynchronizing the copy groups before you perform backup enhances the speed of backup processing.

   **FSServer_A > EX_DRM_RESYNC Operation_A -cg VG01,vol01 -copy_size 7**

3. Back up the file system to the secondary volume. To do this, execute **EX_DRM_FS_BACKUP**. Specify the operation ID **Operation_A** as the argument.

   **FSServer_A > EX_DRM_FS_BACKUP Operation_A**

4. Export the backup record to a temporary file. To back up data from the secondary volume to a tape, you must copy information about the backup that was performed from the primary volume to the secondary volume. Copy this information to the backup server. Execute **EX_DRM_DB_EXPORT** to export information about backup to a temporary file. Temporary files are stored in a temporary directory for extended commands on the file server.

   **FSServer_A > EX_DRM_DB_EXPORT Operation_A**

5. Batch-transfer the temporary files from the file server to the backup server. To transfer the files, execute **EX_DRM_FTP_PUT** on the file server. In this example, the user ID used for logon to the FTP server is **admin** and the password is **password**. Temporary files are stored in a temporary directory for extended commands on the backup server.

   **FSServer_A > EX_DRM_FTP_PUT Operation_A -server BKServer -user admin -password password**

6. Import the temporary files that were transferred from the file server to the backup catalog on the backup server. To import the files, execute **EX_DRM_DB_IMPORT** on the backup server.

   **BKServer > EX_DRM_DB_IMPORT Operation_A**

7. To back up the data, execute **EX_DRM_TAPE_BACKUP** on the backup server. In this example, the mount point directory for tape backup is **/mnt1**.

   **BKServer > EX_DRM_TAPE_BACKUP Operation_A -exopt -mount_pt E:**

   When you execute backup, information about this backup is registered in the backup catalog with the new backup ID, **0000000002**.

### 3.6.2 Example of Restoring a File System

This section gives an example of restoring data that was backed up to a tape and recovering the file system. This example restores the data from the tape to the secondary volume, then resynchronizes the secondary volume to the primary volume, and restores the data. This example uses **Operation_A** as the operation ID that identifies the file system to be restored.

To restore the file system:

1. Check the ID of the backup data to be used for restore processing. To check the ID, execute the **drmtapecat** command on the backup server.

```
BKServer >drmtapecat -hostname BKServer_A -l
BACKUP-ID ORIGINAL-ID HOSTNAME BACKUP-OBJECT INSTANCE SNAPSHOT TIME     EXPIRATION
TIME   BACKUP-MEDIA
0000000002 0000000001 BKServer_A FILESYSTEM  E:   2003/08/01 19:42:15 2003/08/11
20:32:20  -
:
:
```

2. Restore the backed up data from the tape to the secondary volume. To restore the data, execute **EX_DRM_TAPE_RESTORE** on the backup server.

   **BKServer > EX_DRM_TAPE_RESTORE Operation_A -backup_id 0000000002**

3. Export backup information to a temporary file. To restore the data of the secondary volume to the primary volume, you must copy backup information about restore processing performed from the tape to the secondary volume. Copy this information to the file server. Execute **EX_DRM_DB_EXPORT** to export the backup information to a temporary file in the temporary directory for extended commands.

   **BKServer > EX_DRM_DB_EXPORT Operation_A**

4. Execute **EX_DRM_FTP_GET** on the file server to batch-receive the temporary files held on the backup server onto the file server. In this example, the user ID used for logon to the FTP server is **admin** and the password is **password**. Temporary files are stored in a temporary directory for extended commands on the file server.

   **FSServer_A > EX_DRM_FTP_GET Operation_A -server BKServer -user admin -password password**

5. Import the temporary files that were transferred from the backup server to the backup catalog on the file server. To import the files, execute **EX_DRM_DB_IMPORT** on the file server.

   **FSServer_A >EX_DRM_DB_IMPORT Operation_A**

6. Restore the data of the secondary volume to the primary volume. Resynchronize the primary volume and secondary volume, and then restore the data. To restore the data, execute **EX_DRM_FS_RESTORE** on the file server.

   **FSServer_A > EX_DRM_FS_RESTORE.sh  Operation_A -resync**

### 3.6.3 Example of Restoring Data Between Volumes

This section gives an example of recovering a file system when backup data is saved on the secondary volume. This example resynchronizes the secondary volume to the primary volume and then restores the data. This example uses **Operation_A** as the operation ID that identifies the file system to be restored.

To restore the file system:

1. Check the ID of the backup data to be used for restore processing. To check the ID, execute the **drmfscat** command on the file server.

```
FSServer_A >drmfscat E:
INSTANCE: E:
BACKUP-ID: 0000000001 BACKUP-MODE: ON-LINE INSTANCE: E:    ORIGINAL-ID: 0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FSServer_A
T FILE     FS         DG   DEVICE       COPY-GROUP
F -         E:         -    Harddisk2   VG01,vol01
F -         -          -    -             VG01,vol01
:
```

2. Create a backup ID record file by executing **EX_DRM_BACKUPID_SET**, specifying the backup ID.

   **FSServer_A > EX_DRM_BACKUPID_SET Operation_A -backup_id 0000000001**

3. Restore the data of the secondary volume to the primary volume. Resynchronize the primary volume and secondary volume and then restore the data. To restore the data, execute **EX_DRM_FS_RESTORE** on the file server.

   **DBServer_A > EX_DRM_FS_RESTORE Operation_A -resync**

## 3.7 Examples of Using Extended Commands (SQL Server)

This section uses examples to illustrate how to use extended commands. The examples in this section assume the system configuration shown in Figure 3.22.

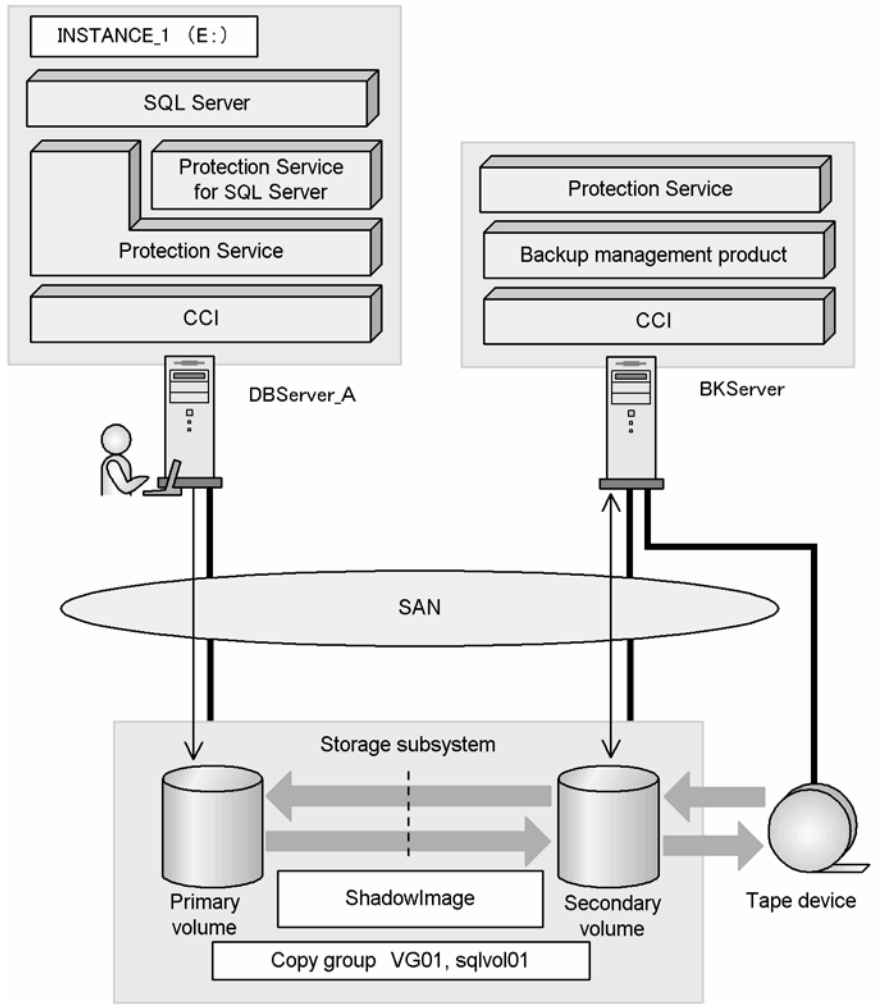



**Figure 3.23 System Configuration: Back Up and Restore an SQL Server DB to Tape**

The examples in this section assume the following conditions:

- The primary volume is NTFS-formatted.
- The primary volume and secondary volume are mirrored.
- The backup management product is installed on the backup server.
- The parameters of the backup management product have been registered by using the **drmtapeinit** command.
- The FTP service on the backup server is started, and the system is set up so a user who has logged onto the operating system of the database server can log onto the FTP server and transfer files to the FTP server. The FTP server ID is **admin**, and the FTP user password is **password**.
- Back up the SQL Server database onto tape using the online format.
- Two SQL Server instances (**INSTANCE_1** and **INSTANCE_2**) exist, and services are running on database server A (**DBServer_A**).
- The instance to be backed up is performing ordinary split operation.
- Extended command temporary file installation folders and VDI metafile storage directories are created by the database server and backup server.
- The secondary volume is not always mounted; it is mounted on the E drive (drive character **E:**) only while it is operating.
- The primary volume configured as a pair with the secondary volume to be backed up will not be backed up until the secondary volume is backed up onto tape.
- The **cscript //H:Cscript** command is executed from the command prompt and the host parameters are updated.

### 3.7.1 Example of Backing Up the SQL Server Database

This section provides an example of online-backing up the SQL Server database onto tape. In this example, the **INSTANCE_1** instance of the **DBServer_A** database server is first online-backed up to the secondary volume, and then backed up from the secondary volume to tape. The operation ID is **Operation_A**. While data is being backed up to tape, another backup cannot be performed.

To back up the SQL Server database:

1. Clear the cache of the secondary volume. Before backing up SQL Server, clear the system cache on the backup server. To clear the system cache, on the backup server, execute the **EX_DRM_CACHE_PURGE** extended command to mount and then unmount the secondary volume. In this example, the copy group name is **VG01,sqlvol01**.
   ```
   BKServer > EX_DRM_CACHE_PURGE Operation_A -cg VG01,sqlvol01
   ```
2. Resynchronize the copy group. On the database server, execute the **EX_DRM_RESYNC** extended command to resynchronize the copy group. When the copy group is resynchronized before backup, the backup can be faster.
   ```
   DBServer_A > EX_DRM_RESYNC Operation_A -cg VG01,sqlvol01
   -copy_size 7
   ```
3. Back up the SQL Server database onto the secondary volume. Perform online backup of the SQL Server database. Execute the **EX_DRM_SQL_BACKUP** extended command with the operation ID **Operation_A** to back up:
   ```
   DBServer_A > EX_DRM_SQL_BACKUP Operation_A -system
   ```
4. Export the backup record to a temporary file. To back up data from the secondary volume to tape, copy the backup record to the backup server. Execute the **EX_DRM_DB_EXPORT** extended command to export the backup record to a temporary file. This temporary file is stored in the temporary-file folder for extended commands on the database server.
   ```
   DBServer_A > EX_DRM_DB_EXPORT Operation_A
   ```
5. Back up the SQL Server metafiles created at the backup to the temporary folder. Back up the SQL Server metafiles created at the backup to the temporary folder for extended commands on the database server so that the SQL Server metafiles and temporary file can be transmitted collectively to the backup server. To back up the SQL Server metafiles, execute the **EX_DRM_SQLFILE_PACK** extended command.
   ```
   DBServer_A > EX_DRM_SQLFILE_PACK Operation_A
   ```
6. Transmit the metafiles and temporary file to the backup server. On the database server, execute the **EX_DRM_FTP_PUT** extended command to transmit the SQL Server metafiles and temporary file collectively to the backup server. In this example, the user ID to log on to the FTP server is admin and the login password is password. The metafiles and temporary file are stored in the temporary folder for extended commands on the backup server.
   ```
   DBServer_A > EX_DRM_FTP_PUT Operation_A -server BKServer
   -user admin -password password
   ```
7.

8. Import the temporary file transmitted from the database server into the backup catalog on the backup server. On the backup server, execute the **EX_DRM_DB_IMPORT** extended command to import the temporary file (that was transmitted from the database server) into the backup catalog.
   ```
   BKServer > EX_DRM_DB_IMPORT Operation_A
   ```

9. On the backup server, deploy the metafiles that were transmitted from the database server. On the backup server, execute the **EX_DRM_SQLFILE_EXTRACT** extended command to deploy the metafiles transmitted from the database server.
   ```
   BKServer > EX_DRM_SQLFILE_EXTRACT Operation_A
   ```

10. Back up the data of the secondary volume to a tape. On the backup server, execute the **EX_DRM_TAPE_BACKUP** extended command to back up the data of the secondary volume. In this example, the drive letter of the secondary volume is assumed to be **E**:
    ```
    BKServer > EX_DRM_TAPE_BACKUP Operation_A -exopt -mount_pt
    E:
    ```

    When this backup is executed, the backup record is registered, with a new backup ID of **0000000002**, in the backup catalog.

### 3.7.2 Example of Restoring the SQL Server Database

This section provides an example of restoring data that has been backed up onto tape and recovering the SQL Server database. In this example, you first restore data from a tape to the secondary volume, and then you resynchronize the secondary volume with the primary volume to restore the data on the primary volume. The operation ID is **Operation_A**.

To restore the SQL Server database:

1. Check the backup ID of the backup you want to use for restoration. On the backup server, execute the **drmsqlcat** command to check the backup ID of the backup you want to use for restoration. To check this backup ID, execute the **drmtapecat** command on the backup server.
```
BKServer >drmtapecat -hostname DBServer_A -l
BACKUP-ID ORIGINAL-ID HOSTNAME BACKUP-OBJECT INSTANCE
SNAPSHOT TIME EXPIRATION TIME BACKUP-MEDIA
0000000002 0000000001 hpcm1 MSSQL LION 2003/
08/01 19:42:15 2003/08/11 20:32:20 -
:
:
```
2. Restore data from its backup tape to the secondary volume. To restore data, on the backup server, execute the **EX_DRM_TAPE_RESTORE** extended command.
```
BKServer > EX_DRM_TAPE_RESTORE Operation_A -backup_id
0000000002
```
3. Export the backup record to a temporary file. To restore data from the secondary volume to the primary volume, the backup information about the restore operation from tape to the secondary volume needs to be copied to the database server. Execute the **EX_DRM_DB_EXPORT** extended command to export the backup record to a temporary file. This temporary file is stored in the temporary-file folder for extended commands.
```
BKServer > EX_DRM_DB_EXPORT Operation_A
```
4. Back up the metafiles created at the restoration to the temporary folder. Back up the metafiles created at the restoration to the temporary folder for extended commands on the backup server so that the metafiles and temporary file can be transmitted collectively to the database server. To back up the metafiles, execute the **EX_DRM_SQLFILE_PACK** command on the backup server.
```
BKServer > EX_DRM_SQLFILE_PACK Operation_A
```
5. On the database server, receive the metafiles and temporary file. On the database server, execute the **EX_DRM_FTP_GET** extended command to receive the metafiles and temporary file collectively from the backup server. In this example, the user ID to log on to the FTP server is admin and the login password is password. The metafiles and temporary file are stored in the temporary folder for extended commands on the database server.
```
DBServer_A > EX_DRM_FTP_GET Operation_A -server BKServer
-user admin -password password
```

6. Import the temporary file transmitted from the backup server to the backup catalog on the database server. Import the temporary file that was transmitted from the backup server into the backup catalog on the database server.
```
DBServer_A >EX_DRM_DB_IMPORT Operation_A
```

7. On the database server, deploy the metafiles that were transmitted from the backup server. On the database server, execute the **EX_DRM_SQLFILE_EXTRACT** extended command to deploy the metafiles transmitted from the backup server.
```
DBServer_A > EX_DRM_SQLFILE_EXTRACT Operation_A
```

8. Restore data in the secondary volume to the primary volume. On the database server, execute the **EX_DRM_SQL_RESTORE** extended command to restore the primary volume by resynchronizing the secondary volume with the primary volume.
```
DBServer_A > EX_DRM_SQL_RESTORE Operation_A -resync
```

9. Recover the SQL Server database. To recover the SQL Server database, execute the **drmsqlrecover** or **drmsqlrecovertool** command.

   When you execute the **drmsqlrecover** command to recover the SQL Server database:
```
DBServer_A > drmsqlrecover INSTANCE_1
KAVX0001-I The drmsqlrecover command will now start.
KAVX0002-I The drmsqlrecover command will now end.
BKServer >
```

   When you execute the **drmsqlrecovertool** command to recover the SQL Server database:
```
DBServer_A > drmsqlrecovertool INSTANCE_1
BKServer >
```

   When the command is executed, the **drmsqlrecovertool** dialog box is displayed. For details about the **drmsqlrecovertool** dialog box, see the description of the **drmsqlrecovertool** command in Chapter 6.

### 3.7.3 Example of Restoring Data Between Volumes for SQL Server

This section provides an example of recovering the SQL Server database when the backup data is stored on the secondary volume. In this example, you resynchronize the secondary volume with the primary volume to restore the data on the primary volume. The operation ID is Operation_A.

To restore the SQL Server database:

1. Check the backup ID of the backup you want to use for restoration. On the backup server, execute the **drmsqlcat** command to check the backup ID of the backup you want to use for restoration.
```
INSTANCE: INSTANCE_1
BACKUP-ID: 0000000001 BACKUP-MODE: ON-LINE INSTANCE: SQL1
ORIGINAL-ID: 0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00
HOSTNAME: DBServer_A
T DB OBJECT FILE FS DG DEVICE
COPY-GROUP
M DB1 METAFILE D:\MSSQL\DBServer_A\INSTANCE_1\META C: -
- -
D DB1 DATAFILE E:\SQL\data1 D: -
Harddisk1 VG01,sqlvol01
T DB1 TRANSACT E:\SQL\tlog E: -
Harddisk2 VG01,sqlvol01
:
```
2. Create a backup ID file. Specify the backup ID to execute the **EX_DRM_BACKUPID_SET** command and create a backup ID file.
```
DBServer_A > EX_DRM_BACKUPID_SET Operation_A -backup_id
0000000001
```
3. Deploy the metafiles that were backed up in the temporary folder. Execute the **EX_DRM_SQLFILE_EXTRACT** command to deploy the metafiles backed up in the temporary folder.
```
DBServer_A > EX_DRM_SQLFILE_EXTRACT Operation_A
```
4. Restore data in the secondary volume to the primary volume. On the database server, execute the **EX_DRM_SQL_RESTORE** extended command to restore the primary volume by resynchronizing the secondary volume with the primary volume.
```
DBServer_A > EX_DRM_SQL_RESTORE Operation_A -resync
```
5. Recover the SQL Server database. To recover the SQL Server database, execute the **drmsqlrecover** or **drmsqlrecovertool** command on the database server.

   When you execute the **drmsqlrecover** command to recover the SQL Server database:
```
DBServer_A > drmsqlrecover INSTANCE_1
KAVX0001-I The drmsqlrecover command will now start.
KAVX0002-I The drmsqlrecover command will now end.
BKServer >
```
   When you execute the **drmsqlrecovertool** command to recover the SQL Server database:
```
DBServer_A > drmsqlrecover INSTANCE_1
DBServer_A > drmsqlrecovertool INSTANCE_1
BKServer >
```
   When you execute the command, the **drmsqlrecovertool** dialog box is displayed. For details about the **drmsqlrecovertool** dialog box, see the description of the **drmsqlrecovertool** command in Chapter 6.

## 3.8 Examples of Using Extended Commands (Exchange Server)

This section uses examples to illustrate how to use extended commands. The examples in this section assume the system configuration shown in Figure 3.24.

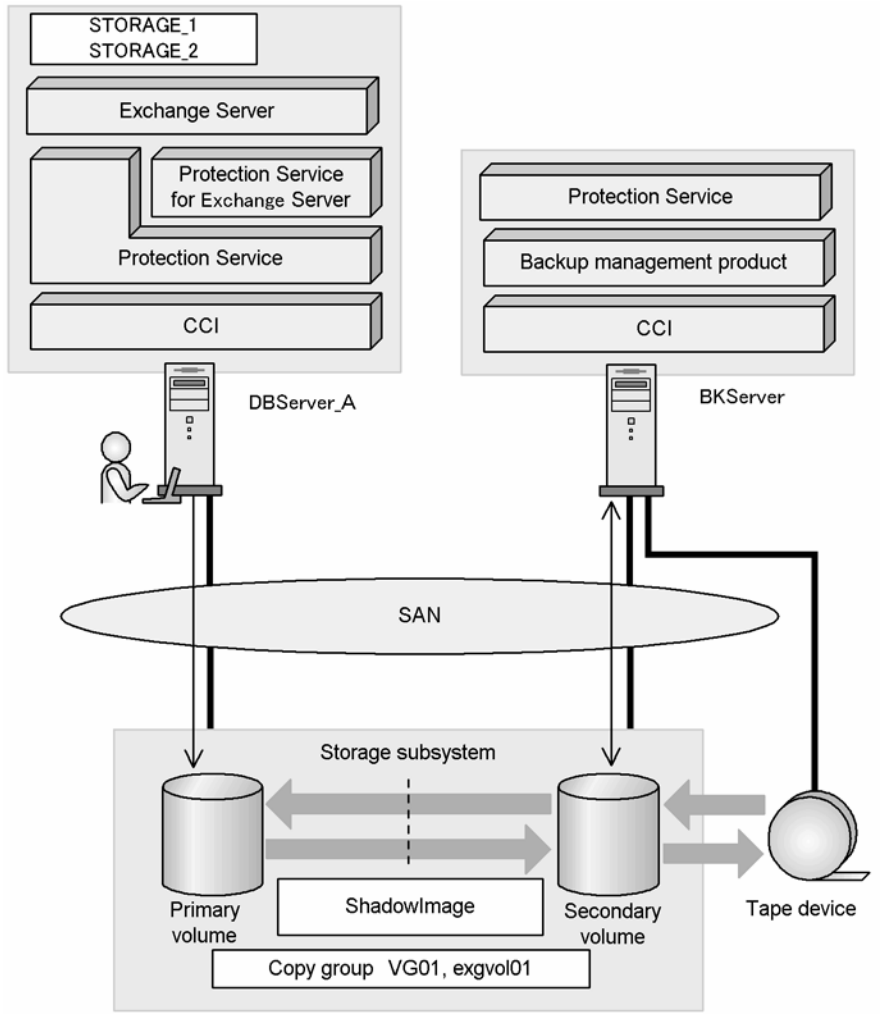



**Figure 3.24 System Configuration: Back Up and Restore an Exchange Server DB to Tape**

The examples in this section assume the following conditions:

- The primary volume is NTFS-formatted.
- The primary volume and secondary volume are mirrored.
- The backup management product is installed on the backup server.
- The parameters of the backup management product have been registered by using the **drmtapeinit** command.
- The FTP service on the backup server is started, and the system is set up so a user who has logged onto the operating system of the database server can log onto the FTP server and transfer files to the FTP server. The FTP server ID is **admin**, and the FTP user password is **password**.
- The Exchange Server used in the system is an Exchange 2000 Enterprise Server.
- Two storage groups (**STORAGE_1** and **STORAGE_2**) exist on database server A (**DBServer_A**), and services are running on database server A.
- The storage group to be backed up is performing ordinary split operation.
- Extended command temporary file installation folders are created by the database server and backup server.
- The secondary volume is not always mounted; it is mounted on the E drive (drive character **E:**) only while it is operating.
- The primary volume configured as a pair with the secondary volume to be backed up will not be backed up until the secondary volume is backed up onto tape.
- The **cscript //H:Cscript** command is executed from the command prompt and the host parameters are updated.

### 3.8.1 Examples of Backing Up the Exchange Database

This section provides examples of the processing flow for backing up the Exchange database onto tape in a system in a multi-server configuration during always-split mode. Use extended commands to execute cold backup and online backup.

**(1) Example of cold backup**

This is an example of performing cold backup onto tape of the Exchange database. In this example, storage groups **STORAGE_1** and **STORAGE_2** are cold backed up onto the secondary volume and then are backed up onto tape from the secondary volume. It uses **Operation_A** as the operation ID. Note that you cannot perform any new backup until the backup data has been backed up to a tape.

To do cold backup of the Exchange database:

1. Clear the cache of the secondary volume. Before performing backup, clear the system cache of the backup server. To clear the system cache, execute **EX_DRM_CACHE_PURGE** on the backup server and mount and then unmount the secondary volume. In this example, the copy group name is **VG01,exgvol01**.
   ```
   BKServer > EX_DRM_CACHE_PURGE Operation_A -cg VG01,exgvol01
   ```
2. Execute **EX_DRM_RESYNC** on the database server to resynchronize the copy groups. Resynchronizing the copy groups before you perform backup enhances the speed of backup processing.
   ```
   DBServer_A > EX_DRM_RESYNC Operation_A -cg VG01,exgvol01 -copy_size 7
   ```
3. Perform a cold backup of the Exchange database. To perform backup, execute **EX_DRM_EXG_BACKUP**. Specify the operation ID **Operation_A** as the argument. In this example, delete the transaction log file, and back up the database.
   ```
   DBServer_A > EX_DRM_EXG_BACKUP Operation_A -mode cold -transact log del
   ```
4. Export the backup record to a temporary file. To back up data from the secondary volume to a tape, you must copy information about backup that was performed from the primary volume to the secondary volume. Copy this information to the backup server. Execute **EX_DRM_DB_EXPORT** to export information about backup to a temporary file. Temporary files are stored in a temporary folder for the extended commands on the database server.
   ```
   DBServer_A > EX_DRM_DB_EXPORT Operation_A
   ```
5. Batch-transfer the temporary files from the database server to the backup server. To transfer the files, execute **EX_DRM_FTP_PUT** on the database server. In this example, the user ID used for logon to the FTP server is **admin** and the password is **password**. Temporary files are stored in a temporary folder for the extended commands on the backup server.
   ```
   DBServer_A > EX_DRM_FTP_PUT Operation_A -server BKServer -user admin -password
   password
   ```

6. Import the temporary files that were transferred from the database server, to the backup catalog on the backup server. To import the files, execute **EX_DRM_DB_IMPORT** on the backup server.
   ```
   BKServer > EX_DRM_DB_IMPORT Operation_A
   ```

7. Back up the data of the secondary volume to a tape. To back up the data, execute **EX_DRM_TAPE_BACKUP** on the backup server. In this example, the drive containing the secondary volume is **E:**.
   ```
   BKServer > EX_DRM_TAPE_BACKUP Operation_A -exopt -mount_pt E:
   ```

   When you execute backup, information about this backup is registered in the backup catalog with the new backup ID **0000000002**.

**(2) Example of online backup**

This is an example of online backup of the Exchange database onto tape. In this example, storage groups **STORAGE_1** and **STORAGE_2** for database server **DBServer_A** are online backed up onto the secondary volume, then the consistency of the Exchange database is verified. Next, these storage groups are backed up from the secondary volume onto tape. **Operation_A** is used as the operation ID. Note that you cannot perform any new backup until the backup data has been backed up onto tape.

To perform online backup of the Exchange database:

1. Clear the cache of the secondary volume. Clear the system cache of the backup server before performing the backup. To clear the system cache, execute the **EX_DRM_CACHE_PURGE** command on the backup server and mount/dismount the secondary volume. In this example, the copy group name is **VG01,exgvol01**.
   ```
   BKServer > EX_DRM_CACHE_PURGE Operation_A -cg VG01,exgvol01
   ```

2. Execute **EX_DRM_RESYNC** on the database server to resynchronize the copy group. You can accelerate the backup process by resynchronizing the copy group before performing the backup.
   ```
   DBServer_A > EX_DRM_RESYNC Operation_A -cg VG01,exgvol01 -copy_size 7
   ```

3. Back up the Exchange database onto the secondary volume. Execute **EX_DRM_EXG_BACKUP** on the database server to do online backup of the Exchange database. Specify the operation ID **Operation_A** as an argument.
   ```
   DBServer_A > EX_DRM_EXG_BACKUP Operation_A -mode online
   ```

4. Export the backup record to a temporary file. To back up from the secondary volume onto tape, you must copy onto the backup server all information relating to the backup operation from the primary volume to the secondary volume. Execute **EX_DRM_DB_EXPORT** to export into a temporary file the information relating to the backup operation. The temporary file is stored in the temporary folder for extended commands on the database server.
   ```
   DBServer_A > EX_DRM_DB_EXPORT Operation_A
   ```

5. Transfer the temporary files from the database server to the backup server all at once. To transfer these files, execute the **EX_DRM_FTP_PUT** command on the database server. In this example, use the user ID **admin** and the password **password** to log onto the FTP server. The temporary files are stored in the temporary folder for extended commands on the backup server.
```
DBServer_A > EX_DRM_FTP_PUT Operation_A -server BKServer -user admin -password
password
```

6. Import the temporary files transferred from the database server to the backup catalog for the backup server by executing the **EX_DRM_DB_IMPORT** command on the backup server.
```
BKServer > EX_DRM_DB_IMPORT Operation_A
```

7. Verify the backed up Exchange database. To verify the consistency of the Exchange database that was online backed up onto the secondary volume, execute the **EX_DRM_EXG_VERIFY** command on the backup server.
```
BKServer > EX_DRM_EXG_VERIFY Operation_A
```

8. Back up the data on the secondary volume onto tape. To back up the data, execute the **EX_DRM_TAPE_BACKUP** command on the backup server. In this example, the drive character of the secondary volume is **E:**.
```
BKServer > EX_DRM_TAPE_BACKUP Operation_A -exopt -mount_pt E:
```

   When you execute the backup, information relating to this backup operation is registered in the backup catalog with the new backup ID **0000000002**.

### 3.8.2 Example of Restoring Exchange Server

This section provides an example of restoring data backed up onto tape and recovering the Exchange database. This example restores the data from the tape to the secondary volume, then resynchronizes the secondary volume to the primary volume, and restores the data. This example uses **Operation_A** as the operation ID.

To restore the Exchange database:

1. Check the backup ID of the backup data. Check the ID of the backup data to be used for restore. To check the ID, execute the **drmtapecat** command on the backup server.
```
BKServer >drmtapecat -hostname DBServer_A -l
BACKUP-ID  ORIGINAL-ID HOSTNAME   BACKUP-OBJECT INSTANCE SNAPSHOT TIME
EXPIRATION TIME BACKUP-MEDIA
0000000001 0000000001  DBServer_A MSEXCHANGE    -        2003/06/01 17:45:36
PERMANENT       MEDIA1
:
:
```

2. Restore the backed up data from the tape to the secondary volume. To restore the data, execute **EX_DRM_TAPE_RESTORE** on the backup server.
```
BKServer > EX_DRM_TAPE_RESTORE Operation_A -backup_id 0000000001
```

3. Export backup information to a temporary file. To restore the data from the secondary volume to the primary volume, you must copy backup information about restore performed from the tape to the secondary volume. Copy this information to the database server. Execute **EX_DRM_DB_EXPORT** to export the backup information to a temporary file in the temporary folder for the extended commands.
```
BKServer > EX_DRM_DB_EXPORT Operation_A
```

4. Receive the temporary files on the database server. Execute **EX_DRM_FTP_GET** on the database server to batch-receive the temporary files held on the backup server onto the database server. In this example, the user ID used for logon to the FTP server is **admin** and the password is **password**. Temporary files are stored in a temporary folder for the extended commands on the database server.
```
DBServer_A > EX_DRM_FTP_GET Operation_A -server BKServer -user admin -password
password
```

5. Import the temporary files that were transferred from the backup server, to the backup catalog on the database server. Import the temporary files that were transferred from the backup server, to the backup catalog on the database server. To import the files, execute **EX_DRM_DB_IMPORT** on the database server.
```
DBServer_A >EX_DRM_DB_IMPORT Operation_A
```

6. Check the backup ID of the backup data. To check the ID, execute the **drmexgcat** command.
```
DBServer_A > drmexgcat -target STORAGE_1
STORAGEGROUP: STORAGE_1
BACKUP-ID:0000000001 BACKUP-MODE: COLD STORAGEGROUP: STORAGE_1
ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:30:00 END-TIME: 2002/06/01 10:31:00 HOSTNAME:DBServer_A
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STORAGE_1)  E:\STR1\priv1.edb      F:          -
Harddisk3    VG01,exgvol01
- -             -                    -                      -           -       -
VG01,exgvol01
M MAILBOXSTORE MAILBOX1(STORAGE_1)  E:\STR1\priv1.stm      F:          -
Harddisk3    VG01,exgvol01
- -             -                    -                      -           -       -
VG01,exgvol01
:
    :
```

7. Restore the data of the secondary volume to the primary volume. Resynchronize the primary volume and secondary volume and then restore the data. To restore the data, execute the **drmexgrestore** command on the database server. To restore the Exchange database that was backed up by performing an online backup, specify the **-recovery** option and execute roll forward.
```
DBServer_A > drmexgrestore 0000000001 -resync -recovery
```

### 3.8.3 Example of Restoring Data Between Volumes

This section provides an example of recovering the Exchange database when the backup data is stored on the secondary volume. This example resynchronizes the secondary volume to the primary volume and then restores the data.

To restore the Exchange database:

1. Check the ID of the backup data to be used for restore. To check the ID, execute the **drmexgcat** command on the database server.

```
DBServer_A > drmexgcat -target STORAGE_1
STORAGEGROUP: STORAGE_1
BACKUP-ID:0000000001 BACKUP-MODE: COLD STORAGEGROUP: STORAGE_1
ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:30:00 END-TIME: 2002/06/01 10:31:00 HOSTNAME:DBServer_A
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STORAGE_1)  E:\STR1\priv1.edb      F:          -
Harddisk3    VG01,exgvol01
- -             -                    -                      -           -       -
VG01,exgvol01
M MAILBOXSTORE MAILBOX1(STORAGE_1)  E:\STR1\priv1.stm      F:          -
Harddisk3    VG01,exgvol01
- -             -                    -                      -           -       -
VG01,exgvol01
:
```

2. Restore the data of the secondary volume to the primary volume. Resynchronize the primary volume and secondary volume, and then restore the data. To restore the data, execute the **drmexgrestore** command on the database server.

```
DBServer_A > drmexgrestore 0000000001 -resync -recovery
```

## 3.9 Log Files for Extended Commands

When the extended command is executed, the execution history of the extended command is recorded in the log file for extended commands. If an error occurred, the error status is also recorded in the log file. The log information is recorded when:

- the extended command started
- the extended command terminated
- a command other than Protection Services commands (**drm*xxxx***) is executed inside the extended command
- a command other than Protection Services commands (**drm*xxxx***) terminated successfully inside the extended command
- a command (including Protection Services commands (**drm*xxxx***)) inside the extended command is executed and then failed

The log file output directory (folder) can store up to two generations of log files. The path names of these log files are as follows:

Current log file:

In UNIX: **/var/opt/drm/script/log/drm_script.log**

In Windows: ***Protection-Services-installation-directory*\script\log\drm_script.log**

Previous log file:

In UNIX: **/var/opt/drm/script/log/drm_script.log.old**

In Windows: ***Protection-Services-installation-directory*\script\log\drm_script.log.old**

If the number of lines in the current log file exceeds the maximum specified with the **MAX_LOG_LINES** entry of the host environment settings file, the current log file is backed up. Then, a new log file is generated to continue logging. If the system fails to record information in the log file when an extended command is executed, log information for the extended command is output to the standard output.

Note that the log information for Protection Services commands executed inside the extended command is output to the standard output log file **drm_trace.log** and the trace log file **drm_pp_trace[1-16].log**.

Table 3.19 shows the items that are output to the log file for extended commands.
The following shows an example of the log file for Copy Controller:

```
2003/07/31 20:15:11.560 |START     |operation1 |FSServer_A |M: |EX_DRM_FS_BACKUP
|KAVX0450-I The EX_DRM_FS_BACKUP command will now start.
2003/07/31 20:17:22.06 |END       |operation1 |FSServer_A |M: |EX_DRM_FS_BACKUP |The
EX_DRM_ORA_BACKUP command will now end.
```

The following shows an example of the log file for Exchange Server:

```
2003/07/31 20:15:11.560 |START     |operation1 |DBServer_A |- |EX_DRM_EXG_BACKUP
|KAVX0450-I The EX_DRM_EXG_BACKUP command will now start.
2003/07/31 20:17:22.06 |END       |operation1 |DBServer_A |- |EX_DRM_EXG_BACKUP
|KAVX0451-I The EX_DRM_EXG_BACKUP command will now end.
```

**Table 3.19 Items that are Output to the Log File for Extended Commands**

| Item | Description |
|---|---|
| Time-stamp | The log output date/time is output to the millisecond.<br>Format: *YYYY*/*MM*/*DD hh*:*mm*:*ss.sss* |
| Log type | The following character string to indicate the log type is output:<br>START: The extended command started<br>END: The extended command terminated<br>INFO: Information<br>WARNING: Warning<br>ERROR: Error<br>DEBUG: Debugging |
| Operation ID | The operation ID for the executed operation is output. |
| File server or database server name | The name of the file/database server that was backed up is output. The character string defined in the specification item **DB_SERVER_NAME** in the operation definition file is output. |
| Instance name | For Copy Controller: The name of the mount point directory or mount point directory list file that was backed up is output.<br>For SQL Server or Exchange Server: The character string defined in the specification item **INSTANCE_NAME** in the operation definition file is output. |
| Extended command's name | The character string that identifies the extended command is output (the extended command's file name except the file extension is output). |
| Options for extended command | The options specified are output. |
| Log message ID | The ID of the log message is output. |
| Log message text | The log message is output by the extended command. |

## 3.10 Extended Command Specifications

### 3.10.1 EX_DRM_BACKUPID_SET (generate a backup ID file)

**Format:**

For Copy Controller:
`EX_DRM_BACKUPID_SET` *`operation-ID`* `-backup_id` *`backup-ID`*

For SQL Server or Exchange Server:
`EX_DRM_BACKUPID_SET.wsf` *`operation-ID`* `-backup_id` *`backup-ID`*

**Description:**

This extended command generates a backup ID file that contains the specified backup ID and stores the file in the temporary directory for extended commands.

Execute this extended command as preparation before restoring the backed up file system or database to the primary volume. Specify the backup ID to be used for restore (the backup ID generated when you backed up the file system or database to the secondary volume) and execute the command.

**Prerequisites:**

- The operation definition file corresponding to the specified operation ID has been created.
- Before executing this extended command, you must confirm the backup ID to be specified with this extended command by viewing the backup catalog information.

  For Copy Controller, get this information using the **drmfscat** command.
  For SQL Server, get this information using the **drmsqlcat** command.
  For Exchange Server, get this information using the **drmexgcat** command.

**Arguments:**

***operation-ID***

Specify the unique character string that indicates the resource to be operated.

**-backup_id *backup-ID***

Specify the backup ID to be used when restoring the backed up file system or database to the primary volume. A backup ID uniquely identifies backup data. It is registered in the backup catalog at backup.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option is specified
- Information could not be acquired from the operation definition file corresponding to the operation ID
- The backup ID could not be recorded in the backup ID file
- A command executed inside the extended command failed
- Information could not be acquired from the host environment settings file
- The storage directory for extended command temporary files that is specified in the operation definition file does not exist

**Example:**

To create a backup ID file that contains the backup ID **0000000001**, execute:

For Copy Controller:
```
EX_DRM_BACKUPID_SET operation01 -backup_id 0000000001
```

For SQL Server or Exchange Server:
```
EX_DRM_BACKUPID_SET.wsf operation01 -backup_id 0000000001
```

### 3.10.2 EX_DRM_CACHE_PURGE (clear the secondary-volume cache)

**Format:**

To clear the cache of the secondary volume in the always-paired mode:

For Copy Controller:
```
EX_DRM_CACHE_PURGE operation-ID
```

For SQL Server or Exchange Server:
```
EX_DRM_CACHE_PURGE.wsf operation-ID
```

To clear the cache of the secondary volume in the always-split mode:

For Copy Controller:
```
EX_DRM_CACHE_PURGE operation-ID
                        -cg copy-group | -cg_file copy-group-list-file
```

For SQL Server or Exchange Server:
```
EX_DRM_CACHE_PURGE.wsf operation-ID
                        -cg copy-group | -cg_file copy-group-list-file
```

**Description:**

This extended command sequentially executes the **drmmount** and **drmumount** commands to clear the cache of the secondary volume.

In the always-paired mode, the cache of the secondary volume for the specified copy group is cleared based on the backup ID created when data is backed up from the primary volume to the secondary volume. In the always-split mode, you need to specify the copy group to clear the cache of the secondary volume since the cache needs to be cleared before the backup.

**Prerequisites:**

- The operation definition file corresponding to the specified operation ID has been created.
- ***Copy Controller:*** When you execute this extended command without specifying a copy group, the file system must have been backed up to a secondary volume by **EX_DRM_FS_BACKUP**, and a backup ID record file must have been generated.

  ***SQL Server:*** When you execute this extended command without specifying a copy group, the database must have been backed up to a secondary volume by **EX_DRM_SQL_BACKUP**, and a backup ID record file must have been generated.

  ***Exchange Server:*** When you execute this extended command without specifying a copy group, the database must have been backed up to a secondary volume by **EX_DRM_EXG_BACKUP**, and a backup ID record file must have been generated.

**Arguments:**

***operation-ID***

Specify the unique character string that indicates the resource to be operated. The information in the operation definition file corresponding to the specified operation ID is used for executing this extended command.

**-cg** ***copy-group***

In the always-split mode, specify the name of the copy group to clear the cache of the secondary volume. When the copy group to be used at the next backup is identified, specify the copy group. When the copy group to be used at the next backup is not identified, specify all the copy groups.

**-cg_file** ***copy-group-list-file***

In the always-split mode, specify the absolute path of the copy group list file that records the copy group for which you want to clear the cache of the secondary volume. Use this option if you want to clear the caches for many copy groups at the same time. When the copy group to be used at the next backup is identified, specify the copy group. When the copy group to be used at the next backup is not identified, specify all the copy groups.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Note:**

***WARNING:*** Make sure to execute this extended command for all secondary volumes of resources to be backed up before backing up a file system or database to a secondary volume. If you back up a file system or database without clearing the cache of the target secondary volume, the data remaining in the cache will overwrite the secondary volume when the target secondary volume is mounted. This may damage the backup data.

**Conditions causing an error:**

- An invalid option is specified
- Information could not be acquired from the operation definition file corresponding to the operation ID
- The backup ID could not be acquired from the backup ID file (when the copy group was not specified)
- Information could not be acquired from the copy group list file (when the file was specified)
- Information could not be acquired from the host environment settings file
- The extended commands temporary file storage folder specified by the operation definition file does not exist
- A command executed inside the extended command failed
- The execution results of a command executed within an extended command could not be acquired

**Examples:**

- To clear the cache of the secondary volume that belongs to the **CG001,dev01** copy group, execute:

  For Copy Controller:
  ```
  EX_DRM_CACHE_PURGE operation01 -cg CG001,dev01
  ```

  For SQL Server or Exchange Server:
  ```
  EX_DRM_CACHE_PURGE.wsf operation01 -cg CG001,dev01
  ```

- To clear the cache of the secondary volume that belongs to the copy group specified in the **C:\temp\CGLIST.txt** copy group list file, execute:

  For Copy Controller:
  ```
  EX_DRM_CACHE_PURGE operation01 -cg_file C:\temp\CGLIST.txt
  ```

  For SQL Server or Exchange Server:
  ```
  EX_DRM_CACHE_PURGE.wsf operation01 -cg_file C:\temp\CGLIST.txt
  ```

- To clear the cache of the secondary volume that belongs to the copy group corresponding to the backup ID recorded in the backup ID file, execute:

  For Copy Controller:
  ```
  EX_DRM_CACHE_PURGE operation01
  ```

  For SQL Server or Exchange Server:
  ```
  EX_DRM_CACHE_PURGE.wsf operation01
  ```

### 3.10.3 EX_DRM_CG_DEF_CHECK (check the contents of a copy group list file)

**Format:**

To check the contents of a copy group list file:

For Copy Controller:
```
EX_DRM_CG_DEF_CHECK -cg_file copy-group-list-file-name
```

For SQL Server or Exchange Server:
```
EX_DRM_CG_DEF_CHECK.wsf -cg_file copy-group-list-file-name
```

To display the command usage:

For Copy Controller:
```
EX_DRM_CG_DEF_CHECK -h
```

For SQL Server or Exchange Server:
```
EX_DRM_CG_DEF_CHECK.wsf -h
```

**Description:**

This extended command checks the contents of a copy group list file. This command first checks to see if the file specified in the argument exists. If it does exist, the command then checks all the copy groups set in the copy group list file for the following items:

- Only one copy group name is specified per line.
- No copy group name specified in the file is duplicated.
- The copy group names specified in the file are included in the list of copy groups that is displayed by the **drmcgctl** command.

In a UNIX environment, copy group names are case sensitive. In a Windows environment, copy group names are not case sensitive.

**Prerequisite:**

- This extended command must be executed on the machine that contains the copy group list file to be checked.

**Arguments:**

**-cg_file *copy-group-list-file-name***

Specify the absolute path name of the copy group list file to be checked.

**-h**

Specify this option to display help for the usage of this extended command.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option is specified
- The file specified in the argument does not exist, or the system cannot access the specified file
- An error was found during checking of the contents of the copy group list file
- A command executed inside the extended command terminated abnormally

**Examples:**

- To check the copy group list file **/usr/home/work/CGDEF.txt** in a UNIX environment, execute:

  For Copy Controller:
  ```
  EX_DRM_CG_DEF_CHECK -cg_file /usr/home/work/CGDEF.txt
  ```

- To check the copy group list file **C:\WORK\CGDEF.txt** in a Windows environment, execute:

  For Copy Controller:
  ```
  EX_DRM_CG_DEF_CHECK -cg_file C:\WORK\CGDEF.txt
  ```

  For SQL Server or Exchange Server:
  ```
  EX_DRM_CG_DEF_CHECK.wsf -cg_file C:\WORK\CGDEF.txt
  ```

### 3.10.4 EX_DRM_DB_EXPORT (export a backup record to a file)

**Format:**

For Copy Controller:
```
EX_DRM_DB_EXPORT operation-ID
```

For SQL Server or Exchange Server:
```
EX_DRM_DB_EXPORT.wsf operation-ID
```

**Description:**

This extended command executes the **drmdbexport** command to export the backup record corresponding to the specified operation ID. The backup record that was exported is recorded in the backup record file of the temporary directory for extended commands.

The backup ID is used to specify the backup record to be exported during the **drmdbexport** command execution from the backup ID file in the temporary directory for extended commands.

**Prerequisites:**

- The operation definition file corresponding to the specified operation ID has been created.
- ***Copy Controller:*** The **EX_DRM_FS_BACKUP** or **EX_DRM_TAPE_RESTORE** extended command must have been executed.

  ***SQL Server:*** The **EX_DRM_SQL_BACKUP** or **EX_DRM_TAPE_RESTORE** extended command must have been executed.

  ***Exchange Server:*** The **EX_DRM_EXG_BACKUP** or **EX_DRM_TAPE_RESTORE** extended command must have been executed.
- The backup ID to be referenced by this extended command must have been stored in the backup ID record file.

**Arguments:**

***operation-ID***

Specify the unique character string that indicates the resource to be operated. The information in the operation definition file corresponding to the specified operation ID is used for executing this extended command.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option is specified
- Information could not be acquired from the operation definition file corresponding to the operation ID
- Information could not be acquired from the host environment settings file
- The storage directory for extended command temporary files that is specified in the operation definition file does not exist
- Information could not be acquired from the backup ID file
- The command executed in the extended command failed
- The execution results of a command executed inside the extended command could not be acquired

**Example:**

To export the backup record, based on the settings in the operation definition file **operation01**:

For Copy Controller:

```
EX_DRM_DB_EXPORT operation01
```

For SQL Server or Exchange Server:

```
EX_DRM_DB_EXPORT.wsf operation01
```

### 3.10.5 EX_DRM_DB_IMPORT (import a backup record from a file)

**Format:**

For Copy Controller:
`EX_DRM_DB_IMPORT` *operation-ID*

For SQL Server or Exchange Server:
`EX_DRM_DB_IMPORT.wsf` *operation-ID*

**Description:**

This extended command executes the **drmdbimport** command to import the backup record corresponding to the specified operation ID. This extended command also generates a backup ID and records it in a backup ID file in the temporary directory for extended commands.

The backup record to be imported by executing the **drmdbimport** command is obtained from the backup record file of the temporary directory for extended commands.

**Prerequisites:**

- The operation definition file corresponding to the specified operation ID has been created.
- The backup record file to be imported by executing this extended command has been generated by executing the **EX_DRM_FTP_PUT** or **EX_DRM_FTP_GET** extended command.

**Arguments:**

***operation-ID***

Specify the unique character string that indicates the resource to be operated. The information in the operation definition file corresponding to the specified operation ID is used for executing this extended command.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option is specified
- Information could not be acquired from the operation definition file corresponding to the operation ID
- The copy source folder of the file to be copied does not exist.
- The backup ID could not be recorded in the backup ID file
- A command executed inside the extended command failed
- Information could not be acquired from the host environment settings file
- The storage directory for extended command temporary files that is specified in the operation definition file does not exist

**Example:**

To import the backup record, based on the settings in the operation definition file **operation01**:

For Copy Controller:

```
EX_DRM_DB_IMPORT operation01
```

For SQL Server or Exchange Server:

```
EX_DRM_DB_IMPORT.wsf operation01
```

### 3.10.6 EX_DRM_FS_BACKUP (back up the file system)

**Format:**

To perform online backup:

```
EX_DRM_FS_BACKUP operation-ID [ -mode online ]
```

To perform cold backup:

```
EX_DRM_FS_BACKUP operation-ID  -mode cold
```

**Description:**

This extended command backs up the file system having the specified operation ID from the primary volume to the secondary volume by executing the **drmfsbackup** command. At this time, the **EX_DRM_FS_BACKUP** command generates a backup ID.

If the data files of the specified storage group or objects such as the various databases are stored in multiple volumes, all primary volumes are backed up to the secondary volume. If you specify an inactive storage group when executing this command, the command terminates abnormally.

**Prerequisite:**

- The operation definition file corresponding to the specified operation ID is available.

**Arguments:**

***operation-ID***

Specify a unique character string identifying the resource that is to be the processing target. Information about the operation definition file corresponding to the specified operation ID is used when executing the extended command.

**-mode online**

Specify this option to perform online backup. With the online backup method, you back up a file system without unmounting it.

If you specify online backup for a file system other than VxFS, this extended command only synchronizes the file system before the online backup. To ensure consistency in the backup data, you need to suppress the updating of data before backup processing.

**-mode cold**

Specify this option to perform cold backup.

Use cold backup for a mounted file system. When executed, this extended command unmounts the specified file system and backs up the volume in the offline mode. When the backup processing is completed, the command mounts the file system again. If unmounting of the file system fails, the command displays an error message and cancels backup processing. If the target volume has already been unmounted, the command cancels backup processing.

If executed on a server with a cluster configuration, this extended command places the target disk resource in the offline mode instead of unmounting the file system, and then backs up the volume. When backup processing is completed, the command places the target disk resources in the online mode again.

Backup processing is canceled if this command is executed in the following cases:

- Placing the disk resource in the offline mode failed.
- The disk resource has already been in the offline mode.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Note:**

The backup information in the backup catalog is managed based on the copy group used as a key. Depending on the backup method, you might not be able to perform restoration, even though the backup data exists on the secondary volume.

The example is described below using the two files, which are located on separate volumes:

- File system A (copy group: **VG01,dev01**)
- File system B (copy group: **VG01,dev02**)

Use the following backup method to back up the file systems:

(a) Back up the file system A and the file system B concurrently. The backup ID **0000000001** is created.

(b) Back up the file system A only. The backup ID **0000000002** is created.

When you use the backup method 2, the backup ID **0000000002** is created, and the old backup information (backup ID: **0000000001**) about the copy group **VG01,dev01** on the file system A is deleted from the backup catalog. In other words, since the backup information about the file system B, which is included in the backup ID **0000000001**, is also deleted from the backup catalog, the file system B cannot be restored even though the backup data exists in the secondary volume. When you restore the file system B, restore the backup data obtained by using the backup method 1 from tape to the secondary volume, and then restore the backup data from the secondary volume to the primary volume.

**Conditions causing an error:**

- An invalid option was specified.
- The system failed to obtain information about the definition file corresponding to the operation ID.
- The specified Protection Services command option cannot be specified as an option of this extended command.
- The system failed to record a backup ID in the backup ID record file.
- A command executed internally terminated abnormally.
- When information collection from the host environment settings file failed
- When there is no storage directory for extended command temporary files that has been specified in the operation definition file

**Example:**

To back up the file system identified by the operation ID **operation01** from the secondary volume using the cold backup method, execute:

```
EX_DRM_FS_BACKUP operation01 -mode cold
```

### 3.10.7 EX_DRM_FS_DEF_CHECK (check contents of operation definition file)

**Format:**

To check the contents of an operation definition file on the file server:

```
EX_DRM_FS_DEF_CHECK operation-ID -db
```

To check the contents of an operation definition file on the backup server:

```
EX_DRM_FS_DEF_CHECK operation-ID -bk
```

To view the command usage:

```
EX_DRM_FS_DEF_CHECK -h
```

**Description:**

The **EX_DRM_FS_DEF_CHECK** command checks the contents of an operation definition file. It first confirms that the file specified in the argument exists and then checks the following for each item specified in the operation definition file.

- The item name and value have been specified.
- The item has been specified only once.
- The number of characters does not exceed the maximum allowable number of characters for that item.

In addition, this command checks the details listed in Table 3.20 for all items specified in the operation definition file.

**Table 3.20 Details Checked in the Operation Definition File**

| Item Name | Details to be Checked |
|---|---|
| BACKUP_OBJECT | FILESYSTEM is specified. |
| DB_SERVER_NAME | If a value of **1** is specified in **SET_DRM_HOSTNAME**, the value of **DB_SERVER_NAME** must match the file server name specified in **DRM_DB_PATH** of Protection Services environment settings file **init.conf**. |
| INSTANCE_NAME | The mount point directory specified in **INSTANCE_NAME** must exist.<br>When a mount point package definition file is specified, the file and the defined mount point should exist. |
| TARGET_NAME | The specified file or directory must exist. *<br>The file and directory which were specified are the mount point directory subordinate who specified by INSTANCE_NAME. |
| DB_DATA_FILE_DIR | ▪ The absolute path is specified.<br>▪ The specified directory must exist. *<br>▪ The lowest grade folder name is "Operation ID." |
| BK_DATA_FILE_DIR | ▪ The absolute path is specified.<br>▪ The specified directory exists. *<br>▪ In UNIX, the directory configuration is ***desired-directory*/*operation-ID***, and the subdirectory under this directory does not exist.<br>▪ In Windows, the directory configuration is ***home-directory-of-the-FTP-site**operation-ID***, and the subdirectory under this directory does not exist. |
| SET_DRM_HOSTNAME | The value 0 or 1 is specified. |

* ***Note:*** In a UNIX environment, directory names are case sensitive. In a Windows environment, directory names are not case sensitive.

**Prerequisites:**

- The command is executed on the server that contains the target file.
- The same host has the mount point directory specified in the operation definition file that is stored in the file server.

**Arguments:**

**-db**

Specify this option when you want to check the contents of an operation definition file on the file server.

**-bk**

Specify this operation when you want to check the contents of an operation definition file on the backup server.

**-f *definition-file-name***

Specify the absolute path name of the operation definition file you want to check.

**-h**

This option displays the command usage.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option was specified.
- The file specified in the argument does not exist, or the system cannot access the file.
- An error was detected when the file contents were checked.
- Access to the file server failed (applicable when the **-db** option is specified).

**Examples:**

- To check the definition file **C:\Program Files\drm\SCRIPT\conf_OP0001.dat** on the file server in a Windows environment, execute:
  ```
  EX_DRM_FS_DEF_CHECK OP0001 -db
  ```
- To check the definition file **C:\Program Files\drm\SCRIPT\conf_OP0001.dat** on the backup server in a Windows environment, execute;
  ```
  EX_DRM_FS_DEF_CHECK OP0001 -bk
  ```
- To check the definition file **/opt/drm/script/conf/_OP0001.dat** on the file server in a UNIX environment, execute:
  ```
  EX_DRM_FS_DEF_CHECK OP0001 -db
  ```
- To check the definition file **/opt/drm/script/conf/_OP0001.dat** on the backup server in a UNIX environment, execute:
  ```
  EX_DRM_FS_DEF_CHECK OP0001 -bk
  ```

### 3.10.8 EX_DRM_FS_RESTORE (restore a file system to the primary volume)

**Format:**

To resynchronize the primary and secondary volumes and then restore a file system:

```
EX_DRM_FS_RESTORE operation-ID -resync [ -force ]
                       [ -target filename-or-directory-name
                        | -f list-filename ]
```

**Description:**

This extended command restores a specified file system from its backup data from the secondary volume to the primary volume by executing the **drmfsrestore** command.

**Prerequisites:**

- The operation definition file corresponding to the specified operation ID is available.
- Before this extended command is executed, **EX_DRM_BACKUPID_SET** or **EX_DRM_DB_IMPORT** has been executed, and the backup ID has been stored in the backup ID record file.

**Arguments:**

***operation-ID***

Specify a unique character string that indicates the target resource. The information in the operation definition file that corresponds to the specified operation ID is used for the execution of this extended command.

**-resync**

Specify this option to resynchronize the primary volume and the secondary volume and then restore the file system. The backup data on the secondary volume is synchronized to the data on the primary volume.

**-force**

Specify this option to forcibly resynchronize the primary volume and the secondary volume and then restore the file system. With this option, perform forced resynchronization if the copy group name of the primary volume obtained when the backup processing was performed on the file server corresponds with the information on the file server, even though the LDEV number and the SERIAL number do not correspond with the LDEV number and the SERIAL number when the backup processing was performed.

**-target *filename-or-directory-name***

Specify this option to restore a file system that contains a specific file or directory. You can specify more than one filename or directory name by separating each by a comma. Specify the filename or directory name as the absolute path.

The specified filename or directory name must have been registered in the backup catalog. However, if the specified file or directory has already been backed up, it does not need to be registered in the backup catalog to restore the file system.

If you omit this option along with the **-f** option, the command restores the entire file system.

**-f** ***list-filename***

To restore a file system that contains multiple files or directories, use this option to specify the name of the file that contains a list of absolute path names of the files or directories. Specify the list filename as the absolute path.

If you omit this option along with the **-target** option, the command restores the entire file system.

**Note:**

- The backup information in the backup catalog is managed based on the copy group used as a key. Depending on the backup method, you might not be able to perform restoration, even though the backup data exists on the secondary volume.

  The example is described below using the two files, which are located on separate volumes:

  - File system A (copy group: **VG01,dev01**)
  - File system B (copy group: **VG01,dev02**)

  Use the following backup method to back up the file systems:

  1. Back up the file system A and the file system B concurrently. The backup ID **0000000001** is created.
  2. Back up the file system A only. The backup ID **0000000002** is created.

  When you use the backup method 2, the backup ID **0000000002** is created, and the old backup information (backup ID: **0000000001**) about the copy group **VG01,dev01** on the file system A is deleted from the backup catalog. In other words, since the backup information about the file system B, which is included in the backup ID **0000000001**, is also deleted from the backup catalog, the file system B cannot be restored even though the backup data exists in the secondary volume. When you restore the file system B, restore the backup data obtained by using the backup method 1 from tape to the secondary volume, and then restore the backup data from the secondary volume to the primary volume.

**Conditions causing an error:**

- An invalid option is specified
- The definition file information corresponding to the operation ID could not be acquired
- The specified option of a Protection Services command is not supported by this extended command
- Information could not be acquired from the backup ID record file
- A command executed inside the extended command terminated abnormally
- The execution results of a command executed inside the extended command could not be acquired
- Information could not be acquired from the host environment settings file fails
- The storage directory for extended command temporary files that is specified in the operation definition file does not exist

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Example:**

To resynchronize and then restore the file system identified by the operation definition file **operation01**, execute:

```
EX_DRM_FS_RESTORE operation01 -resync
```

### 3.10.9 EX_DRM_FTP_GET (get backup record file/metafiles from backup server)

**Format:**

For Copy Controller:

```
EX_DRM_FTP_GET operation-ID -server FTP-server
                  -user FTP-user -password FTP-password
```

For SQL Server or Exchange Server:

```
EX_DRM_FTP_GET.wsf operation-ID -server FTP-server
                  -user FTP-user -password FTP-password
```

**Description:**

This command transfers the SQL server metafiles and the backup information file corresponding to the operation ID specified from the temporary directory for extended commands on the FTP server to the temporary directory for extended commands on the FTP client. If old backup information files and SQL server metafiles exist in the target directory, those files are deleted before the files on the FTP client are transferred.

**Prerequisites:**

- The operation definition file corresponding to the specified operation ID has been created.
- This extended command must be executed on the FTP client.
- The files that this extended command will transfer have already been generated by executing the **EX_DRM_DB_EXPORT** extended command.
- The directory/folder specified in **BK_DATA_FILE_DIR** of the operation definition file was created as the file transfer source folder for the FTP server before this extended command was executed.

  If the FTP server's source directory has an invalid structure, files may be transferred from an unexpected directory.

**Arguments:**

Specify the arguments of this extended command in the following order: ***operation-ID***, **-server** ***FTP-server-name***, **-user** ***FTP-user-name***, **-password** ***FTP-password***.

***operation-ID***

Specify the unique character string that indicates the resource to be operated. The information in the operation definition file corresponding to the specified operation ID is used for executing this extended command.

**-server** ***FTP-server***

In ***FTP-server***, specify the host name of the FTP server from which you want to transfer the files.

**-user** ***FTP-user***

In ***FTP-user***, specify the FTP user name used when connecting to the FTP server.

**-password** ***FTP-password***

In ***FTP-password***, specify the FTP user password used when connecting to the FTP server.

**Note:**

In the UNIX environment, if the **LANG** value of root user and the **LANG** value of ftp service on the backup server are not equal, the **LANG** value of ftp service on the backup server must be specified as **DRM_FTP_LANG** environment value and execute this command.

If these LANG values are the same, you do not have to specify the **DRM_FTP_LANG** environment value.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option is specified
- Information could not be acquired from the operation definition file corresponding to the operation ID
- Connection to the FTP server or file transmission failed
- A command executed inside the extended command failed
- The backup information file to be transferred by this extended command does not exist
- Information could not be acquired from the host environment settings file
- The storage directory for extended command temporary files specified in the operation definition file does not exist

**Example:**

The file transmission from the FTP server to the FTP client is performed, based on the settings in the operation definition file **operation01**: The FTP server **serverA**, the FTP user **ftp_user**, and the FTP password **ftp_passwd** are used to connect in this example.

For Copy Controller:

```
EX_DRM_FTP_GET operation01 -server serverA -user ftp_user -password ftp_passwd
```

For SQL Server or Exchange Server:

```
EX_DRM_FTP_GET.wsf operation01 -server serverA -user ftp_user -password ftp_passwd
```

### 3.10.10 EX_DRM_FTP_PUT (send backup record file/metafiles to backup server)

**Format:**

For Copy Controller:

```
EX_DRM_FTP_PUT operation-ID -server FTP-server
                  -user FTP-user -password FTP-password
```

For SQL Server or Exchange Server:

```
EX_DRM_FTP_PUT.wsf operation-ID -server FTP-server
                  -user FTP-user -password FTP-password
```

**Description:**

This command transfers the SQL server metafiles and the backup information file corresponding to the operation ID specified in the arguments from the temporary directory for extended commands on the FTP client to the temporary directory for extended commands on the FTP server. If old backup information files and SQL server metafiles exist in the target folder, those files are deleted before the files on the FTP server are transferred.

**Prerequisites:**

- The operation definition file corresponding to the specified operation ID has been created.
- This extended command must be executed on the FTP client.
- The backup information file that this extended command will transfer has already been generated by executing the **EX_DRM_DB_EXPORT** extended command.
- The directory/folder specified in **BK_DATA_FILE_DIR** of the operation definition file was created as the file transfer destination directory/folder for the FTP server before this extended command is executed.

  If the FTP server's target directory has an invalid structure, files may be transferred to an unexpected directory.

**Arguments:**

Specify the arguments of this extended command in the following order: ***operation-ID***, **-server** ***FTP-server-name***, **-user** ***FTP-user-name***, **-password** ***FTP-password***.

***operation-ID***

Specify the unique character string that indicates the resource to be operated. The information in the operation definition file corresponding to the specified operation ID is used for executing this extended command.

**-server** ***FTP-server***

In ***FTP-server***, specify the host name of the FTP server to which you want to transfer the files.

**-user** ***FTP-user***

In ***FTP-user***, specify the FTP user name used when connecting to the FTP server.

**-password** ***FTP-password***

In ***FTP-password***, specify the FTP user password used when connecting to the FTP server.

**Note:**

In the UNIX environment, if the **LANG** value of root user and the **LANG** value of ftp service on the backup server are not equal, the **LANG** value of ftp service on the backup server must be specified as **DRM_FTP_LANG** environment value and execute this command.

If these LANG values are the same, you do not have to specify the **DRM_FTP_LANG** environment value.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option is specified
- Information could not be acquired from the operation definition file corresponding to the operation ID
- Connection to the FTP server or file transmission failed
- A command executed inside the extended command failed
- The backup information file to be transferred by this extended command does not exist
- Information could not be acquired from the host environment settings file
- The storage directory for extended command temporary files specified in the operation definition file does not exist

**Example:**

The file transfer from the FTP client to the FTP server is performed, based on the settings in the operation definition file **operation01**. The FTP server **serverA**, the FTP user **ftp_user**, and the FTP password **ftp_passwd** are used to connect in this example.

For Copy Controller:
```
EX_DRM_FTP_PUT operation01 -server serverA -user ftp_user -password ftp_passwd
```

For SQL Server or Exchange Server:
```
EX_DRM_FTP_PUT.wsf operation01 -server serverA -user ftp_user -password ftp_passwd
```

### 3.10.11 EX_DRM_HOST_DEF_CHECK (check contents of host env. settings file)

**Format:**

To check the contents of a host environment settings file on the file server:
```
EX_DRM_HOST_DEF_CHECK -db -f environment-settings-filename
```

To check the contents of a host environment settings file on the database server:
```
EX_DRM_HOST_DEF_CHECK.wsf -db -f environment-settings-filename
```

To check the contents of a host environment settings file on the backup server:

For Copy Controller:
```
EX_DRM_HOST_DEF_CHECK -bk -f environment-settings-filename
```

For SQL Server or Exchange Server:
```
EX_DRM_HOST_DEF_CHECK.wsf -bk -f environment-settings-filename
```

To display help for the use of this extended command:

For Copy Controller:
```
EX_DRM_HOST_DEF_CHECK -h
```

For SQL Server or Exchange Server:
```
EX_DRM_HOST_DEF_CHECK.wsf -h
```

**Description:**

This extended command checks the contents of the host environment settings file. First, this extended command checks whether the specified file exists. Then, when the file exists, this extended command checks the contents of the **HOST_ROLE** and **MAX_LOG_LINES** entries in the host environment settings file for the settings shown in

Table 3.21.

**Table 3.21 Items Checked for the Host Environment Settings File**

| Item | Items Checked |
|---|---|
| HOST_ROLE | ▪ The item name and a value are specified.<br>▪ Only one item is specified.<br>▪ The number of characters does not exceed the maximum for the item.<br>▪ If the **-db** argument is specified in the extended command, **DB** is specified in the item.<br>▪ If the **-bk** argument is specified in the extended command, **BK** is specified in the item. |
| MAX_LOG_LINES | ▪ The item name and a value are specified.<br>▪ Only one item is specified.<br>▪ The number of characters does not exceed the maximum for the item.<br>▪ The specified value is an integer in the range from 1,000 to 100,000. |

**Prerequisite:**

This extended command must be executed on the machine that contains the host environment settings file to be checked.

**Arguments:**

**-db**

Specify this option to check the contents of a host environment settings file on the file or database server.

**-bk**

Specify this option to check the contents of a host environment settings file on the backup server.

**-f *environment-settings-file-name***

In ***file-name***, specify the absolute path name of the host environment settings file you want to check.

**-h**

Specify this option to display help for the usage of this extended command.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option was specified
- The file specified in the argument does not exist, or the system cannot access the file
- The check of the contents of the file for setting up the host environment detected an abnormality

**Examples for UNIX:**

- To check the contents of the host environment settings file **/opt/drm/script/conf/host.dat** on the file server, execute:
  ```
  EX_DRM_HOST_DEF_CHECK -db  -f /opt/drm/script/conf/host.dat
  ```
- To check the contents of the host environment settings file **/opt/drm/script/conf/host.dat** on the backup server, execute:
  ```
  EX_DRM_HOST_DEF_CHECK -bk  -f /opt/drm/script/conf/host.dat
  ```

**Examples for Windows:**

- To check the contents of the host environment settings file **C:\Program Files\drm\SCRIPT\conf\host.dat** on the file or database server, execute:

  For Copy Controller:
  ```
  EX_DRM_HOST_DEF_CHECK -db -f "C:\Program Files\drm\SCRIPT\conf\host.dat"
  ```

  For SQL Server or Exchange Server:
  ```
  EX_DRM_HOST_DEF_CHECK.wsf -db -f "C:\Program Files\drm\SCRIPT\conf\host.dat"
  ```
- To check the contents of the host environment settings file **C:\Program Files\drm\SCRIPT\conf\host.dat** on the backup server, execute:

  For Copy Controller:
  ```
  EX_DRM_HOST_DEF_CHECK -bk -f "C:\Program Files\drm\SCRIPT\conf\host.dat"
  ```

  For SQL Server or Exchange Server:
  ```
  EX_DRM_HOST_DEF_CHECK.wsf -bk -f "C:\Program Files\drm\SCRIPT\conf\host.dat"
  ```

### 3.10.12 EX_DRM_RESYNC (resynchronize a copy group)

**Format:**

To resynchronize the copy group in the always-paired mode:

For Copy Controller:
```
EX_DRM_RESYNC operation-ID [ -copy_size copy-track-size ]
```

For SQL Server or Exchange Server:
```
EX_DRM_RESYNC.wsf operation-ID [ -copy_size copy-track-size ]
```

To resynchronize more than one copy group in the always-split mode:

For Copy Controller:
```
EX_DRM_RESYNC operation-ID
                    { -cg copy-group | -cg_file copy-group-list-file }
                      [ -copy_size copy-track-size ]
```

For SQL Server or Exchange Server:
```
EX_DRM_RESYNC.wsf operation-ID
                    { -cg copy-group | -cg_file copy-group-list-file }
                      [ -copy_size copy-track-size ]
```

**Description:**

This command executes the **drmresync** command and resynchronizes copy groups. Executing this extended command before you back up the file system or database to the secondary volume enhances the speed of backup processing.

In the always-paired mode, the specified copy group is resynchronized based on the backup ID created when data is backed up from the primary volume to the secondary volume. In the always-split mode, you must resynchronize the copy group before backing up the data. Select the copy group to be resynchronized from the execution results of the **drmcgctl** or **drmfscat** command.

However, if there are copy groups that are not used for the backup, those copy groups are specified automatically. If no copy groups are used, the first copy group in order that was defined as a pair is specified.

When all copy groups are used for the backup, the copy groups are specified beginning with the first copy group to be backed up.

**Prerequisites:**

- The operation definition file corresponding to the specified operation ID has been created.
- The copy group list file has already been created when copy groups are resynchronized by using the copy group list file.
- ***Copy Controller:*** In the always-paired mode, the file system was backed up to the secondary volume using **EX_DRM_FS_BACKUP**, and the backup ID record file has already been created.

  ***SQL Server:*** In the always-paired mode, the SQL Server database was backed up to the secondary volume using **EX_DRM_SQL_BACKUP**, and the backup ID file has already been created.

  ***Exchange Server:*** In the always-paired mode, the Exchange Server database was backed up to the secondary volume using **EX_DRM_EXG_BACKUP**, and the backup ID file has already been created.

**Arguments:**

Specify the arguments of this extended command in the following order: ***operation-ID***, **-cg** ***copy-group-name***, **-cg_file** ***copy-group-list-file***, **-copy_size** ***copy-track-size***.

***operation-ID***

Specify the unique character string that indicates the resource to be operated. The information in the operation definition file corresponding to the specified operation ID is used for executing this extended command.

**-cg** ***copy-group***

In the always-split mode, specify the name of a copy group you want to resynchronize. Specify the copy group to be used at the next backup.

**-cg_file** ***copy-group-list-file***

In the always-split mode, specify the absolute path name of the copy group list file that contains the copy group you want to resynchronize. Use this item if you want to resynchronize many copy groups all at one time. Specify the copy group to be used at the next backup.

**-copy_size** ***copy-track-size***

In copy-track-size, specify a numeric value (range from 1 to 15) as the copy track size to be used for copy group resynchronization. If you do not specify this option, the extended command uses the copy track size specified in the **DRM_COPY_SIZE** environment variable of Protection Services.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option is specified
- Information could not be acquired from the operation definition file corresponding to the operation ID
- Information could not be acquired from the backup ID file (when no copy group is specified)
- Information could not be acquired from the copy group list file (when the file was specified)
- An invalid copy track size is specified
- A command executed inside the extended command failed
- The execution results of a command executed inside the extended command could not be acquired
- Information could not be acquired from the host environment settings file
- The storage directory for extended command temporary files that is specified in the operation definition file does not exist

**Examples:**

- To resynchronize the pair volume of the copy group **CG001,dev01**, execute:

  For Copy Controller:
  ```
  EX_DRM_RESYNC operation01 -cg CG001,dev01
  ```

  For SQL Server or Exchange Server:
  ```
  EX_DRM_RESYNC.wsf operation01 -cg CG001,dev01
  ```

- In a UNIX environment, to resynchronize the pair volumes of the copy group specified in the list file **/var/opt/drm/script/tmp/operation01/CGLIST.txt** in batch mode, execute:
  ```
  EX_DRM_RESYNC operation01 -cg_file
  /var/opt/drm/script/tmp/operation01/CGLIST.txt
  ```

-

- In a Windows environment, to resynchronize the pair volumes of the copy group specified in the list file **C:\temp\CGLIST.txt** in batch mode, execute:

  For Copy Controller:
  ```
  EX_DRM_RESYNC operation01 -cg_file C:\temp\CGLIST.txt
  ```

  For SQL Server or Exchange Server:
  ```
  EX_DRM_RESYNC.wsf operation01 -cg_file C:\temp\CGLIST.txt
  ```

- To resynchronize the pair volume of the copy group corresponding to the backup ID recorded in the backup ID file, execute:

  For Copy Controller:
  ```
  EX_DRM_RESYNC operation01
  ```

  For SQL Server or Exchange Server:
  ```
  EX_DRM_RESYNC.wsf operation01
  ```

### 3.10.13 EX_DRM_TAPE_BACKUP (back up secondary vol. data/metafiles to tape)

**Format:**

In UNIX:
```
EX_DRM_TAPE_BACKUP operation-ID
                [ -exopt [ -mount_pt mount-point-directory-name | -raw]
                  [ -force ] ]
```

In Windows:
```
EX_DRM_TAPE_BACKUP operation-ID
                  [ -exopt [ -mount_pt mount-point-directory-name ]
                   [ -raw ][ -force ] ]
```

You can also use the following command for Exchange Server:
```
EX_DRM_TAPE_BACKUP operation-ID
                   [ [ -mount_pt mount-point-directory-name ][ -raw ] ]
```

**Description:**

This extended command executes the **drmmount**, **drmmediabackup**, and **drmumount** commands, mounts the secondary volume at a specific mount point on the backup server, and backs up data from the secondary volume to a tape. When the tape backup is complete, the secondary volume is automatically unmounted. Regardless of the result of the **drmmediabackup** command, if the **drmmount** command ended normally, the **drmumount** command will be executed.

**Prerequisites:**

- The operation definition file corresponding to the specified operation ID has been created.
- The backup management product is used with Protection Services.
- The backup ID has been stored in the backup ID file by executing the **EX_DRM_DB_IMPORT** extended command.
- The mount point directory has been created.

**Arguments:**

***operation-ID***

Specify the unique character string that indicates the resource to be operated. The information in the operation definition file corresponding to the specified operation ID is used for executing this extended command.

**-exopt**

Specify this option in order to specify the **-mount_pt**, **-raw**, and **-force** options. Specify the **-mount_pt**, **-raw**, and **-force** options in this order.

**-mount_pt** ***mount-point-directory-name***

Specify the name of the mount point directory on which the secondary volume is to be mounted. The secondary volume is mounted at the specified mount point, and data is backed up from the secondary volume to a tape. If you are executing this extended command in a UNIX environment, this option and the **-raw** option are mutually exclusive.

**In UNIX:**

If the specified mount point directory name is **/**, the extended command mounts the secondary volume at the mount point used for the secondary volume.

Specify the mount point directory name as an absolute path name with a length of less than 255 bytes. Note that you cannot use any of the following special characters: \ / : . * ? “ < > |

When this option is omitted, the extended command mounts the secondary volume on **/var/opt/drm/mnt**.

**In Windows:**

Specify the drive letter or the absolute path for the drive letter.

When only the drive name is specified, this command searches for unused drives in the alphabetical order from the specified drive, and then mounts the drive.

If a path including a drive letter is specified, the extended command mounts the secondary volume on ***path-specified-in*-mount_pt*drive-character-of-primary-volume**mount-point-of-primary-volume***.

For example, if the primary volume is mounted on **M:\MNT**, and **S:\SVOLMNT** is specified in **-mount_pt**, then the extended command mounts the secondary volume on **S:\SVOLMNT\M\MNT**.

Specify the mount point directory name as an absolute path name of 64 bytes or less. Note that you cannot use the space character and any of the following special characters: \ / : . * ? “ < > |

When this option is omitted, the secondary volume is mounted on a drive not used during extended command execution.

**-raw**

Specify this option when you want to back up the secondary volume as a raw device. When this extended command backs up the secondary volume as a raw device, this extended command does not mount the secondary volume and performs a backup for each logical volume. When this extended command is executed in a UNIX environment, this option and the **-mount_pt** option are mutually exclusive.

When this option is omitted, the secondary volume is backed up as a file system (for Copy Controller) or database. In a UNIX environment, if this option is not specified and raw data, file system data, and/or database data coexist on the secondary volume to be backed up, raw volume data is backed up as a raw device, file system data is backed up as a file system, and database data is backed up as a database.

**-force**

***WARNING:*** Data may be damaged if you specify this option during normal backup operation.

Specify this option to execute the mount operation forcibly. When the copy group name of the primary volume acquired during backup of the file/database server matches the file/database server information, the secondary volume is forcibly mounted, even if the LDEV or SERIAL number does not match.

If this option is omitted and the LDEV number, SERIAL number, or the copy group name of the primary volume acquired during backup of the file/database server does not match the file server information, the extended command terminates abnormally without mounting the secondary volume.

Specify this option in a case such as when the secondary volume is replaced for a reason such as a failure or when the LDEV number or SERIAL number was changed and it is necessary to forcibly mount only the copy group name of the primary volume onto the secondary volume as a key. Data may be damaged if you specify this option during normal backup operation.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option is specified
- Information could not be acquired from the operation definition file corresponding to the operation ID
- The arguments of this extended command include an option of a Protection Services command that cannot be used for this extended command
- Information could not be acquired from the backup ID file
- A command executed inside the extended command failed
- The execution results of a command executed inside the extended command could not be acquired
- Information could not be acquired from the host environment settings file
- The storage direcotry for extended command temporary files that is specified in the operation definition file does not exist

**Examples:**

- To back up the secondary volume as a raw device, based on the settings in the operation definition file **operation01**, execute:
  ```
  EX_DRM_TAPE_BACKUP operation01 -exopt -raw
  ```
- To forcibly mount the secondary volume identified by the operation ID **operation01** and execute tape backup, execute:
  ```
  EX_DRM_TAPE_BACKUP operation01 -exopt -force
  ```

### 3.10.14 EX_DRM_TAPE_RESTORE (restore data from backup tape to S-VOL)

**Format:**

In UNIX:

```
EX_DRM_TAPE_RESTORE operation-ID -backup_id backup-ID
                [ -exopt [ -mount_pt mount-point-directory-name ]
                [ -raw ]
                [ -force ] ]
```

In Windows:

```
EX_DRM_TAPE_RESTORE operation-ID -backup_id backup-ID
               [ -exopt [ -mount_pt mount-point-directory-name ]
               [ -raw ]
               [ -force ] ]
```

You can also use the following command for Exchange Server:

```
EX_DRM_TAPE_RESTORE operation-ID -backup_id backup-ID
               [ -mount_pt mount-point-directory-name][ -raw ]
```

**Description:**

This extended command executes the **drmmount**, **drmmediarestore**, and **drmumount** commands and restores backup data and SQL Server metafiles from tape to the secondary volume. The extended command also creates a backup ID record file containing the backup ID. Regardless of the result of the **drmmediabackup** command, if the **drmmount** command ended normally, the **drmumount** command will be executed.

In the environment using VERITAS Backup Exec, when you execute **EX_DRM_TAPE_RESTORE**, the **drmmediarestore** command is executed, and then the window starts. The status of the window starting the extended command is **WAIT**. Check the following message displayed in the window to restore the backup data.

After restoration, enter one of the following keywords:

- **YES** (finishes successfully)
- **NO** (finishes abnormally)
- **CANCEL** (cancels the operation)

Enter the correct password after the restore operation finishes by using VERITAS Backup Exec.

When the **drmmediarestore** command finishes, the command prompt will close. By using the command prompt starting the extended command, execute the subsequent operations.

**Prerequisites:**

- The operation definition file corresponding to the specified operation ID has been created.
- The backup management product is used with Protection Services.
- The backup ID to be specified in this extended command has already been determined by executing the **drmtapecat** command.
- The mount point directory has been created.

**Arguments:**

***operation-ID***

Specify the unique character string that indicates the resource to be operated. The information in the operation definition file corresponding to the specified operation ID is used for executing this extended command.

**-backup_id *backup-ID***

In ***backup-ID***, specify the backup ID of the backup you want to use for restoration. The backup ID is a unique ID to identify backup data and registered in the backup catalog during backup. To check the desired backup ID, execute the **drmtapecat** command.

**-exopt**

Specify this option in order to specify the **-mount_pt**, **-raw**, and/or **-force** options. Specify the **-mount_pt**, **-raw**, and **-force** options in this order.

**-mount_pt** ***mount-point-directory-name***

Specify the name of the mount point directory on which the secondary volume is to be mounted. The secondary volume is mounted at the specified mount point, and data is backed up from the secondary volume to a tape.

**In UNIX:**

If the specified mount point directory name is **/**, the extended command mounts the secondary volume at the mount point used for the secondary volume.

Specify the mount point directory name as an absolute path with a length of less than 255 bytes. Note that you cannot use any of the following special characters: \ / : . * ? “ < > |

This option and the **-raw** option are mutually exclusive.

When this option is omitted, the extended command mounts the secondary volume at **/var/opt/drm/mnt**.

**In Windows:**

Specify the drive letter or the absolute path from the drive letter.

When only the drive name is specified, this command searches for unused drives in the alphabetical order from the specified drive, and then mounts the drive.

If a path including a drive letter is specified, the extended command mounts the secondary volume on ***path-specified-in*-mount_pt*drive-letter-of-primary-volume**mount-point-of-primary-volume***.

For example, if the primary volume is mounted on **M:\MNT**, and **S:\SVOLMNT** is specified in **-mount_pt**, then the extended command mounts the secondary volume on **S:\SVOLMNT\M\MNT**.

Specify the mount point directory name as an absolute path name of 64 bytes or less. Note that you cannot use the space character and any of the following special characters: \ / : . * ? “ < > |

When this option is omitted, the secondary volume is mounted on a drive not used during extended command execution.

**-raw**

Specify this option if the target data to be restored was backed up to tape as raw device data.

If the data to be restored was backed up by specifying **EX_DRM_TAPE_RESTORE** with the **-raw** option, the data will be restored successfully even if you do not specify this option. If the data to be restored was backed up without specifying the **-raw** option, the extended command terminates abnormally when you specify this option.

When this extended command is executed in a UNIX environment, this option and the **-mount_pt** option are mutually exclusive.

**-force**

***WARNING:*** Data may be damaged if you specify this option for normal backup processing.

Specify this option in order to execute the mount operation forcibly. If the copy group name of the primary volume acquired when executing backup on the file/database server matches the information on the file/database server, the secondary volume is mounted forcibly even if the LDEV number or SERIAL number do not match.

If this option is omitted and the LDEV number, SERIAL number, or the copy group name of the primary volume acquired during backup of the file/database server does not match the file/database server information, the extended command terminates abnormally without mounting the secondary volume.

Specify this option when you need to forcibly mount the secondary volume only using the copy group name of the primary volume as the key, such as when the secondary volume has been replaced for reasons such as errors or a change in the LDEV number or SERIAL number. Data may be damaged if you specify this option for normal backup processing.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option is specified
- Information could not be acquired from the operation definition file corresponding to the operation ID
- The arguments of this extended command include an option of a Protection Services command that cannot be used for this extended command
- The backup ID could not be recorded in the backup ID file
- A command executed inside the extended command failed
- The execution results of a command executed inside the extended command could not be acquired
- Information could not be acquired from the host environment settings file
- The storage directory for extended command temporary files that is specified in the operation definition file does not exist

**Examples:**

- To restore the backup data identified by the operation ID **operation01** from a tape to the secondary volume:

  ***In UNIX:*** **0000000001** is the backup ID that was created when this data was backed up to tape. The secondary volume is mounted on the drive **/mnt1**.

  ```
  EX_DRM_TAPE_RESTORE operation01 -backup_id 0000000001 -exopt -mount_pt /mnt1
  ```

  ***In Windows:*** **0000000001** is the backup ID that was created when this data was backed up to tape. The secondary volume is mounted on the drive **E:**.

  ```
  EX_DRM_TAPE_RESTORE operation01 -backup_id 0000000001 -exopt -mount_pt E:
  ```

- To restore the backup data identified by the operation ID **operation01** from a tape to the secondary volume by forcibly mounting it at the specified mount point:

  ***In UNIX:*** **0000000001** is the backup ID that was created when this data was backed up to tape. The secondary volume is mounted on the drive **/mnt1**.

  ```
  EX_DRM_TAPE_RESTORE operation01 -backup_id 0000000001 -exopt -mount_pt /mnt1
  -force
  ```

  ***In Windows:*** **0000000001** is the backup ID that was created when this data was backed up to tape. The secondary volume is mounted on the drive **E:**.

  ```
  EX_DRM_TAPE_RESTORE operation01 -backup_id 0000000001 -exopt -mount_pt E:
  -force
  ```

## 3.11 Extended Command Specifications (SQL Server only)

This section provides the specifications for the following extended commands for Protection Services for SQL Server:

3.11.1 EX_DRM_SQL_BACKUP (back up the file system)

3.11.2 EX_DRM_SQL_DEF_CHECK (check the operation definition file)

3.11.3 EX_DRM_SQL_RESTORE (restore SQL Server database to primary volume)

3.11.4 EX_DRM_SQL_TLOG_BACKUP (back up the SQL Server transaction log)

3.11.5 EX_DRM_SQLFILE_EXTRACT (deploy the SQL Server metafiles)

3.11.6 EX_DRM_SQLFILE_PACK (back up the SQL Server metafiles)

### 3.11.1 EX_DRM_SQL_BACKUP (back up the file system)

**Format:**

```
EX_DRM_SQL_BACKUP.wsf operation-ID [ -system ]
```

**Description:**

This extended command executes the **drmsqlbackup** command to back up the SQL Server database of the instance that was specified by the operation ID from the primary volume to the secondary volume. When this extended command performs a backup, a backup ID is generated.

If the data files, databases, and other objects of the resolved instance exist on multiple volumes, all the primary volumes for them will be backed up to the secondary volumes. When the SQL Server instance is backed up, online backup is performed. The command fails when the instance that is not running is specified.

**Prerequisite:**

- The operation definition file corresponding to the specified operation ID is available.

**Arguments:**

***operation-ID***

Specify the unique character string that indicates the resource to be operated. The information in the operation definition file corresponding to the specified operation ID is used for executing this extended command.

**-system**

Use this option to specify the system database as the database you want to back up. When this option is used, SQL Server is terminated during backup.

If this option is specified when the database name is specified in **TARGET_NAME** of the operation definition file that corresponds to the specified operation ID, the extended command terminates abnormally.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Note:**

The backup information in the backup catalog is managed based on the copy group used as a key. Depending on the backup method, you might not be able to perform restoration, even though the backup data exists on the secondary volume.

The example is described below using the two databases, which are located on separate volumes:

- Database A (copy group: **VG01,sql01**)
- Database B (copy group: **VG01,sql01**)

Use one of the following backup methods to back up the databases:

1. Back up databases A and B concurrently. The backup ID **0000000001** is created.
2. Back up database A only. The backup ID **0000000002** is created.

When you use backup method 2, backup ID **0000000002** is created, and the old backup information (backup ID: **0000000001**) about copy group **VG01,sql01** on database A is deleted from the backup catalog. In other words, since the backup information about database B, which is included in backup ID **0000000001**, is also deleted from the backup catalog, database B cannot be restored even though the backup data exists in the secondary volume. When you restore database B, restore the backup data obtained by using backup method 1 from tape to the secondary volume, and then restore the backup data from the secondary volume to the primary volume.

**Conditions causing an error:**

- An invalid option is specified
- Information could not be acquired from the operation definition file corresponding to the operation ID
- The Protection Services command option that cannot be specified as an option of this extended command is specified
- The backup ID could not be recorded in the backup ID file
- A command executed inside the extended command failed

**Example:**

- To back up from the system database to the secondary volume, based on the settings in the operation definition file operation01, execute:
  ```
  EX_DRM_SQL_BACKUP.wsf operation01 -system
  ```

### 3.11.2 EX_DRM_SQL_DEF_CHECK (check the operation definition file)

**Format:**

To check the contents of an operation definition file on the database server, use:
`EX_DRM_SQL_DEF_CHECK.wsf -db -f definition-file-name`

To check the contents of an operation definition file on the backup server, use:
`EX_DRM_SQL_DEF_CHECK.wsf -bk -f definition-file-name`

To display help for the use of this extended command, use:
`EX_DRM_SQL_DEF_CHECK.wsf -h`

**Description:**

This extended command checks the contents of the operation definition file. First, this extended command checks whether the specified file exists. Then, when the file exists, this extended command checks the following contents in the operation definition file:

- Whether an item name and a value are specified
- Whether only one item is specified
- Whether the number of specified characters does not exceed the maximum

Table 3.22 lists and describes the items in the operation definition file that are checked.

**Prerequisites:**

- The user account of the user currently logged into Windows must allow connection to the database server.
- The SQL Server service is running on the database server.
- The SQL Server instance specified in the file you want to check exists on a host when the command is executed on the database server.
- Queries can be issued to the databases in the same SQL Server instance when the command is executed on the 2.
- The initial settings for the instance specified in **INSTANCE_NAME** have been specified by executing the **drmsqlinit** command.

**Arguments:**

**-db**

Specify this option to check the contents of the operation definition file on the database server.

**-bk**

Specify this option to check the contents of the operation definition file on the backup server.

**-f *definition-file-name***

Specify the absolute path name of the operation definition file you want to check.

**-h**

Specify this option to display help for the usage of this extended command.

**Table 3.22 Items Checked in the Operation Definition File**

| Entry Name | Checked Contents |
|---|---|
| BACKUP_OBJECT | Whether MSSQL is specified |
| DB_SERVER_NAME | ▪ Whether the database connection can be established by executing a combination of **DB_SERVER_NAME** and **INSTANCE_NAME**<br>▪ Whether the value of **DB_SERVER_NAME** matches the database server name set in **DRM_DB_PATH** of the Protection Services environment settings file **init.conf** when **1** is specified to **SET_DRM_HOSTNAME** |
| INSTANCE_NAME | Whether the database connection can be established by executing a combination of **DB_SERVER_NAME** and **INSTANCE_NAME** |
| TARGET_NAME | ▪ Whether the database name exists (by checking the contents of the sysdatabases table in the master database) *<br>▪ Whether the tempdb database is included in the databases to be backed up |
| AP_FILE_DIR | ▪ Whether the absolute path is specified<br>▪ Whether the specified folder exists<br>▪ Whether the specification of this entry matches the value of **VDI_METAFILE_DIR** in the environment settings file on the database server *<br>▪ Whether this entry is set to a different value than the value set to **DB_DATA_FILE_DIR** in the case of the operation definition on the database server<br>▪ Whether this entry is set to a different value than the value set to **BK_DATA_FILE_DIR** in the case of the operation definition file on the backup server |
| DB_DATA_FILE_DIR | ▪ Whether the absolute path is specified<br>▪ Whether the specified folder exists *<br>▪ Whether this entry is set to a different value than the value set to **AP_FILE_DIR** |
| BK_DATA_FILE_DIR | ▪ Whether the absolute path is specified<br>▪ Whether the specified folder exists *<br>▪ Whether the configuration of the specified folder is home-directory-of-the-FTP-site/database-server-name\instance-nameand there are no subfolders under this folder<br>▪ Whether this entry is set to a different value than the value set to **AP_FILE_DIR** |
| SET_DRM_HOSTNAME | Whether the value is either 0 or 1 |

* Database and folder names are not case sensitive.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- When an invalid option is specified.
- When the file specified in the argument does not exist, or the system cannot access the file.
- When the system cannot access the database server (when the **-db** option is specified).
- When the system detects an error in the results of the file check.

**Examples:**

To check the contents of the operation definition file **C:\Program Files\drm\SCRIPT\conf_OP0001.dat** on the database server, execute:

```
EX_DRM_SQL_DEF_CHECK.wsf -db -f "C:\Program Files\drm\script\conf\_OP0001.dat"
```

To check the contents of the operation definition file **C:\Program Files\drm\SCRIPT\conf_OP0001.dat** on the backup server, execute:

```
EX_DRM_SQL_DEF_CHECK.wsf -bk -f "C:\Program Files\drm\script\conf\_OP0001.dat"
```

### 3.11.3 EX_DRM_SQL_RESTORE (restore SQL Server DB to primary volume)

**Format:**

To restore the primary volume by resynchronizing it with the secondary volume, use:

```
EX_DRM_SQL_RESTORE.wsf operation-ID -resync [ -force ] [ -undo ]
                       [ -target database(s) | -f database-list-file ]
```

To apply only metafiles to the primary volume, use:

```
EX_DRM_SQL_RESTORE.wsf operation-ID -no_resync [ -undo ]
                       [ -target database(s) | -f database-list-file ]
```

**Description:**

This extended command executes the **drmsqlrestore** command to restore the backup data in the specified database from the secondary volume to the primary volume.

**Prerequisites:**

- The operation definition file corresponding to the specified operation ID has been created.
- The backup ID has been stored in the backup ID file by executing the **EX_DRM_BACKUPID_SET** or **EX_DRM_DB_IMPORT** extended command.

**Arguments:**

***operation-ID***

Specify the unique character string that indicates the resource to be operated. The information in the operation definition file corresponding to the specified operation ID is used for executing this extended command.

**-resync**

Specify this option to restore the primary volume by resynchronizing it with the secondary volume. The backup data in the secondary volume is synchronized to the primary volume.

**-no_resync**

Specify this option if you want to apply only metafiles to the primary volume without restoring the backup data from the secondary volume to the primary volume. Specify this option when you want to restore data without using the **drmsqlrestore** command.

**-force**

Specify this option to restore the primary volume by forcibly resynchronizing it with the secondary volume. With this option, perform forced resynchronization if the copy group name of the primary volume obtained when the backup processing was performed on the database server corresponds with the information on the database server, even though the LDEV number and the SERIAL number do not correspond with the LDEV number and the SERIAL number when the backup processing was performed. Use this option only when the restore operation cannot be performed by the resynchronization even though the **-resync** option is specified, for example, when the LDEV number was changed by LDEV replacement. Specifying this option while performing a normal restoration may damage the data.

**-undo**

Specify this option to restore the database in the standby mode. When this option is specified, the database can be used in the read-only mode after restoration. A temporary file is created for each database in the undo-log file storage directory registered by using the **drmsqlinit** command.

If this option is not specified, this extended command performs normal restoration. Immediately after normal restoration, the database will be placed in the loading status, in which you cannot use the database.

**-target *database(s)***

Specify this option to restore the instance(s) containing the specified database(s). The database(s) you specify must be found in the backup catalog specified by the backup ID. If you specify a database not found in that backup catalog, this extended command does not restore the database. When you want to specify more than one database, use a comma to separate each file or directory name.

If you specify neither this option nor the **-f** option, this extended command restores the entire instance specified by the backup ID.

**-f *database-list-file***

In the same way as the **-target** option, specify this option to restore the instance(s) containing the specified database(s). Unlike **-target**, this option uses an argument that is the name of a file that contains a list of databases you want to restore. This list file must be created beforehand. In ***database-list-file***, specify the absolute path name of the list file.

If you specify neither this option nor the **-target** option, this extended command restores all the objects contained in the instance specified by the backup ID.

**Note:**

The backup information in the backup catalog is managed based on the copy group used as a key. Depending on the backup method, you might not be able to perform restoration, even though the backup data exists on the secondary volume.

The example is described below using two databases which are located on separate volumes:

- Database A (copy group: **VG01,sql01**)
- Database B (copy group: **VG01,sql01**)

Use the following backup method to back up the databases:

1. Back up database A and database B concurrently. The backup ID **0000000001** is created.
2. Back up database A only. The backup ID **0000000002** is created.

When you use backup method 2, backup ID **0000000002** is created, and the old backup information (backup ID: **0000000001**) about copy group **VG01,sql01** on database A is deleted from the backup catalog. In other words, since the backup information about database B, which is included in backup ID **0000000001**, is also deleted from the backup catalog, database B cannot be restored even though the backup data exists in the secondary volume. When you restore database B, restore the backup data obtained by using backup method 1 from tape to the secondary volume, and then restore the backup data from the secondary volume to the primary volume.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- This extended command fails in the following cases:
- An invalid option is specified
- Information could not be acquired from the operation definition file corresponding to the operation ID
- The Protection Services command option that cannot be specified as an option of this extended command is specified
- Information could not be acquired from the backup ID file
- A command executed inside the extended command failed

**Examples:**

To restore the primary volume by resynchronizing the primary volume with the secondary volume, based on the settings in the operation definition file **operation01**, execute:

```
EX_DRM_SQL_RESTORE.wsf operation01 -resync
```

### 3.11.4 EX_DRM_SQL_TLOG_BACKUP (back up the SQL Server transaction log)

**Format:**

```
EX_DRM_SQL_TLOG_BACKUP.wsf operation-ID
```

**Description:**

This extended command executes the **drmsqllogbackup** command to back up the SQL Server transaction log corresponding to the specified operation ID.

**Prerequisite:**

The operation definition file corresponding to the specified operation ID has been created.

**Argument:**

***operation-ID***

Specify the unique character string that indicates the resource to be operated. The information in the operation definition file corresponding to the specified operation ID is used for executing this extended command.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option is specified
- Information could not be acquired from the operation definition file corresponding to the operation ID
- A command executed inside the extended command failed

**Examples:**

To back up the transaction log for the resource, based on the settings in the operation definition file **operation01**, execute:

```
EX_DRM_SQL_TLOG_BACKUP.wsf operation01
```

### 3.11.5 EX_DRM_SQLFILE_EXTRACT (deploy the SQL Server metafiles)

**Format:**

```
EX_DRM_SQLFILE_EXTRACT.wsf operation-ID
```

**Description:**

This extended command copies the SQL Server metafiles from the temporary folder for extended commands to the folder specified in the **AP_FILE_DIR** entry of the operation definition file corresponding to the operation ID.

When this extended command is executed on the backup server, this extended command first deletes all the SQL Server metafiles from the copy destination folder. Then, this extended command copies the SQL Server metafiles from the copy source folder to the copy destination folder. By deleting old metafiles, this extended command prevents old metafiles from being backed up to a tape.

On the database server, all the SQL Server metafiles generated when the database is backed up to the secondary volume are protected. Therefore, if this extended command is executed on the database server, the SQL Server metafiles are not deleted.

**Prerequisites:**

- The operation definition file corresponding to the specified operation ID has been created.
- The backup ID file from which this extended command will acquire information has been generated by executing the **EX_DRM_BACKUPID_SET** or **EX_DRM_DB_IMPORT** extended command.

**Argument:**

*operation-ID*

Specify the unique character string that indicates the resource to be operated. The information in the operation definition file corresponding to the specified operation ID is used for executing this extended command.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option is specified
- Information could not be acquired from the operation definition file corresponding to the operation ID
- The copy destination folder for the target file does not exist
- Information could not be acquired from the backup ID file
- A command executed inside the extended command failed

**Example:**

To deploy the SQL Server metafiles, based on the settings in the operation definition file **operation01**, execute:

```
EX_DRM_SQLFILE_EXTRACT.wsf operation01
```

### 3.11.6 EX_DRM_SQLFILE_PACK (back up the SQL Server metafiles)

**Format:**

```
EX_DRM_SQLFILE_PACK.wsf operation-ID
```

**Description:**

This extended command backs up the SQL Server metafiles from the folder specified in the **AP_FILE_DIR** entry of the operation definition file corresponding to the operation ID to the temporary folder for extended commands.

When this command is executed on the database server, all the SQL Server metafiles in the backup-target directory are deleted, and then back up the SQL Server metafiles from the backup-source directory to the backup-target directory.

If this extended command is executed on the backup server, the SQL Server metafiles are not deleted from the temporary folder for extended commands.

**Prerequisites:**

- The operation definition file corresponding to the specified operation ID has been created.
- The temporary folder for extended commands has been created.

**Argument:**

***operation-ID***

Specify the unique character string that indicates the resource to be operated. The information in the operation definition file corresponding to the specified operation ID is used for executing this extended command.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option is specified
- Information could not be acquired from the operation definition file corresponding to the operation ID
- The copy destination folder for the target file does not exist
- A command executed inside the extended command failed

**Example:**

To back up the SQL Server metafiles, based on the settings in the operation definition file **operation01**, execute:

```
EX_DRM_SQLFILE_PACK.wsf operation01
```

## 3.12 Extended Command Specifications (Exchange Server only)

### 3.12.1 EX_DRM_EXG_BACKUP (back up the file system)

**Format:**

```
EX_DRM_EXG_BACKUP.wsf operation-ID [ -system ]
```

**Description:**

The **EX_DRM_EXG_BACKUP** command executes the drmexgbackup command and backs up the Exchange database of the storage group specified in the operation ID from the primary volume to the secondary volume. At this time, it generates a backup ID.

If the data files of the specified storage group or objects such as the various databases are stored in multiple volumes, all primary volumes are backed up to the secondary volume. If you specify an inactive storage group when executing this command, the command terminates abnormally.

To back up onto tape the Exchange database that was online backed up by this extended command onto the secondary volume, you must first verify the consistency of the Exchange database. To verify the consistency of the Exchange database and back it up onto tape, execute the **EX_DRM_EXG_VERIFY** command and then execute **EX_DRM_TAPE_BACKUP**.

To restore the Exchange database that was online backed up from the secondary volume to the primary volume by this extended command, execute the **drmexgrestore** command with the **-recovery** option specified.

**Prerequisite:**

The operation definition file corresponding to the specified operation ID is available.

**Arguments:**

***operation-ID***

Specify a unique character string identifying the resource that is to be the processing target. Information about the operation definition file corresponding to the specified operation ID is used when executing the extended command.

Executing the command with this option deletes the transaction log file. This means that you can no longer restore data by specifying the **-recovery** option based on backup data you obtained earlier. Specify this option if you did not specify the **-recovery** option when you restored data other than the recent backup data.

If you are using a circulating log, this option is ineffective. For details about circulating logs, see the Exchange Server documentation.

**-mode cold**

Specify this option for cold backup of the Exchange database. If you specify neither this option nor the **-mode online** option, the system assumes this option.

**-mode online**

Specify this option for online backup of the Exchange database. When you specify this option, you cannot specify the **-transact_log_del** or **-c offline** option. If you specify neither this option nor the **-mode cold** option, the system assumes the **-mode cold** option.

**-transact_log_del**

Specify this option when you want to delete a committed transaction log file. By deleting the transaction log file, you can increase the amount of free disk space.

Executing the command with this option specified deletes the transaction log file. This means that you can no longer restore data by specifying the **-recovery** option based on backup data you obtained earlier. Specify this option if you did not specify the **-recovery** option when you restored data other than the recent backup data.

If you are using a circulating log, this option is ineffective. For details about circulating logs, see the Exchange Server documentation.

**-c { offline | online }**

To switch offline before backing up a cluster resource of a physical disk in a cluster environment, specify **-c offline**. To back up a cluster resource while still online, specify **-c online**. The default is **-c offline**. This option is ineffective in a non-cluster environment.

**-hostname *virtual-server-name***

Specify the name of the Exchange virtual server you want to back up. You can also specify the name of the Exchange virtual server in the operation definition file. If you specify the name of the Exchange virtual server in both the operation definition file and this option, the value specified in the **-hostname** option has priority. Specify this option only for a cluster environment. This option is effective only when you specified **1** for **SET_DRM_HOSTNAME** in the operation definition file. If you specified **0**, this option is ineffective.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Note:**

- The backup information in the backup catalog is managed based on the copy group used as a key. Depending on the backup method, you might not be able to perform restoration, even though the backup data exists on the secondary volume.

  The example is described below using the two storage groups, which are located on separate volumes:

  - Storage group A (copy group: **VG01,exg01**)
  - Storage group B (copy group: **VG01,exg02**)

Use the following backup method to back up the storage groups:

1. Back up the storage group A and the storage group B concurrently. The backup ID **0000000001** is created.
2. Back up the storage group A only. The backup ID **0000000002** is created.

When you use the backup method 2, the backup ID **0000000002** is created, and the old backup information (backup ID: **0000000001**) about the copy group **VG01,exg01** on the storage group A is deleted from the backup catalog. In other words, since the backup information about the storage group B, which is included in the backup ID **0000000001**, is also deleted from the backup catalog, the file system B cannot be restored even though the backup data exists in the secondary volume. When you restore the storage group B, restore the backup data obtained by using the backup method 1 from tape to the secondary volume, and then restore the backup data from the secondary volume to the primary volume.

**Conditions causing an error**

- An invalid option was specified.
- The system failed to obtain information about the definition file corresponding to the operation ID.
- The specified Protection Services command option cannot be specified as an option of this extended command.
- The system failed to record a backup ID in the backup ID record file.
- A command executed internally terminated abnormally.

**Example:**

Delete the transaction log file based on the settings in the operation definition file **operation01** and back up the database to the secondary volume.

```
EX_DRM_EXG_BACKUP.wsf operation01 -transact_log_del
```

### 3.12.2 EX_DRM_EXG_DEF_CHECK (check contents of operation definition file)

**Format:**

To check the contents of an operation definition file on the database server:
`EX_DRM_EXG_DEF_CHECK.wsf -db -f definition-file-name`

To check the contents of an operation definition file on the backup server:
`EX_DRM_EXG_DEF_CHECK.wsf -bk -f definition-file-name`

To view the command usage:
`EX_DRM_EXG_DEF_CHECK.wsf -h`

**Description:**

The **EX_DRM_EXG_DEF_CHECK** command checks the contents of an operation definition file. It first confirms that the file specified in the argument exists and then checks the following for each item specified in the operation definition file.

- The item name and value have been specified.
- The item has been specified only once.
- The number of characters does not exceed the maximum allowable number of characters for that item.

In addition, this command checks the details listed in Table 3.23 for all items specified in the operation definition file.

**Table 3.23 Details Checked in the Operation Definition File**

| Item | Details to be Checked |
|---|---|
| BACKUP_OBJECT | MSEXCHANGE is specified. |
| DB_SERVER_NAME | ▪ The Exchange server name or virtual server name exists.<br>▪ If **1** is specified to **SET_DRM_HOSTNAME**, the value of **DB_SERVER_NAME** matches the database server name set in **DRM_DB_PATH** of Protection Services environment settings file **init.conf**. |
| INSTANCE_NAME | A hyphen (**-**) is specified. |
| TARGET_NAME | A storage group name exists *1 |
| DB_DATA_FILE_DIR | ▪ The absolute path is specified.<br>▪ The specified folder exists. *2 |
| BK_DATA_FILE_DIR | ▪ The absolute path is specified.<br>▪ The specified folder exists *2<br>▪ The configuration of the specified folder is ***home-directory-of-the-FTP-site*/*target-server-name*/-** and there are no subfolders in this folder. |
| SET_DRM_HOSTNAME | The value **0** or **1** is specified. |

***Notes:***

1. This item is checked only if the target Exchange Server is an Exchange 2000 Enterprise Server or Exchange 2003 Enterprise Edition.
2. Specification of the folder name is not case sensitive.

**Prerequisites:**

- Protection Services commands can be executed by a user account currently logged on to Windows.
- If the command is executed on the database server, it can access the domain controller of the Windows domain that manages the Exchange server. Also, the DNS service has been started on the database server.

**Arguments:**

**-db**

Specify this option when you want to check the contents of an operation definition file on the database server.

**-bk**

Specify this operation when you want to check the contents of an operation definition file on the backup server.

**-f *definition-file-name***

Specify the absolute path name of the operation definition file you want to check.

**-h**

This option displays the command usage.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- An invalid option was specified.
- The file specified in the argument does not exist, or the system cannot access the file.
- The check of the contents of the operation definition file detected an abnormality.

**Examples:**

Check the definition file **C:\Program Files\drm\SCRIPT\conf_OP0001.dat** on the database server.

```
EX_DRM_EXG_DEF_CHECK.wsf -db -f "C:\Program Files\drm\script\conf\_OP0001.dat"
```

Check the definition file **C:\Program Files\drm\SCRIPT\conf_OP0001.dat** on the backup server.

```
EX_DRM_EXG_DEF_CHECK.wsf -bk -f "C:\Program Files\drm\script\conf\_OP0001.dat"
```

### 3.12.3 EX_DRM_EXG_VERIFY (verify consistency of Exchange database)

**Format:**

```
EX_DRM_EXG_VERIFY.wsf operation-ID
                  [ -mount_pt mount-point-directory-name ] [ -force ]
```

**Description:**

This extended command executes the **drmmount** command, the **drmexgverify** command, and the **drmumount** command to verify the consistency of the Exchange database that was online backed up onto the secondary volume. To use **EX_DRM_TAPE_BACKUP** to back up the Exchange database from the secondary volume onto tape, execute this extended command to prepare for the tape backup.

When an error is detected in the consistency of the Exchange database, you must re-execute the backup onto the secondary volume.

**Prerequisites:**

- The backup catalog to be verified by this extended command has been imported to the backup server.
- The backup ID of the backup catalog was set in the backup ID record file by the **EX_DRM_DB_IMPORT** or **EX_DRM_BACKUPID_SET** command.
- This files used by the **ESEUTIL** utility (**ESEUTIL.exe**, **ESE.dll**, **EXOSAI.dll**, **EXCHMEM.dll**) required to execute this extended command have been copied to the backup server.

  Storage folder of the files used by the **ESEUTIL** utility:
  *installation-destination-of-the-Exchange-Server*\bin

  Copy destination of files on the backup server:
  *installation-destination-of-Protection-Service*\bin\util

**Arguments:**

***operation-ID***

Specify the unique character string that indicates the resource to be operated. The information in the operation definition file corresponding to the specified operation ID is used for executing this extended command.

**-mount_pt *mount-point-directory-name***

Specify the name of the mount point directory for mounting the secondary volume. When this option and the **-force** option are both specified, specify them in the order **-mount_pt**, **-force**.

When only the drive name is specified, this command searches for unused drives in the alphabetical order and mounts the secondary volume onto the specified drive. When a drive is specified by a path including a drive character, this command mounts the volume onto ***path-specified-in*-mount_pt*drive-character-of-the-primary-volume**mount-point-of-the-primary-volume***. For example, if the primary volume is mounted onto **M:\MNT** and **S:\SVOLMNT** is specified in **-mount_pt**, the secondary volume is mounted on **S:SVOLMNT\M\MNT**.

Specify a mount point directory name as an absolute path of 64 bytes or less. However, you cannot use the space character and the following special characters:
\ / : . * ? “ < > |

If this option is not specified, the secondary volume is mounted on a drive not used during extended command execution.

**-force**

***WARNING:*** Data may be damaged if you specify the **-force** option for a normal backup operation.

Specify this option to execute the mount operation forcibly. When this option and the **-mount_pt** option are both specified, specify them in the order **-mount_pt**, **-force**.

With this option, perform forced resynchronization if the copy group name of the primary volume obtained when the backup processing was performed on the database server corresponds with the information on the database server, even though the LDEV number and the SERIAL number do not correspond with the LDEV number and the SERIAL number when the backup processing was performed.

Specify this option in a case such as when the secondary volume is replaced for a reason such as a failure or when the LDEV number or SERIAL number was changed and it is necessary to forcibly mount only the copy group name of the primary volume onto the secondary volume as a key. Data may be damaged if you specify this option for a normal backup operation.

If you do not specify this option and if the copy group name of the primary volume acquired when backup on the database server is executed, the LDEV number, and the SERIAL number do not match the backup server information, the extended command will terminate abnormally without mounting the secondary volume.

**Return values:**

**0**: Normal termination

**2**: Abnormal termination

**Conditions causing an error:**

- When an invalid option is specified.
- When information could not be acquired from the definition file corresponding to the operation ID.
- When a command executed inside the extended command abnormally terminated.

**Example:**

Verify the consistency of the Exchange database determined by the operation ID **operation01**.

```
EX_DRM_EXG_VERIFY.wsf operation01
```

# Chapter 4 Operations (for UNIX)

This chapter uses examples to explain how to perform some key Protection Services operations in UNIX.

4.1 Creating the dictionary map file

4.2 Backing up and restoring a file system (offline tape storage)

4.3 Deleting backup data

Figure 4.1 shows the flow of operations when you use Protection Services to back up and restore data.

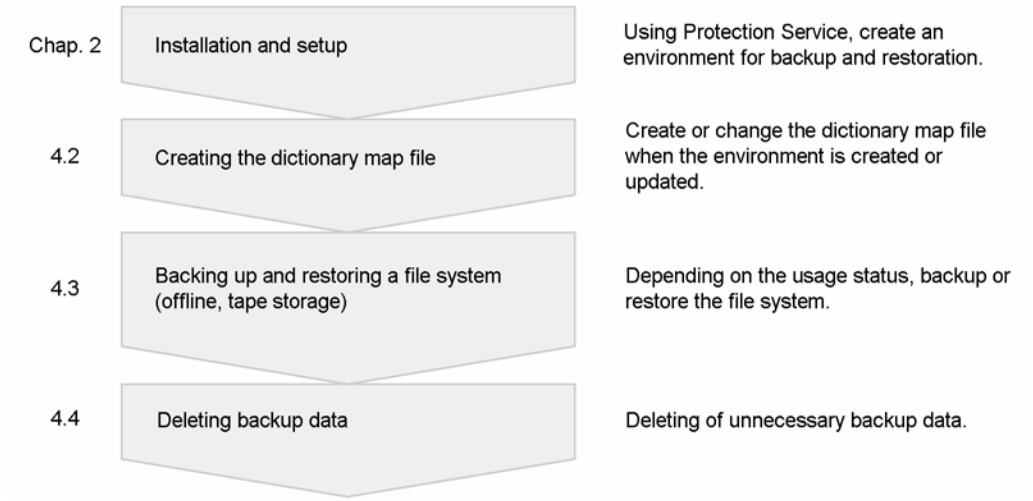



**Figure 4.1 Flow of Operations (for UNIX)**

## 4.1 Creating the Dictionary Map File

Use the dictionary map file to store information about the mapping between backup objects and RAID devices. You will need to create the dictionary map file to automatically control databases and RAID devices when you back up and restore data.

You need to update the dictionary map file when:

- You modify the CCI configuration definition files.
- You change mount points.
- You change the disk configuration, by adding or removing hard disks.
- You execute the **drmdbsetup** utility to change the storage location of the dictionary map file.

To create the dictionary map file, execute the **drmfsdisplay** command with the **-refresh** option specified.

```
PROMPT> drmfsdisplay –refresh
```

## 4.2 Backing Up and Restoring a File System (Offline Tape Storage)

This section gives an example of how to back up a file system on a file server to tape on a backup server. This section also gives an example of how to restore the file system from the tape to the file server. This example is based on the system configuration shown in Figure 4.2.

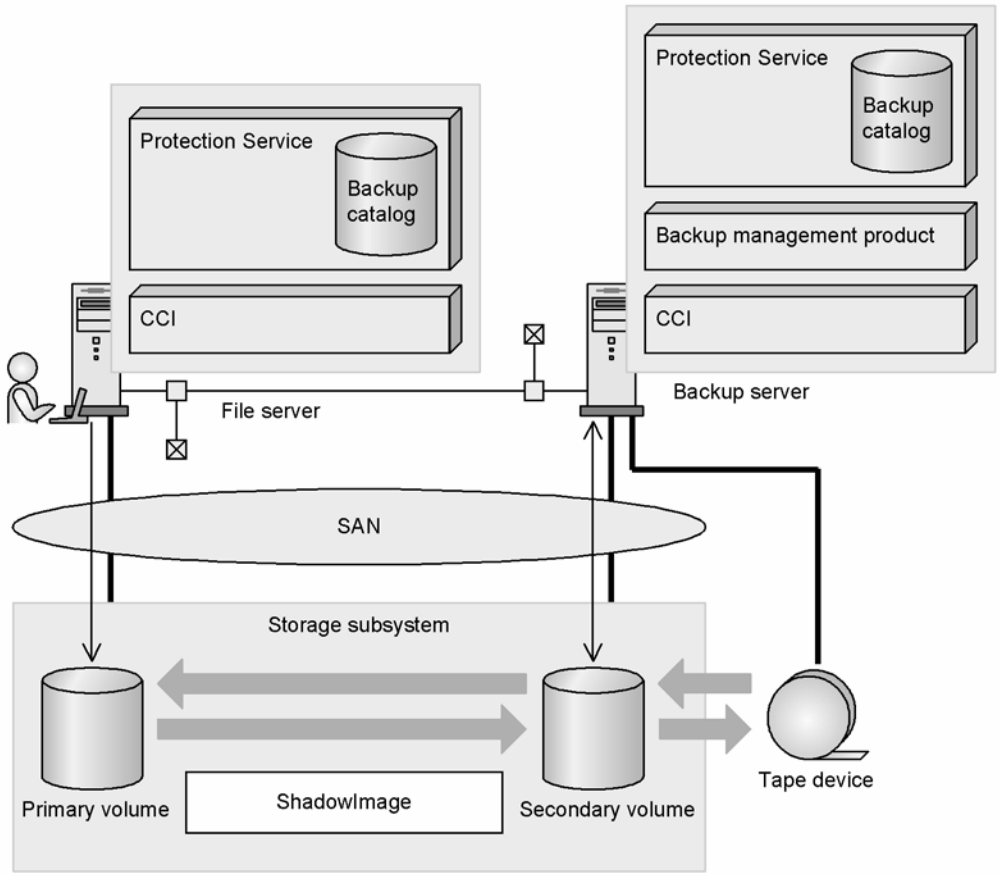



**Figure 4.2 System Configuration: Back Up and Restore a File System to Tape**

The following are assumed:

- The primary volume is mounted in the **/mnt** directory, and is formatted as one of the following:
  - In Solaris: VxFS
  - In HP-UX: VxFS
- A logical volume manager is installed on the file server and the backup server:
  - In Solaris: VxVM
  - In HP-UX: LVM
- The primary volume and secondary volume are mirrored (as set by ShadowImage and CCI).
- A secondary volume is not usually mounted. It should be mounted as required in the **/mnt** directory.
- The offline backup method is used.
- Since the primary volume is frozen during backup to the secondary volume, the applications are stopped temporarily.
- A backup management product is installed on the backup server.
- Parameters for the backup management product have been registered using the **drmtapeinit** command.

### 4.2.1 Backing Up a File System to Tape

This section describes how to perform offline backup of a file system to tape. You back up the data in the primary volume to the secondary volume using offline backup, and then back up the data in the secondary volume to tape. No new backups can be performed until the data is backed up to tape.

To back up a file system to tape:

1. Back up the target file system to the secondary volume. Perform offline backup of the file system indicated by the mount point **/mnt**. To perform the offline backup, execute the **drmfsbackup** command.

   ```
   PROMPT> drmfsbackup /mnt -mode cold
   KAVX0001-I The drmfsbackup command will now start.
   KAVX0019-I Copying file(s) now...
   KAVX0040-I The backup ID has been assigned as follows.
              Backup ID = 0000000001
   KAVX0002-I The drmfsbackup command will now end.
   PROMPT>
   ```

   When this command is executed, the backup record is registered in the backup catalog of the file server, using a new backup ID (an unused, consecutive ID). In this example, the new backup ID is **0000000001**.

2. Confirm that backup to the secondary volume has finished successfully. To confirm this, execute the **drmfscat** command.

   ```
   PROMPT> drmfscat /mnt
   INSTANCE: /mnt ORIGINAL-ID: 0000000001
   BACKUP-ID:0000000001 BACKUP-MODE: ONLINE INSTANCE: /mnt
   START-TIME: 2002/06/01 10:00:00 END-TIME: 10:03:00 HOSTNAME: FILESERV1
   T FILE       FS        DG       DEVICE               COPY-GROUP
   F -          /mnt      -        /dev/rdsk/c4t20d10   FS001,DDrive
   F -          -         -        -                    FS001,DDrive
   PROMPT>
   ```

3. Export the backup record to a temporary file. To back up the secondary volume to tape, you will need to take the information pertaining to the operations performed during backup from the primary volume to the secondary volume, and copy it to the backup server. Execute the **drmdbexport** command to export the information pertaining to backup operations to the temporary file **/tmp/EX-FILE1.drm**.

   ```
   PROMPT> drmdbexport 0000000001 -f /tmp/EX-FILE1.drm
   KAVX0001-I The drmdbexport command will now start.
   KAVX0002-I The drmdbexport command will now end.
   PROMPT>
   ```

4. Transfer the temporary file **/tmp/EX FILE1.drm**, which contains the exported backup record, from the file server to the backup server. To transfer the file, execute the **rcp** (remote copy) command.

   ```
   PROMPT> rcp /tmp/EX-FILE1.drm backup-server-name:/tmp
   PROMPT>
   ```

5. Import the temporary file **/tmp/EX-FILE1.drm** transferred from the file server to the backup catalog of the backup server. To import the file, execute the **drmdbimport** command on the backup server.

```
PROMPT> drmdbimport -f /tmp/EX-FILE1.drm
KAVX0001-I The drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000001
KAVX0002-I The drmdbimport command will now end.
PROMPT>
```

6. Confirm that the import has finished successfully. To confirm this, execute the **drmfscat** command.

```
PROMPT> drmfscat /mnt
INSTANCE: /mnt
BACKUP-ID:0000000001 BACKUP-MODE: ONLINE INSTANCE: /mnt ORIGINAL-ID: 0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE          FS           DG        DEVICE              COPY-GROUP
F -             /mnt         -         /dev/rdsk/c4t20t10  FS001,DDrive
F -             -            -         -                   FS001,DDrive
PROMPT>
```

7. Mount the secondary volume. In this example, the mount point of the secondary volume is **/mnt**.

```
PROMPT> drmmount 0000000001 -mount_pt /mnt
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = /mnt
KAVX0401-I Mounting has finished.
           Mount point = /mnt
KAVX0002-I The drmmount command will now end.
PROMPT>
```

8. Back up the data in the secondary volume to tape. To back up the data, execute the **drmmediabackup** command on the backup server.

```
PROMPT> drmmediabackup 0000000001
KAVX0001-I The drmmediabackup command will now start.
KAVX0402-I Backup processing will now start.
           To see more details on backup progress, use the monitoring method of
the backup management product.
           Source = /mnt
KAVX0403-I Backup processing has finished.
           Source = /mnt
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000002
KAVX0002-I The drmmediabackup command will now end.
PROMPT>
```

When you perform backup, the information about the backup operation is registered in the backup catalog with a new backup ID (0000000002).

9. Specify the backup ID **0000000001**, which was specified during mounting, and unmount the secondary volume.

```
PROMPT> drmumount 0000000001
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = /mnt
KAVX0407-I Unmounting has finished.
           Mount point = /mnt
KAVX0002-I The drmumount command will now end.
PROMPT>
```

10. Confirm that backup has finished successfully. To confirm this, execute the **drmtapecat** command on the backup server.

```
PROMPT> drmtapecat 0000000002
BACKUP-ID   BACKUP-OBJECT  SNAPSHOT TIME        EXPIRATION TIME      BACKUP-MEDIA
0000000002  FILESYSTEM     2002/06/01 10:00:00  2002/06/02 10:00:00  MEDIA1
PROMPT>
```

### 4.2.2 Restoring a File System

This section explains the procedures involved in restoring data backed up to tape. Once the data on the tape has been restored to the secondary volume, the secondary volume and primary volume will be resynchronized.

To restore a file system from tape:

1. Check the backup ID of the backup data to be used for the restoration. To check this, execute the **drmtapecat** command on the backup server.

```
PROMPT> drmtapecat
BACKUP-ID   BACKUP-OBJECT  SNAPSHOT TIME        EXPIRATION TIME      BACKUP-MEDIA
0000000002  FILESYSTEM     2002/06/01 10:00:00  2002/06/02 10:00:00  MEDIA1
PROMPT>
```

2. Specify the backup ID **0000000002**, and mount the secondary volume. In this example, the mount point of the secondary volume is **/mnt**.

```
PROMPT> drmmount 0000000002 -mount_pt /mnt
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = /mnt
KAVX0401-I Mounting has finished.
           Mount point = /mnt
KAVX0002-I The drmmount command will now end.
PROMPT>
```

3. Restore the backup data from tape to the secondary volume. To restore the data, execute the **drmmediarestore** command on the backup server.

```
PROMPT> drmmediarestore 0000000002
KAVX0001-I The drmmediarestore command will now start.
KAVX0404-I Restoration will now start.
           To see more details on restoration progress, use the monitoring method
of the backup management product.
           Source = /mnt
           Target = /mnt
KAVX0405-I Restoration has finished.
           Source = /mnt
           Target = /mnt
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000003
KAVX0002-I The drmmediarestore command will now end.
PROMPT>
```

   When the restoration is performed, information pertaining to the restoration operations is registered in the backup catalog, using a new backup ID (an unused, consecutive ID). In this example, the new backup ID is **0000000003**. At this point, since the status of the secondary volume will be updated, the backup ID **0000000001**, which was used to manage the status of the secondary volume before the update, is deleted from the backup catalog on the backup server.

4. Specify the backup ID **0000000002**, which was specified during mounting, and unmount the secondary volume.

```
PROMPT> drmumount 0000000002
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = /mnt
KAVX0407-I Unmounting has finished.
           Mount point = /mnt
KAVX0002-I The drmumount command will now end.
PROMPT>
```

5. Confirm that the restoration finished successfully. To confirm this, execute the **drmfscat** command on the backup server.

```
PROMPT> drmfscat /mnt
INSTANCE: /mnt
BACKUP-ID:0000000003 BACKUP-MODE: ONLINE INSTANCE: /mnt ORIGINAL-ID: 0000000003
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE          FS          DG        DEVICE             COPY-GROUP
F -             /mnt        -         /dev/rdsk/c4t20d10 FS001,DDrive
F -             -           -         -                  FS001,DDrive
PROMPT>
```

6. Export the backup record to a temporary file. In a multi-server configuration, to perform a restoration from a secondary volume to a primary volume, you will need to take the information pertaining to the operations performed during the restoration from the tape to the secondary volume, and copy it to the file server. Execute the **drmdbexport** command to export the backup record to the temporary file **/tmp/EX-FILE1.drm**.

```
PROMPT> drmdbexport 0000000003 -f /tmp/EX-FILE1.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
PROMPT>
```

7. Transfer the exported temporary file **/tmp/EX-FILE1.drm** from the backup server to the file server. To transfer the file, execute the **rcp** (remote copy) command.

```
PROMPT> rcp /tmp/EX-FILE1.drm file-server-name:/tmp
PROMPT>
```

8. Take the temporary file transferred from the backup server, and import it into the backup catalog of the file server. Import the temporary file **/tmp/EX FILE1.drm**, which was transferred from the backup server, to the file server. To import the file, execute the **drmdbimport** command on the file server.

```
PROMPT> drmdbimport -f /tmp/EX-FILE1.drm
KAVX0001-I The drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000002
KAVX0002-I The drmdbimport command will now end.
PROMPT>
```

   When you execute the command, the backup record is registered in the backup catalog of the file server with a new backup ID (**0000000002**). The restoration from tape to the secondary volume is reflected on the backup catalog of the file server. Therefore, the backup ID **0000000001**, which indicates the previous status of the secondary volume, is deleted from the backup catalog of the file server.

9. Confirm that the import has finished successfully. To confirm this, execute the **drmfscat** command.

```
PROMPT> drmfscat /mnt
INSTANCE: /mnt
BACKUP-ID:0000000002 BACKUP-MODE: ONLINE INSTANCE: /mnt ORIGINAL-ID: 0000000002
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE          FS           DG        DEVICE              COPY-GROUP
F -             D:           -         /dev/rdsk/c4t20d10  FS001,DDrive
F -             -            -         -                   FS001,DDrive
PROMPT>
```

10. Restore the data on the secondary volume to the primary volume. To perform the restoration, resynchronize the primary and secondary volumes. To resynchronize, execute the **drmfsrestore** command on the file server.

```
PROMPT> drmfsrestore 0000000002 -resync
KAVX0001-I The drmfsrestore command will now start.
KAVX0019-I Copying file(s) now...
KAVX0002-I The drmfsrestore command will now end.
PROMPT>
```

## 4.3 Deleting Backup Data

If the backup data on the secondary volume is no longer necessary, delete it. You can delete the backup data on the secondary volume once you back it up to tape or restore the primary volume from the backup data in the secondary volume.

To delete the backup data, execute the **drmresync** command, specifying the backup ID of the data to be deleted.

```
PROMPT> drmresync –backup_id backup-ID
KAVX0001-I The drmresync command will now start.
KAVX0002-I The drmresync command will now end.
PROMPT>
```

When you execute this command, the primary volume and the secondary volume will be resynchronized, and mirrored. Now the backup record of the specified backup ID will be deleted from the backup catalog.

# Chapter 5 Operations (for Windows)

This chapter uses examples to explain how to perform some key Protection Services operations in Windows.

Common operations:

- 5.1 Notes on use
- 5.2 Creating the dictionary map file
- 5.3 Deleting backup data

Copy Controller operations:

- 5.4 Backing up and restoring a file system (offline tape storage)

SQL Server operations:

- 5.5 Backing up, restoring, and recovering an SQL Server database (online tape storage)
- 5.6 Backing up, restoring, and recovering an SQL Server database (from a different host)
- 5.7 Using the SQL Server log-shipping functionality

Exchange Server operations:

- 5.8 Backing up, restoring, and recovering storage groups (using online backup to tape)
- 5.9 Backing up, restoring, and recovering storage groups (using cold backup to tape)

Figure 5.1 shows the flow of operations when you use Protection Services – Copy Controller to back up and restore data. Figure 5.2 shows the flow of operations when you use Protection Services for SQL Server to back up and restore a database. Figure 5.3 shows the flow of operations when you use Protection Services for Exchange Server to back up, restore, and recover a database.

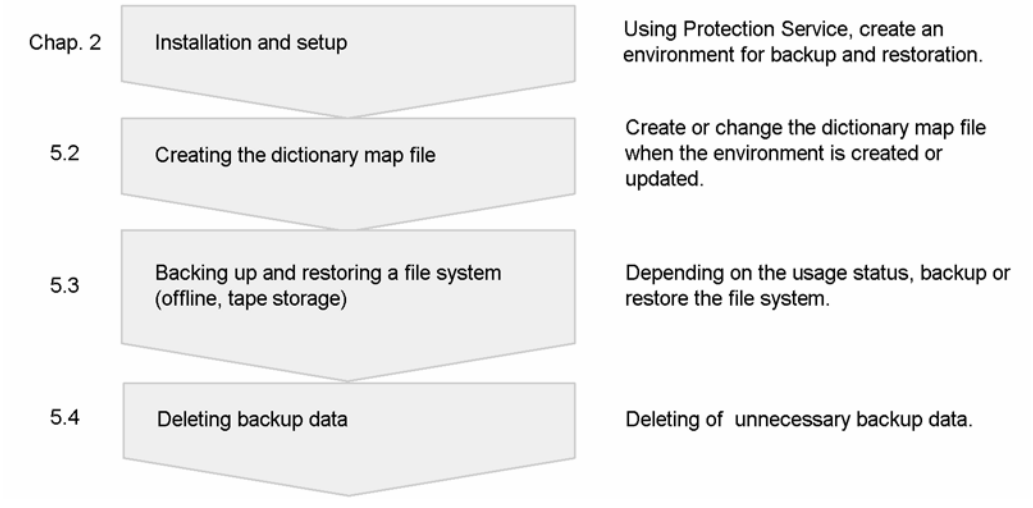



**Figure 5.1 Flow of Operations (Windows, Copy Controller only)**

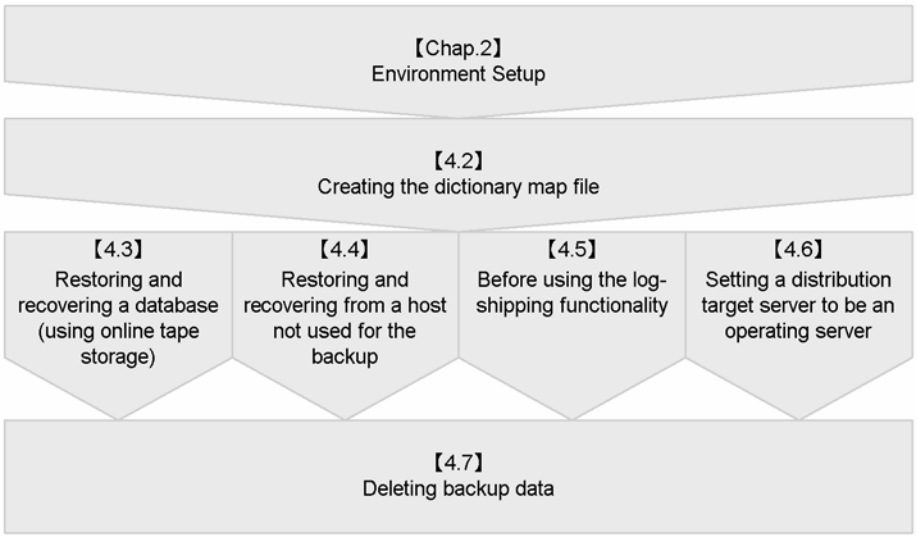



**Figure 5.2 Flow of Operations (SQL Server)**

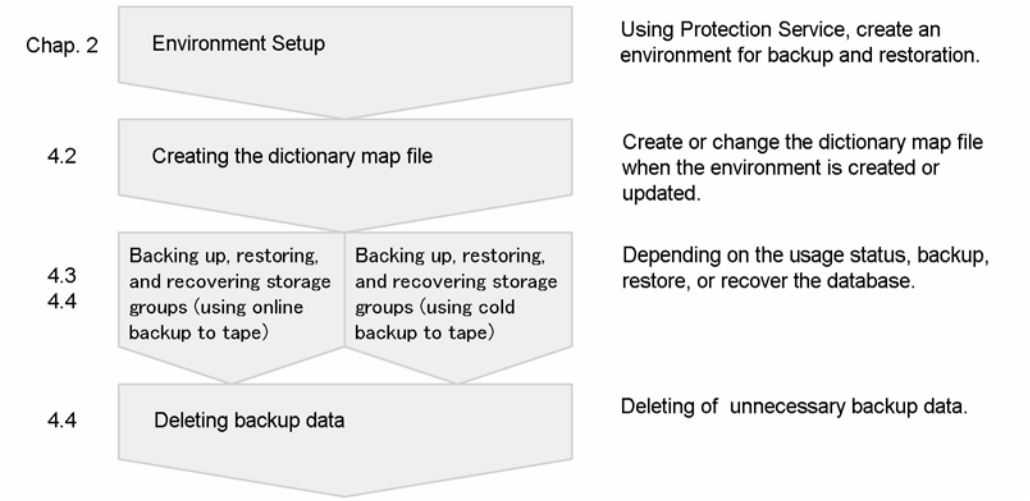



**Figure 5.3 Flow of Operations (Exchange Server)**

## 5.1 Notes on Use

### 5.1.1 Exchange Server

Note the following when performing an online backup for the Exchange database and verifying this database.

- **Note on online backup**

  The **drmexgbackup** command performs an online backup by forcibly copying data from the primary volume to the secondary volume without dismounting the information store. Microsoft does not guarantee this backup method for Exchange Server. It may be impossible to restore the backup data acquired by this function. To ensure restoration of the backup data, first use the **drmexgbackup** command to perform a cold backup. Then, make sure that the backup data is stored, and then perform an online backup.

- **Note on verification of the database**

  Use the **drmexgverify** command to verify the integrity of the data that was backed up online by the **drmexgbackup** command. This command only verifies the integrity for the Exchange database (***.edb** file), and not for the Exchange streaming database (***.stm** file). This means that even if the **drmexgverify** command successfully terminates the verification, the Exchange streaming database may have been corrupted. In this case, the backup data cannot be restored.

## 5.2 Creating the Dictionary Map File

Use the dictionary map file to store information about the mapping between backup objects and RAID devices. You will need to create the dictionary map file to automatically control databases and RAID devices when you back up and restore data.

You will need to update the dictionary map file when:

- You modified the CCI configuration definition files.
- You changed mount points.
- You changed the disk configuration by adding or removing hard disks.
- You executed the **drmdbsetup** utility to change the storage location of the dictionary map file.
- You changed the database configuration

**Copy Controller:** To create the dictionary map file for Copy Controller, execute the **drmfsdisplay** command with the **-refresh** option specified.

**SQL Server:** To create the dictionary map file for SQL Server, execute the **drmsqldisplay** command with the **-refresh** option specified.

**Exchange Server:** To create the dictionary map file for Exchange Server, execute the **drmexgdisplay** command with the **-refresh** option specified.

## 5.3 Deleting Backup Data

If the backup data in the secondary volume is no longer necessary, you may delete it. You can delete the backup data in the secondary volume after you either back up the data in the secondary volume to tape, or restore the primary volume from the backup data in the secondary volume.

To delete backup data, execute the **drmresync** command specifying the backup ID of the data to be deleted.

```
PROMPT> drmresync –backup_id backup-ID
KAVX0001-I The drmresync command will now start.
KAVX0002-I The drmresync command will now end.
PROMPT>
```

When you execute this command, the primary volume and the secondary volume are resynchronized to be mirrored. The backup information of the specified backup ID is deleted from the backup catalog.

## 5.4 Backing Up and Restoring a File System (Offline Tape Storage)

This section uses an example to explain how to back up a file system on a file server to tape on a backup server, and restore the file system on the file server from the tape. This example is based on the system configuration shown in Figure 5.4.

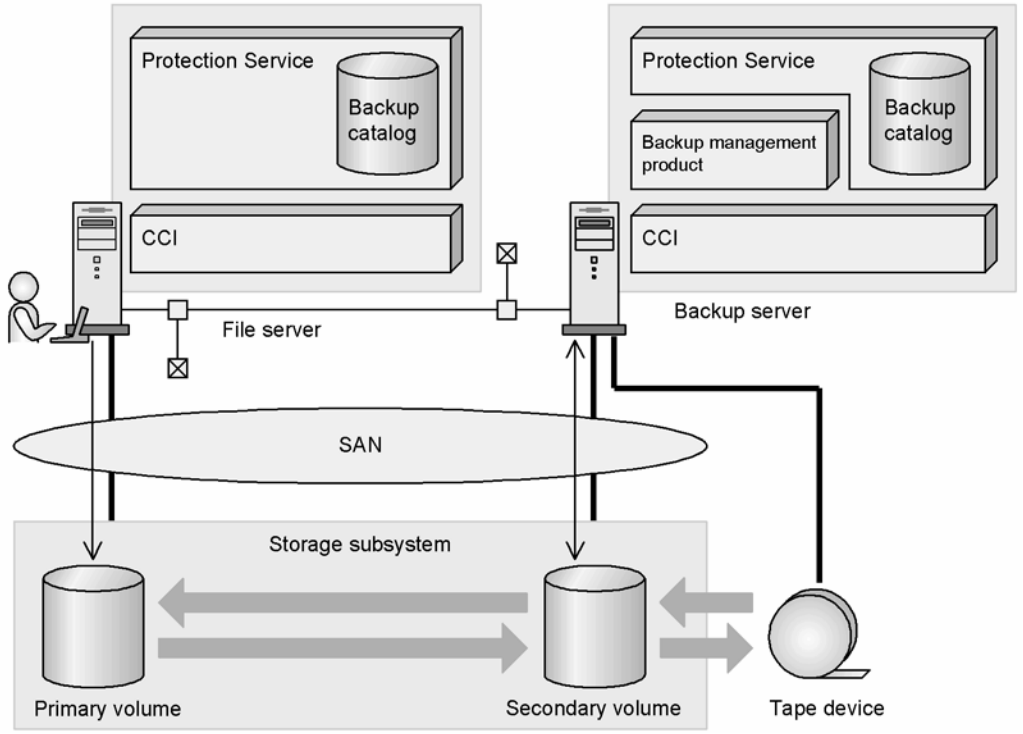



**Figure 5.4 System Configuration: Tape Backup and Restoration (File System)**

This example assumes the following conditions:

- The primary volume is NTFS-formatted and mounted on the **D** drive.
- The primary volume and the secondary volume are mirrored (as set by ShadowImage and CCI).
- Normally, the secondary volume is not mounted. It is mounted on the **E** drive when necessary.
- The offline backup method is used.
- The primary volume cannot be accessed from the file server because the primary volume is unmounted while the secondary volume is being backed up.
- A backup management product is installed on the backup server.
- The parameters for the backup management product have been registered using the **drmtapeinit** command.

### 5.4.1 Backing Up a File System to Tape

This section describes how to perform offline backup of a file system to tape. You back up the data in the primary volume to the secondary volume using offline backup, and then back up the data in the secondary volume to tape. No new backups can be performed until the data is backed up to tape.

To back up a file system to tape:

1. Immediately before you perform a backup, clear the system cache of the backup server. To clear the system cache, temporarily unmount the secondary volume.

```
PROMPT> drmmount -copy_group FS001,DDrive -mount_pt E:
KAVX0001-I The drmmount command will now start.
KAVX0002-I The drmmount command will now end
PROMPT> drmumount -copy_group FS001,DDrive
KAVX0001-I The drmumount command will now start.
KAVX0002-I The drmumount command will now end.
PROMPT>
```

2. Back up the file system to the secondary volume. Perform offline backup of the file system specified by the drive letter **D:**. To perform backup, execute the **drmfsbackup** command.

```
PROMPT> drmfsbackup D: -mode cold
KAVX0001-I The drmfsbackup command will now start.
KAVX0019-I Copying file(s) now...
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000001
KAVX0002-I The drmfsbackup command will now end.
PROMPT>
```

   When you execute the command, the backup information is registered in the backup catalog on the file server with a new (unused and sequential) backup ID. The backup ID is **0000000001**.

3. Check the backup execution results. Confirm that backup to the secondary volume has completed successfully. To confirm this, execute the **drmfscat** command.

```
PROMPT> drmfscat D:
INSTANCE: D:
BACKUP-ID:0000000001 BACKUP-MODE: COLD INSTANCE: D:ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE          FS           DG        DEVICE             COPY-GROUP
F -             D:           -         Harddisk1          FS001,DDrive
F -             -            -         -                  FS001,Ddrive
PROMPT>
```

4. When you back up the data in the secondary volume to tape, you need to copy the information about the backup operation from the primary volume to the secondary volume to the backup server. Execute the **drmdbexport** command to export the information about the backup operation to the temporary file **C:\temp\EX-FILE1.drm**.

```
PROMPT> drmdbexport 0000000001 -f C:\temp\EX-FILE1.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
PROMPT>
```

5. Transfer the temporary file **C:\temp\EX-FILE1.drm**, which contains the exported backup information, from the file server to the backup server. To transfer the file, execute the **ftp** command. In this example, the FTP root folder is **C:\FTP_ROOT**. The temporary file is transferred to the backup server as **C:\FTP_ROOT\EX-FILE1.drm**.

```
PROMPT> ftp backup-server-name
ftp> Username: login-name
ftp> password: password
ftp> put C:\temp\EX-FILE1.drm
ftp> quit
PROMPT>
```

6. Import the temporary file **C:\FTP_ROOT\EX-FILE1.drm**, which was transferred from the file server, to the backup catalog of the backup server. To import the file, execute the **drmdbimport** command on the backup server.

```
PROMPT> drmdbimport -f C:\FTP_ROOT\EX-FILE1.drm
KAVX0001-I The drmcgctl command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000001
KAVX0002-I The drmcgctl command will now end.
PROMPT>
```

7. Check the import results. Confirm that the import has completed successfully. To confirm this, execute the **drmfscat** command.

```
PROMPT> drmfscat D:
INSTANCE: D:
BACKUP-ID:0000000001 BACKUP-MODE: COLD INSTANCE: D: ORIGINAL-ID:0000000001
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE  FS  DG  DEVICE     COPY-GROUP
F -     D:  -   Harddisk1  FS001,DDrive
F -     -   -   -          FS001,DDrive
PROMPT>
```

8. Mount the secondary volume. In this example, the mount point of the secondary volume is **E:**.

```
PROMPT> drmmount 0000000001 -mount_pt E:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = E:
KAVX0401-I Mounting has finished.
           Mount point = E:
KAVX0002-I The drmmount command will now end.
PROMPT>
```

9. Back up the data in the secondary volume to tape. To perform backup, execute the **drmmediabackup** command on the backup server.

```
PROMPT> drmmediabackup 0000000001
KAVX0001-I The drmmediabackup command will now start.
KAVX0402-I Backup processing will now start.
           To see more details on backup progress, use the monitoring method of
the backup management product.
           Source = E:
KAVX0403-I Backup processing has finished.
           Source = E:
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000002
KAVX0002-I The drmmediabackup command will now end.
PROMPT>
```

   When you perform backup, the information about the backup operation is registered in the backup catalog with a new backup ID (**0000000002**).

10. Unmount the secondary volume. Specify the backup ID **0000000001**, which was specified during mounting, and unmount the secondary volume.

```
PROMPT> drmumount 0000000001
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = E:
KAVX0407-I Unmounting has finished.
           Mount point = E:
KAVX0002-I The drmumount command will now end.
PROMPT>
```

11. Check the backup execution results. Confirm that backup has completed successfully. To confirm this, execute the **drmtapecat** command on the backup server.

```
PROMPT> drmtapecat 0000000002
BACKUP-ID   BACKUP-OBJECT  SNAPSHOT TIME        EXPIRATION TIME      BACKUP-MEDIA
0000000002  FILESYSTEM     2002/06/01 10:00:00  2002/06/02 10:00:00  MEDIA1
PROMPT>
```

### 5.4.2 Restoring a File System

This section explains the procedures involved in restoring data backed up to tape. Once the data on the tape has been restored to the secondary volume, the secondary volume and primary volume will be resynchronized.

To restore a file system from tape:

1. Check the backup ID of the backup data to be used for the restoration. To check the ID, execute the **drmtapecat** command on the backup server.

```
PROMPT> drmtapecat
BACKUP-ID   BACKUP-OBJECT  SNAPSHOT TIME      EXPIRATION TIME        BACKUP-MEDIA
0000000002  FILESYSTEM     2002/06/01 10:00:00  2002/06/02 10:00:00  MEDIA1
PROMPT>
```

2. Specify the backup ID **0000000002**, and mount the secondary volume. In this example, the mount point of the secondary volume is **E:**.

```
PROMPT> drmmount 0000000002 -mount_pt E:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = E:
KAVX0401-I Mounting has finished.
           Mount point = E:
KAVX0002-I The drmmount command will now end.
PROMPT>
```

3. Restore the backup data from tape to the secondary volume. To restore the backup data, execute the **drmmediarestore** command on the backup server.

```
PROMPT> drmmediarestore 0000000002
KAVX0001-I The drmmediarestore command will now start.
KAVX0404-I Restoration will now start.
           To see more details on restoration progress, use the monitoring method
of the backup management product.
           Source = E:
           Target = E:
KAVX0405-I Restoration has finished.
           Source = E:
           Target = E:
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000003
KAVX0002-I The drmmediarestore command will now end.
PROMPT>
```

When the restoration is performed, information pertaining to the restoration operations is registered in the backup catalog, using a new backup ID (an unused, consecutive ID). In this example, the new backup ID is **0000000003**. At this point, since the status of the secondary volume will be updated, the backup ID **0000000001**, which was used to manage the status of the secondary volume before the update, is deleted from the backup catalog on the backup server.

4. Specify the backup ID **0000000002**, which was specified during mounting, and unmount the secondary volume.

```
PROMPT> drmumount 0000000002
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = E:
KAVX0407-I Unmounting has finished.
           Mount point = E:
KAVX0002-I The drmumount command will now end.
PROMPT>
```

5. Check the execution results for the restoration from the tape to the secondary volume. Confirm that the restoration completed successfully. To confirm this, execute the **drmfscat** command on the backup server.

```
PROMPT> drmfscat D:
INSTANCE: D:
BACKUP-ID:0000000003 BACKUP-MODE: COLD INSTANCE: D: ORIGINAL-ID:0000000003
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE  FS  DG  DEVICE     COPY-GROUP
F -     D:  -   Harddisk1  FS001,DDrive
F -     -   -   -          FS001,DDrive
PROMPT>
```

6. Export the backup information to a temporary file. To restore data from a secondary volume to a primary volume in a multi-server configuration, you must take the backup information for the restore operation from the tape to the secondary volume and copy that information to the file server. Execute the **drmdbexport** command to export the backup information to the **FTP** root folder. In this example, the FTP root folder is **C:\FTP_ROOT**, and the backup information is exported to **C:\FTP_ROOT\EX-FILE1.drm**.

```
PROMPT> drmdbexport 0000000003 -f C:\FTP_ROOT\EX-FILE1.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
PROMPT>
```

7. From the file server, get temporary file **C:\FTP_ROOT\EX-FILE1.drm**, which was exported from the backup server. To get the file, execute the **ftp** command. The temporary file is stored in the current directory. In this example, the current directory is **C:**.

```
PROMPT> ftp backup-server-name
ftp> Username: login-name
ftp> password: password
ftp> get EX-FILE1.drm
ftp> quit
PROMPT>
```

8. Import the temporary file **C:\temp\EX-FILE1.drm**, which was obtained from the backup server, to the file server. To do so, execute the **drmdbimport** command on the file server.

```
PROMPT> drmdbimport -f C:\temp\EX-FILE1.drm
KAVX0001-I The drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000002
KAVX0002-I The drmdbimport command will now end.
PROMPT>
```

   When you execute the command, the backup information is registered in the backup catalog of the file server with a new backup ID (**0000000002**). The restoration from tape to the secondary volume is reflected on the backup catalog of the file server. Therefore, the backup ID **0000000001**, which indicates the previous status of the secondary volume, is deleted from the backup catalog of the file server.

9. Confirm that the import has completed successfully. To confirm this, execute the **drmfscat** command.

```
PROMPT> drmfscat D:
INSTANCE: D:
BACKUP-ID:0000000002 BACKUP-MODE: COLD INSTANCE: D: ORIGINAL-ID:0000000002
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE  FS  DG  DEVICE    COPY-GROUP
F -     D:  -  Harddisk1  FS001,DDrive
F -     -   -  -          FS001,DDrive
PROMPT>
```

10. Restore the data on the secondary volume to the primary volume. To perform the restoration, resynchronize the primary and secondary volumes. To resynchronize, execute the **drmfsrestore** command on the file server.

```
PROMPT> drmfsrestore 0000000002 -resync
KAVX0001-I The drmfsrestore command will now start.
KAVX0019-I Copying file(s) now...
KAVX0002-I The drmfsrestore command will now end.
PROMPT>
```

## 5.5 Backing up, Restoring, and Recovering an SQL Server DB (online tape storage)

This section uses an example to explain how to back up data to the tape of a SQL Server database backup server, restore the data to the database server, and perform a recovery that applies the SQL Server database transaction log. This example is based on the system configuration shown in the following diagram.

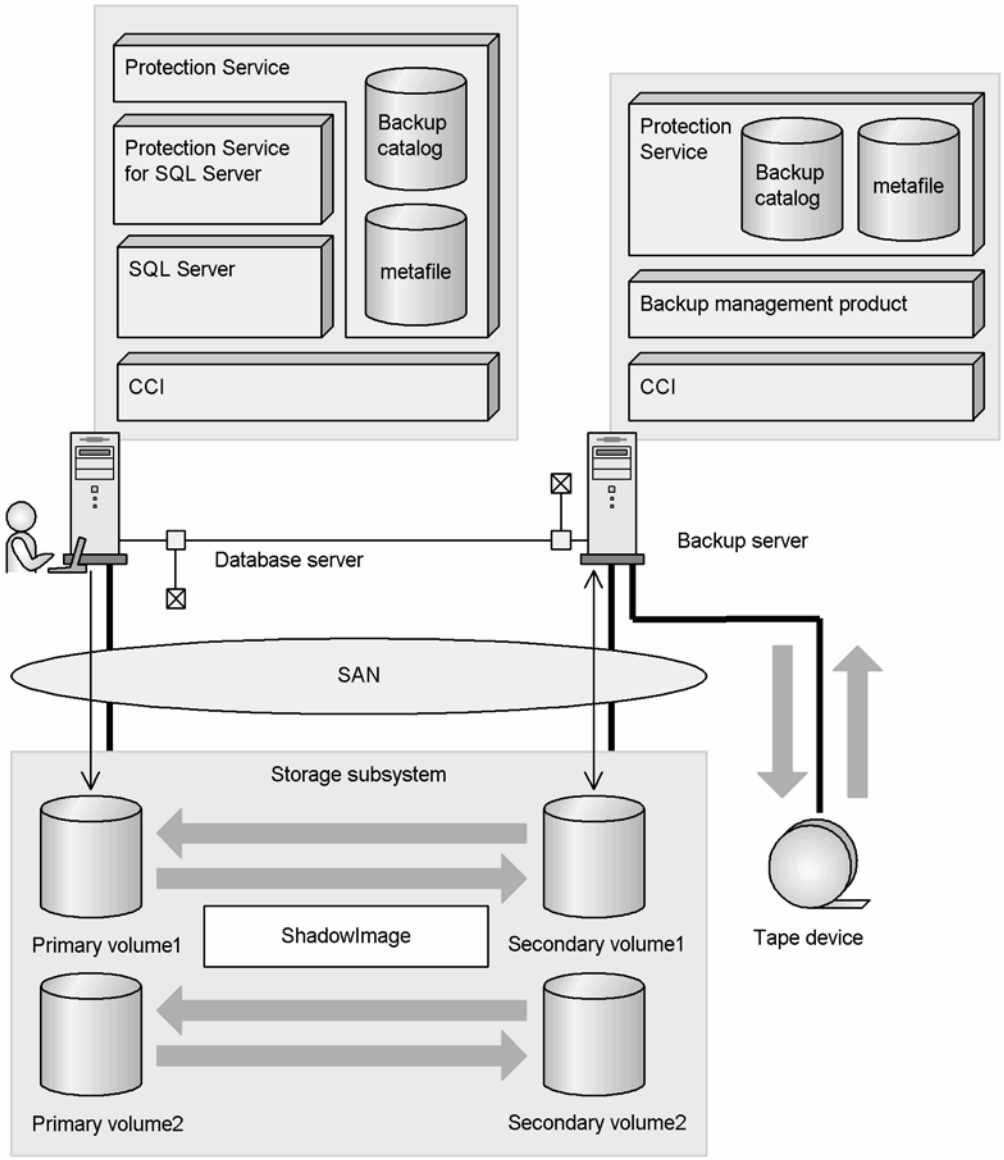



**Figure 5.5 System Configuration: Tape Backup and Restoration (SQL Server DB)**

This example assumes the following conditions:

- The primary volumes are formatted as NTFS and are mounted on the D drive and E drive of the database server, and both volumes are used for SQL Server database. The volume for storing data files cannot be used to store logs also.
- The primary volume and the secondary volume are mirrored (as set by the volume replication function and CCI).
- Normally, the secondary volumes are not mounted. If necessary, one secondary volume is mounted on the D drive and the other secondary volume is mounted on the E drive.
- A backup management product is installed on the backup server.
- The parameters for the backup management product have been registered using the **drmtapeinit** command.
- The SQL Server database backup will be to tape, using the online backup method.

### 5.5.1 Backing Up an SQL Server Database

This section explains the procedures involved in performing an online backup to tape for an SQL Server database. Once an online backup of the data is performed from the primary volume to the secondary volume, the secondary volume is backed up to tape. No new backups can be performed until the data is backed up to tape.

To back up an SQL Server database to tape:

1. Immediately before you perform a backup, clear the system cache of the backup server. To clear the system cache, temporarily unmount the secondary volume.

```
PROMPT> drmmount -copy_group SQL001,B001 -mount_pt D:
KAVX0001-I The drmmount command will now start.
KAVX0002-I The drmmount command will now end.
PROMPT> drmumount -copy_group SQL001,B001
KAVX0001-I The drmumount command will now start.
KAVX0002-I The drmumount command will now end.
PROMPT> drmmount -copy_group SQL002,B001 -mount_pt D:
KAVX0001-I The drmmount command will now start.
KAVX0002-I The drmmount command will now end.
PROMPT> drmumount -copy_group SQL002,B001
KAVX0001-I The drmumount command will now start.
KAVX0002-I The drmumount command will now end.
```

2. Back up the SQL Server database to the secondary volume. To perform an online backup for SQL Server database, execute the **drmsqlbackup** command:

```
PROMPT> drmsqlbackup SQL1
KAVX0001-I The drmsqlbackup command will now start.
KAVX1017-I SQL Server information is being collected now
KAVX1207-I Backing up the database...
KAVX0019-I Copying file(s) now...
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000001
KAVX0002-I The drmsqlbackup command will now end.
PROMPT>
```

   When this command is executed, backup information is registered in the backup catalog of the database server, using a new backup ID (an unused, consecutive ID). In this example, the new backup ID is **0000000001**.

3. Check the backup execution results. To confirm that backup to the secondary volume finished successfully, execute the **drmsqlcat** command.

```
PROMPT> drmsqlcat SQL1
INSTANCE: SQL1BACKUP-ID: 0000000001 BACKUP-MODE: ON-LINE INSTANCE: SQL1
ORIGINAL-ID: 0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: SQL1
T  DB   OBJECT    FILE             FS  DG  DEVICE     COPY-GROUP
M  DB1  METAFILE  C:\METADIR\Meta1 C:  -   -          -
D  DB1  DATAFILE  D:\SQL\data1     D:  -   Harddisk1  SQL001,B001
-  -    -        -                -   -   -          SQL001,B001
T  DB1  TRANSACT  E:\SQL\tlog      E:  -   Harddisk2  SQL002,B001
-  -    -        -                -   -   -          SQL002,B001
PROMPT>
```

4. Export the backup information to a temporary file. To back up the secondary volume to tape, you will need to take the information pertaining to the operations performed during backup from the primary volume to the secondary volume, and copy it to the backup server. Execute the **drmdbexport** command to export the information pertaining to backup operations to the temporary file **C:\temp\EX-FILE1.drm**:

```
PROMPT> drmdbexport 0000000001 -f C:\temp\EX-FILE1.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
PROMPT>
```

5. Transfer the exported temporary file from the database server to the backup server. Transfer the exported temporary file **C:\temp\EX-FILE1.drm** from the database server to the backup server. To transfer the file, execute the **ftp** command. The following assumes that the FTP root folder is **C:\FTP_ROOT**. The temporary file is transferred to the backup server as **C:\FTP_ROOT\EX-FILE1.drm**.

```
PROMPT> ftp backup-server-name
ftp> Username: (logon-name)
ftp> password: (password)
ftp> put C:\temp\EX-FILE1.drm
ftp> quit
PROMPT>
```

6. Take the temporary file transferred from the database server, and import it into the backup catalog of the backup server. Import into the backup catalog of the backup server the temporary file **C:\temp\EX-FILE1.drm** that was transferred from the database server. To import the file, execute the **drmdbimport** command on the backup server.

```
PROMPT> drmdbimport -f C:\FTP_ROOT\EX-FILE1.drm
KAVX0001-I The drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000001
KAVX0002-I The drmdbimport command will now end.
```

7. Check the import results. To confirm that the import finished successfully, execute the **drmsqlcat** command.

```
PROMPT> drmsqlcat SQL1
INSTANCE: SQL1
BACKUP-ID: 0000000001 BACKUP-MODE: ON-LINE INSTANCE: SQL1 ORIGINAL-ID: 0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: SQL1
T  DB   OBJECT    FILE             FS  DG  DEVICE     COPY-GROUP
M  DB1  METAFILE  C:\METADIR\Meta1 C:  -   -          -
D  DB1  DATAFILE  D:\SQL\data1     D:  -   Harddisk1  SQL001,B001
-  -    -        -                -   -   -          SQL001,B001
T  DB1  TRANSACT  E:\SQL\tlog      E:  -   Harddisk2  SQL002,B001
-  -    -        -                -   -   -          SQL002,B001
PROMPT>
```

8. Mount the secondary volume. The following assumes that the mount point for the secondary volume is **E:**.

```
PROMPT> drmmount 0000000001 -mount_pt E:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = E:
KAVX0401-I Mounting has finished.
           Mount point = E:
KAVX0002-I The drmmount command will now end.
PROMPT>
```

9. Back up the data on the secondary volume to tape. To perform the backup, execute the **drmmediabackup** command on the backup server. In this example, the drive letter of the secondary volume is **E:**.

```
PROMPT> drmmediabackup 0000000001
KAVX0001-I The drmmediabackup command will now start.
KAVX0402-I Backup processing will now start.
           To see more details on backup progress, use the monitoring method of
the backup management product.
           Source = E:
KAVX0403-I Backup processing has finished.
           Source = E:
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000002
KAVX0002-I The drmmediabackup command will now end.
PROMPT>
```

   When backup is performed, information pertaining to the backup operations is registered in the backup catalog, using the new backup ID **0000000002**.

10. Unmount the secondary volume. To unmount the secondary volume, specify the backup ID used when mounting **0000000001**.

```
PROMPT> drmumount 0000000001
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = E:
KAVX0407-I Unmounting has finished.
           Mount point = E:
KAVX0002-I The drmumount command will now end.
PROMPT>
```

11. Check the tape backup execution results. To confirm that backup finished successfully, execute the **drmtapecat** command on the backup server:

```
PROMPT> drmtapecat 0000000002
BACKUP-ID  BACKUP-OBJECT  SNAPSHOT TIME  EXPIRATION TIME  BACKUP-MEDIA
0000000002 MSSQL  2002/06/01 10:00:00  2002/06/02 10:00:00  MEDIA1
PROMPT>
```

### 5.5.2 Backing Up an SQL Server Transaction Log

This section explains how to backup a transaction log, which needs to be done in order to perform recovery for SQL Server database

To back up a transaction log:

1. Back up the transaction log. To back up the transaction log, execute the **drmsqllogbackup** command.
```
PROMPT> drmsqllogbackup SQL1 -target DB1
KAVX0001-I The drmsqllogbackup command will now start.
KAVX0002-I The drmsqllogbackup command will now end.
PROMPT>
```
2. Check the backup ID with which the transaction logs were backed up.
```
PROMPT> drmsqllogbackup SQL1 -v BACKUP-ID
ORIGINAL-ID   BACKUP_ID    DB
0000000002    0000000002   DB1
PROMPT>
```
3. Check the contents of the backed-up transaction log.
```
PROMPT> drmsqllogbackup SQL1 -target DB1 -v
# ORIGINAL-ID: 0000000002 BACKUP-ID: 0000000002
[DB1]
C:\LogBackup\DB1_20021106010100_0001.bk
C:\LogBackup\DB1_20021106010110_0002.bk
C:\LogBackup\DB1_20021106010120_0003.bk
PROMPT>
```

### 5.5.3 Restoring and Recovering an SQL Server Database

This section explains how to restore data backed up to tape, and perform a recovery for SQL Server database. Once the data on the tape has been restored to the secondary volume, the secondary volume and primary volume will be resynchronized. SQL Server database recovery applies the transaction log.

To restore the SQL Server database from tape:

1. Check the backup ID of the backup data. To check the backup ID of the backup data to be used for the restoration, execute the **drmtapecat** command on the backup server.
```
PROMPT> drmtapecat
BACKUP-ID  BACKUP-OBJECT  SNAPSHOT TIME  EXPIRATION TIME  BACKUP-MEDIA
0000000002  MSSQL  2002/06/01 10:00:00  2002/06/02 10:00:00  MEDIA1
PROMPT>
```
2. Mount the secondary volume by specifying backup ID **0000000002**. The following assumes that the mount point for the secondary volume is **E:**.
```
PROMPT> drmmount 0000000002 -mount_pt E:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = E:
KAVX0401-I Mounting has finished.
           Mount point = E:
KAVX0002-I The drmmount command will now end.
PROMPT>
```

3. Restore the backup data from the tape to the secondary volume. To perform the restoration, execute the **drmmediarestore** command on the backup server.

```
PROMPT> drmmediarestore 0000000002
KAVX0001-I The drmmediarestore command will now start.
KAVX0404-I Restoration will now start.
           To see more details on restoration progress, use the monitoring method
of the backup management product.
           Source = E:
           Target = E:
KAVX0405-I Restoration has finished.
           Source = E:
           Target = E:
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000003
KAVX0002-I The drmmediarestore command will now end.
PROMPT>
```

   When the restoration is performed, information pertaining to the restoration operations is registered in the backup catalog, using a new backup ID (an unused, consecutive ID). In this example, the new backup ID is **0000000003**. At this point, since the status of the secondary volume will be updated, the backup ID **0000000001**, which was used to manage the status of the secondary volume before the update, is deleted from the backup catalog on the backup server.

4. Unmount the secondary volume. To unmount the secondary volume, specify the backup ID used when mounting **0000000002**.

```
PROMPT> drmumount 0000000002
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = E:
KAVX0407-I Unmounting has finished.
           Mount point = E:
KAVX0002-I The drmumount command will now end.
PROMPT>
```

5. Check the execution results of the restoration from the tape to the secondary volume. To confirm that the restoration finished successfully, execute the **drmsqlcat** command on the backup server.

```
PROMPT> drmsqlcat SQL1
INSTANCE: SQL1
BACKUP-ID: 0000000003 BACKUP-MODE: ON-LINE INSTANCE: SQL1 ORIGINAL-ID: 0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: SQL1
T  DB   OBJECT    FILE             FS  DG  DEVICE     COPY-GROUP
M  DB1  METAFILE  C:\METADIR\Meta1 C:  -   -          -
D  DB1  DATAFILE  D:\SQL\data1     D:  -   Harddisk1  SQL001,B001
-  -    -         -                -   -   -          SQL001,B001
T  DB1  TRANSACT  E:\SQL\tlog      E:  -   Harddisk2  SQL002,B001
-  -    -         -                -   -   -          SQL002,B001
PROMPT>
```

6. Export the backup information to a temporary file. In a multi-server configuration, to perform a restoration from a secondary volume to a primary volume, you will need to copy the information pertaining to the operations performed during the restoration from the tape to the secondary volume. You copy this information to the database server. Execute the **drmdbexport** command to export the backup information to the FTP root folder. The following assumes that the FTP root folder is **C:\FTP_ROOT**, and that the backup information is exported to **C:\FTP_ROOT\EX-FILE1.drm**.

```
PROMPT> drmdbexport 0000000003 -f C:\FTP_ROOT\EX-FILE1.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
PROMPT>
```

7. Transfer the temporary file to the database server. Use the **ftp** command to transfer the temporary file **C:\FTP_ROOT\EX-FILE1.drm** (created in step 6) to the database server. The temporary file will be stored in the current directory. The following assumes that the current directory is **C:**.

```
PROMPT> ftp database-server-name
ftp> Username: (logon-name)
ftp> password: (password)
ftp> get EX-FILE1.drm
ftp> quit
PROMPT>
```

8. Import the temporary file into the backup catalog on the database server. Import the temporary file **C:\EX-FILE1.drm** (transferred from the backup server in step 7) into the backup catalog on the database server. To import the file, execute the **drmdbimport** command on the database server.

```
PROMPT> drmdbimport -f C:\EX-FILE1.drm
KAVX0001-I The drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000002
KAVX0002-I The drmdbimport command will now end.
PROMPT>
```

   At a restoration, backup information is registered in the backup catalog of the database server under the new backup ID **0000000002**. Also, since the fact that a restoration was performed from tape to the secondary volume is reflected in the backup catalog, the backup ID **0000000001**, which was used to manage the status of the secondary volume before the update, is deleted from the backup catalog on the database server.

9. Check the import results. To confirm that the import finished successfully, execute the **drmsqlcat** command.

```
PROMPT> drmsqlcat SQL1
INSTANCE: SQL1
BACKUP-ID: 0000000002 BACKUP-MODE: ON-LINE INSTANCE: SQL1 ORIGINAL-ID: 0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: SQL1
T  DB   OBJECT    FILE             FS  DG  DEVICE     COPY-GROUP
M  DB1  METAFILE  C:\METADIR\Meta1 C:  -   -          -
D  DB1  DATAFILE  D:\SQL\data1     D:  -   Harddisk1  SQL001,B001
-  -    -         -                -   -   -          SQL001,B001
T  DB1  TRANSACT  E:\SQL\tlog      E:  -   Harddisk2  SQL002,B001
-  -    -         -                -   -   -          SQL002,B001
PROMPT>
```

10. Restore the data on the secondary volume to the primary volume. Resynchronize the primary and secondary volumes. To perform the resynchronization, execute the **drmsqlrestore** command on the database server.

```
PROMPT> drmsqlrestore 0000000002 -resync
KAVX0001-I The drmsqlrestore command will now start.
KAVX1316-I Performing restore pre-processing...
KAVX1000-I Logged on to the SQL Server system.
KAVX1300-I Restore processing will now start.
KAVX1000-I Logged on to the SQL Server system.
KAVX1301-I Restore processing has finished.
KAVX1318-I Performing restore post-processing..
KAVX1001-I Logged off from the SQL Server system.
KAVX0002-I The drmsqlrestore command will now end.
PROMPT>
```

11. Perform recovery for SQL Server database. To apply the transaction log and recover the SQL Server database, execute the **drmsqlrecover** or **drmsqlrecovertool** command on the database server.

    – Using the **drmsqlrecover** command:

```
PROMPT> drmsqlrecover SQL1
KAVX0001-I The drmsqlrecover command will now start.
KAVX1017-I SQL Server information is being collected now.
KAVX1302-I Recovery processing will now start.
KAVX1303-I Recovery processing has finished.
KAVX0002-I The drmsqlrecover command will now end.
PROMPT>
```

    – Using the **drmsqlrecovertool** command:

```
PROMPT> drmsqlrecovertool SQL1
PROMPT>
```

    When you execute this command, the **drmsqlrecovertool** dialog box appears. For details about the **drmsqlrecovertool** dialog box, see section 6.5.7.

### 5.5.4 Recovering SQL Server Transaction Logs

This subsection describes how to recover transaction logs. There are two methods you can use to recover transaction logs:

- Recovery using the **drmsqlrecovertool** dialog box. For details about the **drmsqlrecovertool** dialog box, see section 6.5.7.
- Recovery using the **drmsqlrecover** command

**(1) Recovery using the drmsqlrecovertool dialog box**

To recover transaction logs using the **drmsqlrecovertool** dialog box:

1. Execute the **drmsqlrecovertool** command, specifying the instance name. The **drmsqlrecovertool** dialog box is displayed when you execute the command.
   ```
   PROMPT> drmsqlrecovertool sql1
   ```
2. From **Target database**, select the database to be recovered.
3. Select the backup file of a transaction log you wish to recover. Click the **Add** button to select a transaction log backup file from the Browse for File dialog box that is displayed. The selected transaction log backup file appears in the **Transaction log back list**. An asterisk (*) appears next to each displayed file whose recovery is complete.
4. Select the recovery mode and whether to roll forward. Use **Recovery mode** to select the recover mode, and use **Roll Forward?** to select whether to roll forward.
5. Click the **Recover** button. The transaction log of the selected backup file is recovered. After recovery is complete, an asterisk appears next to the file name displayed in **Transaction log backup list**.

**(2) Recovery using the drmsqlrecover command**

To recover transaction logs using the **drmsqlrecover** command:

1. Create a file that lists backed-up transaction logs. You can create a file that lists backed-up transaction logs for recovery. When you execute the following command with an instance name and the **-v** option specified, the command displays the latest backup ID as the base point for recovery. If you want to change the base point, specify the backup ID you want to use as the base point.
   ```
   PROMPT> drmsqllogbackup SQL1 -target DB1 -v > C:\temp\SQLTXLOG.txt
   ```
2. Use the created list file to recover SQL Server database.
   ```
   PROMPT> drmsqlrecover SQL1 -target DB1 -transact_log_list C:\temp\SQLTXLOG.txt
   ```

## 5.6 Backing up, Restoring, and Recovering an SQL Server DB (from a different host)

This section uses an example to explain how to restore and recover SQL Server database data from a host other than the host that was used to make the backup. This explanation assumes the system configurations shown in Figure 5.6 and Figure 5.7.

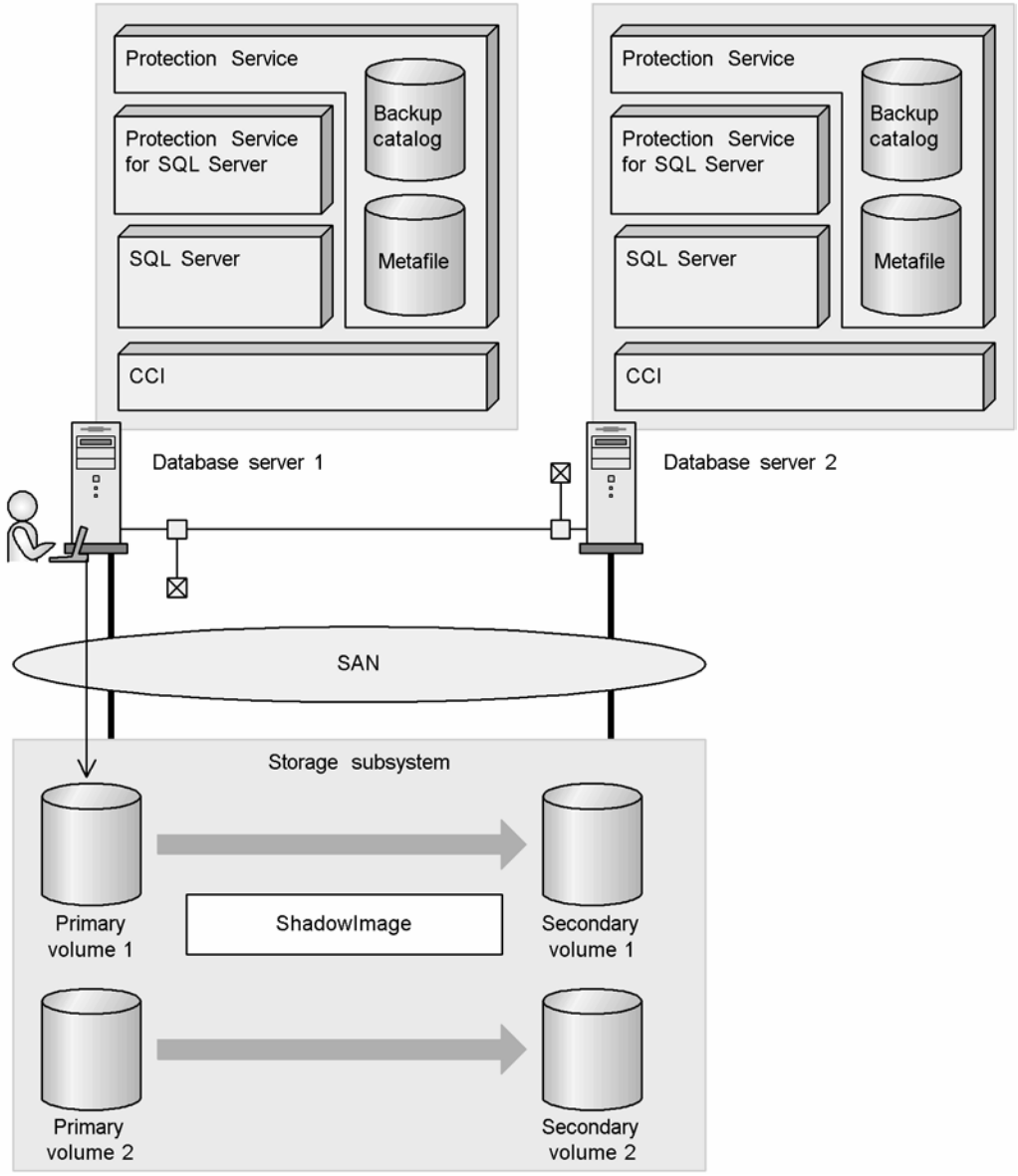



**Figure 5.6 System Configuration: Restoring and Recovering from a Different Host (backup)**

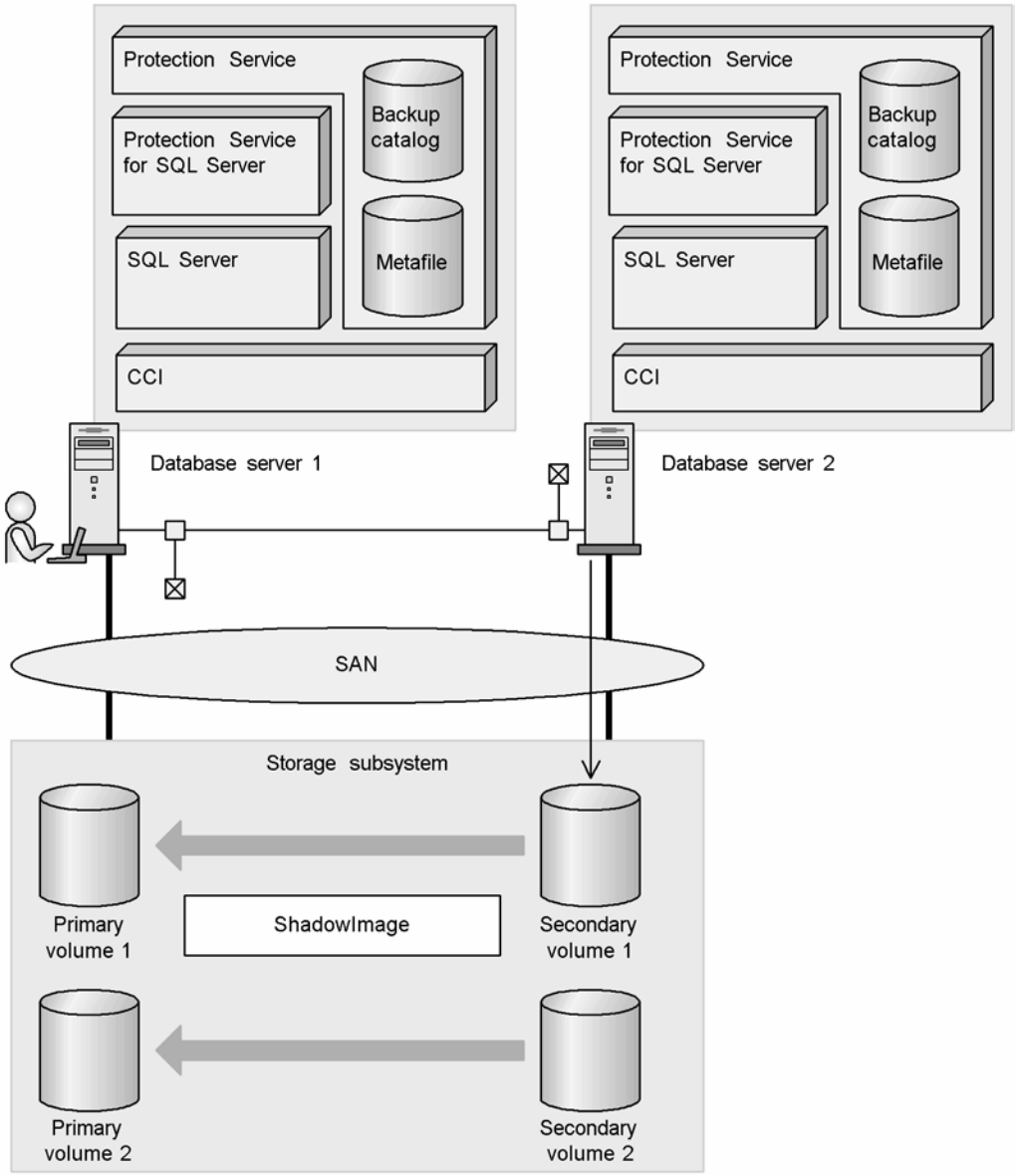



**Figure 5.7 System Configuration: Restoring and Recovering from a Different Host (restoring)**

The following assumptions are used:

- The primary volumes are formatted with **NTFS**, and are mounted on the **D** and **E** drives. Both volumes are used for SQL Server database. A volume used for storing data files cannot also be used to store logs.
- The primary and secondary volumes are mirrored (as set by the volume replication function and CCI).
- A metafile and backup catalog are on the server to be restored.
- The metafile pathnames are the same on both database server 1 and database server 2.
- The system database is not specified when restoring.
- The **drmsqlinit** command and the **drmsqldisplay -refresh** command have been executed on the server to be restored.
- An instance has been created on the server to be restored that is the same as the one on database server 1.
- For restoring, the primary volumes are mounted on database server 2.

To restore and recover SQL Server database data from a host that was not used to perform the backup:

1. Back up SQL Server database to the secondary volumes. To back up SQL Server database online, execute the **drmsqlbackup** command.

```
PROMPT> drmsqlbackup SQL1
KAVX0001-I The drmsqlbackup command will now start.
KAVX1017-I SQL Server information is being collected now.
KAVX1207-I Backing up the database...
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000001
KAVX0002-I The drmsqlbackup command will now end.
PROMPT>
```

   When you execute this command, the backup information is registered into the backup catalog on database server 1 under a new backup ID (the next unused ID). The following assumes that the new backup ID is **0000000001**.

2. Check the backup execution results. To confirm that backup to the secondary volumes finished successfully, execute the **drmsqlcat** command.

```
PROMPT> drmsqlcat SQL1
INSTANCE: SQL1
BACKUP-ID: 0000000001 BACKUP-MODE: ON-LINE INSTANCE: SQL1 ORIGINAL-ID: 0000000001
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: SQL1
T  DB   OBJECT    FILE             FS  DG  DEVICE     COPY-GROUP
M  DB1  METAFILE  C:\METADIR\Meta1 C:  -   -          -
D  DB1  DATAFILE  D:\SQL\data1     D:  -   Harddisk1  SQL001,B001
-  -    -         -                -   -   -          SQL001,B001
T  DB1  TRANSACT  E:\SQL\tlog      E:  -   Harddisk2  SQL002,B001
-  -    -         -                -   -   -          SQL002,B001
PROMPT>
```

3. Export the backup information to a temporary file. You must copy to database server 2 the information pertaining to the operations performed in backing up the primary volumes to the secondary volumes. Execute the **drmdbexport** command to export the information pertaining to the backup operations to the temporary file **C:\temp\EX-FILE1.drm**.

```
PROMPT> drmdbexport 0000000001 -f C:\temp\EX-FILE1.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
PROMPT>
```

4. Transfer the exported temporary file from database server 1 to database server 2. Use the **ftp** command to transfer the exported temporary file **C:\temp\EX-FILE1.drm** from database server 1 to database server 2.

```
PROMPT> ftp database-server2-name
ftp> Username: (logon-name)
ftp> password: (password)
ftp> put C:\temp\EX-FILE1.drm
ftp> quit
PROMPT>
```

5. Import the temporary file transferred from database server 1 **C:\temp\EX-FILE1.drm** into the backup catalog on database server 2. To import the file, execute the **drmdbimport** command on database server 2.

```
PROMPT> drmdbimport -f C:\temp\EX-FILE1.drm
KAVX0001-I The drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000001
KAVX0002-I The drmdbimport command will now end.
PROMPT>
```

6. Check the import results. To confirm that the import finished successfully, execute the **drmsqlcat** command on database server 2.

```
PROMPT> drmsqlcat SQL1
INSTANCE: SQL1
BACKUP-ID: 0000000001 BACKUP-MODE: ON-LINE INSTANCE: SQL1 ORIGINAL-ID: 0000000001
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: SQL1
T  DB   OBJECT    FILE             FS  DG  DEVICE     COPY-GROUP
M  DB1  METAFILE  C:\METADIR\Meta1 C:  -   -          -
D  DB1  DATAFILE  D:\SQL\data1     D:  -   Harddisk1  SQL001,B001
-  -    -         -                -   -   -          SQL001,B001
T  DB1  TRANSACT  E:\SQL\tlog      E:  -   Harddisk2  SQL002,B001
-  -    -         -                -   -   -          SQL002,B001
PROMPT>
```

7. Restore the data on the secondary volumes to the primary volumes. To restore the data and resynchronize the primary and secondary volumes, execute the **drmsqlrestore** command on database server 2.

```
PROMPT> drmsqlrestore 0000000001 -resync -nochk_host
KAVX0001-I The drmsqlrestore command will now start.
KAVX1316-I Performing restore pre-processing...
KAVX1000-I Logged on to the SQL Server system.
KAVX1300-I Restore processing will now start.
KAVX1000-I Logged on to the SQL Server system.
KAVX1301-I Restore processing has finished.
KAVX1318-I Performing restore post-processing...
KAVX1001-I Logged off from the SQL Server system.
KAVX0002-I The drmsqlrestore command will now end.
PROMPT>
```

8. Recover SQL Server database. To recover SQL Server database, execute the **drmsqlrecover** or **drmsqlrecovertool** command on database server 2.

   – Using the **drmsqlrecover** command:

   ```
   PROMPT> drmsqlrecover SQL1
   KAVX0001-I The drmsqlrecover command will now start.
   KAVX1017-I SQL Server information is being collected now.
   KAVX1302-I Recovery processing will now start.
   KAVX1303-I Recovery processing has finished.
   KAVX0002-I The drmsqlrecover command will now end.
   PROMPT>
   ```

   – Using the **drmsqlrecovertool** command:

   ```
   PROMPT> drmsqlrecovertool SQL1
   PROMPT>
   ```

   When you execute this command, the **drmsqlrecovertool** dialog box appears. For details about the **drmsqlrecovertool** dialog box, see section 6.5.7.

## 5.7 Using the SQL Server Log-Shipping Functionality

### 5.7.1 Before Using the SQL Server Log-Shipping Functionality

This section explains the example of synchronizing the database on the source server and the database on the distribution server and setting logship operations on the source server, before using the log-shipping functionality for Microsoft SQL Server database 2000 Enterprise Edition. This explanation assumes the system configuration shown in Figure 5.8.

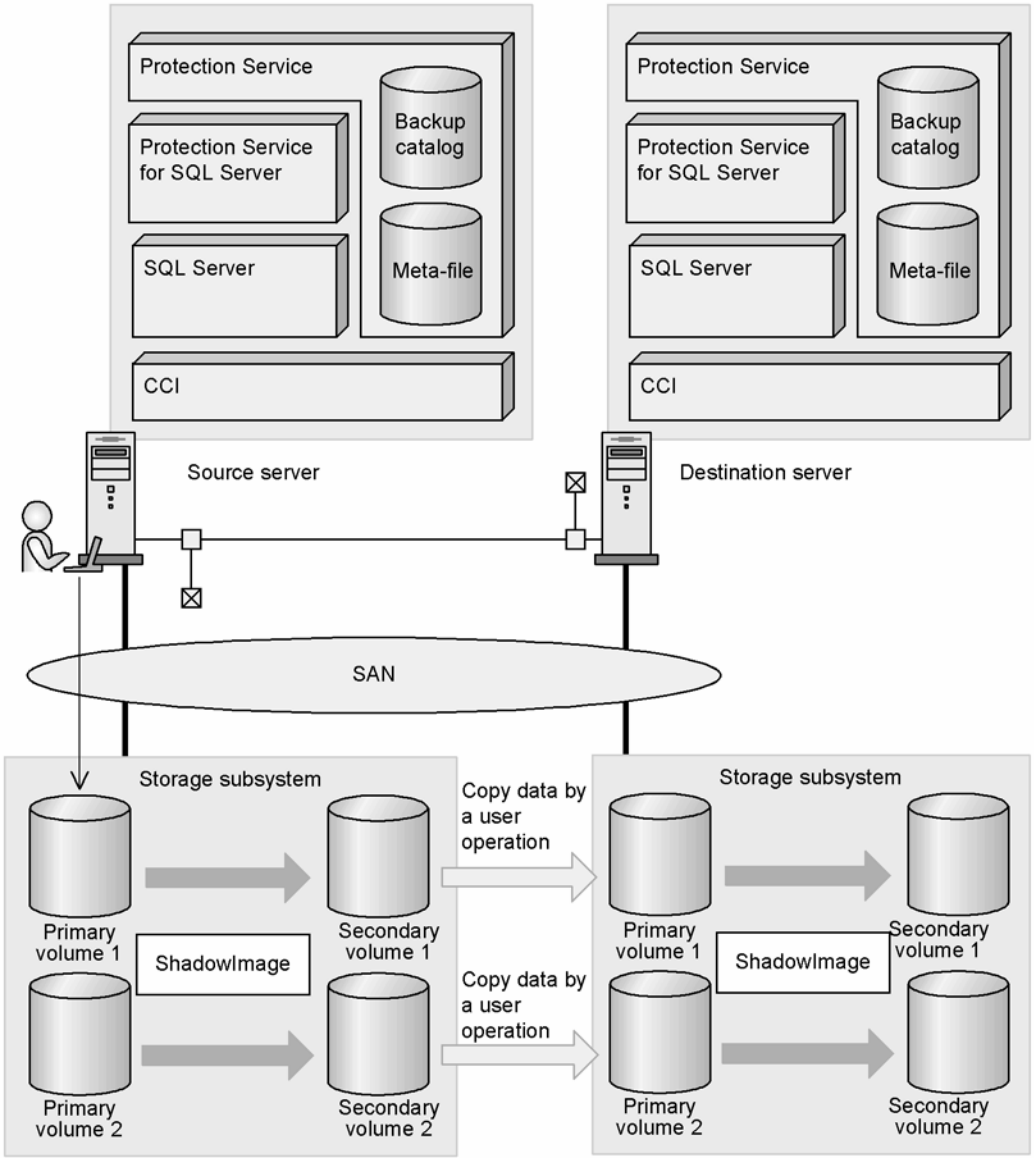



**Figure 5.8 System Configuration: SQL Server Logship Operations**

The following assumptions are used:

- The primary volumes on the source server and the volumes on the distribution target server are formatted with **NTFS**, and are mounted on the **D** and **E** drives, respectively.
- The primary and secondary volumes on the source server are mirrored (as set by the volume replication function and CCI).
- The secondary volumes on the source server are formatted with **NTFS**, and are not mounted.
- The **drmsqlinit** command has been executed on the distribution target server.
- The same instance has been created on both the source server and the distribution target server.
- The FTP server is running.
- The system database is not specified when restoring.

The following explains the procedure for synchronizing the database on the source server and the database on the distribution server and setting logship operations on the source server.

To set logship operations on the source server:

1. Back up SQL Server database to the secondary volumes. To back up SQL Server database online, execute the **drmsqlbackup** command on the source server.

```
PROMPT> drmsqlbackup SQL1
KAVX0001-I The drmsqlbackup command will now start.
KAVX1017-I SQL Server information is being collected now.
KAVX1207-I Backing up the database...
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000001
KAVX0002-I The drmsqlbackup command will now end.
PROMPT>
```

   When you execute this command, the backup information is registered into the backup catalog on the source server under a new backup ID (the next unused ID). The following assumes that the new backup ID is **0000000001**.

2. Check the backup execution results. To confirm that backup to the secondary volumes finished successfully, execute the **drmsqlcat** command on the source server.

```
PROMPT> drmsqlcat SQL1
INSTANCE: SQL1
BACKUP-ID: 0000000001 BACKUP-MODE: ON-LINE INSTANCE: SQL1 ORIGINAL-ID: 0000000001
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: SQL1
T  DB   OBJECT    FILE             FS  DG  DEVICE     COPY-GROUP
M  DB1  METAFILE  C:\METADIR\Meta1 C:  -   -          -
D  DB1  DATAFILE  D:\SQL\data1     D:  -   Harddisk1  SQL001,B001
-  -    -         -                -   -   -          SQL001,B001
T  DB1  TRANSACT  E:\SQL\tlog      E:  -   Harddisk2  SQL002,B001
-  -    -         -                -   -   -          SQL002,B001
PROMPT>
```

3. Export the backup information to a temporary file. You must copy to the distribution target server the information pertaining to the operations performed in backing up the primary volumes to the secondary volumes. Execute the **drmdbexport** command on the source server to export the information pertaining to the backup operations to the temporary file **C:\temp\EX-FILE1.drm**.

```
PROMPT> drmdbexport 0000000001 -f C:\temp\EX-FILE1.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
PROMPT>
```

4. Transfer the metafile and the temporary file from the source server to the distribution target server. Use the **ftp** command to transfer the metafile **C:\METADIR\Meta1** and the exported temporary file **C:\temp\EX-FILE1.drm** from the source server to the distribution target server.

```
PROMPT> ftp distribution-destination-server-name
ftp> Username: (logon-name)
ftp> password: (password)
ftp> put C:\temp\EX-FILE1.drm
ftp> put C:\METADIR\Meta1
ftp> quit
PROMPT>
```

5. Copy the backup data. Copy to the distribution target server volumes the data that was backed up to the secondary volumes in step 1.

6. Import the temporary file into the backup catalog on the distribution target server. To import the temporary file **C:\temp\EX-FILE1.drm** (transferred from the source server in step 4) into the backup catalog on the distribution target server, execute the **drmdbimport** command on the distribution target server.

```
PROMPT> drmdbimport -f C:\temp\EX-FILE1.drm
KAVX0001-I The drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000001
KAVX0002-I The drmdbimport command will now end.
PROMPT>
```

7. Check the import results. To confirm that the import finished successfully, execute the **drmsqlcat** command on the distribution target server.

```
PROMPT> drmsqlcat SQL1
INSTANCE: SQL1
BACKUP-ID: 0000000001 BACKUP-MODE: ON-LINE INSTANCE: SQL1 ORIGINAL-ID: 0000000001
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: SQL1
T  DB   OBJECT    FILE             FS  DG  DEVICE     COPY-GROUP
M  DB1  METAFILE  C:\METADIR\Meta1 C:  -   -          -
D  DB1  DATAFILE  D:\SQL\data1     D:  -   Harddisk1  SQL001,B001
-  -    -         -                -   -   -          SQL001,B001
T  DB1  TRANSACT  E:\SQL\tlog      E:  -   Harddisk2  SQL002,B001
-  -    -         -                -   -   -          SQL002,B001
PROMPT>
```

8. Restore the backup data to the distribution target server volumes. Check that the backup data has been copied to the distribution target server volumes, and then restore the backup data from the distribution target server. When restoring, apply the metafile to the backup data without recovering the backup data from the secondary volumes to the primary volumes, and place the database into standby status. To restore in this manner, execute the **drmsqlrestore** command as shown below:

```
PROMPT> drmsqlrestore 0000000001 -no_resync -undo -nochk_host
KAVX0001-I The drmsqlrestore command will now start.
KAVX1316-I Performing restore pre-processing...
KAVX1000-I Logged on to the SQL Server system.
KAVX1300-I Restore processing will now start.
KAVX1000-I Logged on to the SQL Server system.
KAVX1301-I Restore processing has finished.
KAVX1318-I Performing restore post-processing...
KAVX1001-I Logged off from the SQL Server system.
KAVX0002-I The drmsqlrestore command will now end.
PROMPT>
```

9. Set up logship operation on the source server. For information on how to set up logship operation, see the SQL Server documentation.

### 5.7.2 Setting a Distribution Target Server to be an Operating Server

This section uses an example to explain how to set a distribution target server to be an operating server when using the log-shipping functionality for Microsoft SQL Server 2000 Enterprise Edition, if such is required due to a failure on the source server during logship operation or for some other reason. This explanation assumes the system configuration shown in Figure 5.9.

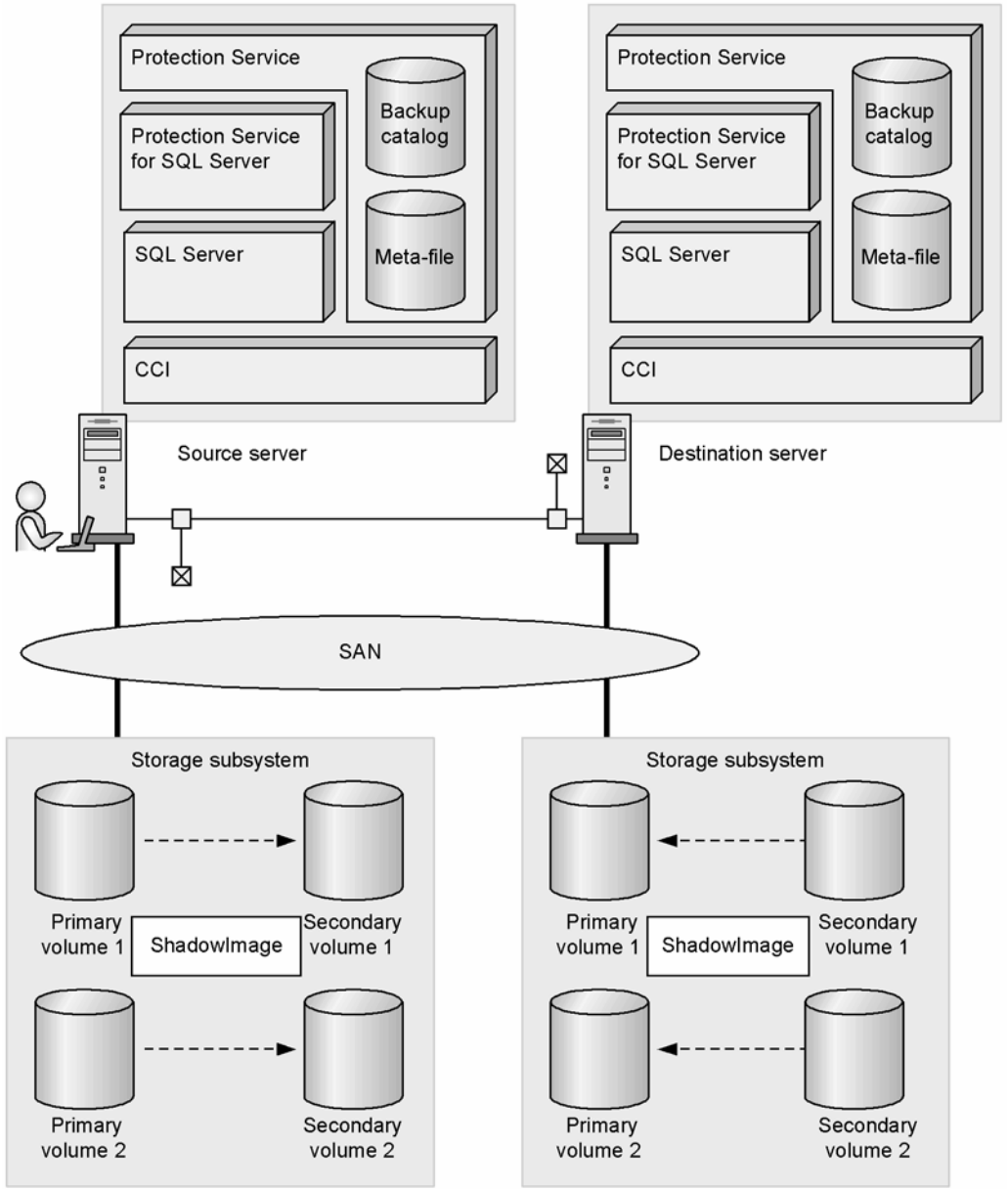



**Figure 5.9 System Configuration: Setting a Distribution Target Server as an Operating Server**

The following assumptions are used:

- The distribution target server volumes are formatted with **NTFS**, and are mounted on the **D** and **E** drives.
- The **drmsqlinit** command has been executed on the distribution target server.
- The system database is not specified when restoring.
- The database on the distribution target server is in the standby status.

To set a distribution target server to be an operation server:

1. Recover SQL Server database. To recover SQL Server database, execute the **drmsqlrecover** command on the distribution target server.
```
PROMPT> drmsqlrecover SQL1
KAVX0001-I The drmsqlrecover command will now start.
KAVX1302-I Recovery processing will now start.
KAVX1303-I Recovery processing has finished.
KAVX0002-I The drmsqlrecover command will now end.
PROMPT>
```
2. Place the standby database online. To use a Protection Services command after restoring the database, execute **drmsqldisplay -refresh**.

## 5.8 Backing Up, Restoring, and Recovering Storage Groups (online backup to tape)

This section explains by way of examples how to perform online backup of storage groups to tape, how to restore that data to a database server, and how to recover that data from the database. These explanations assume the system configuration shown in Figure 5.10.

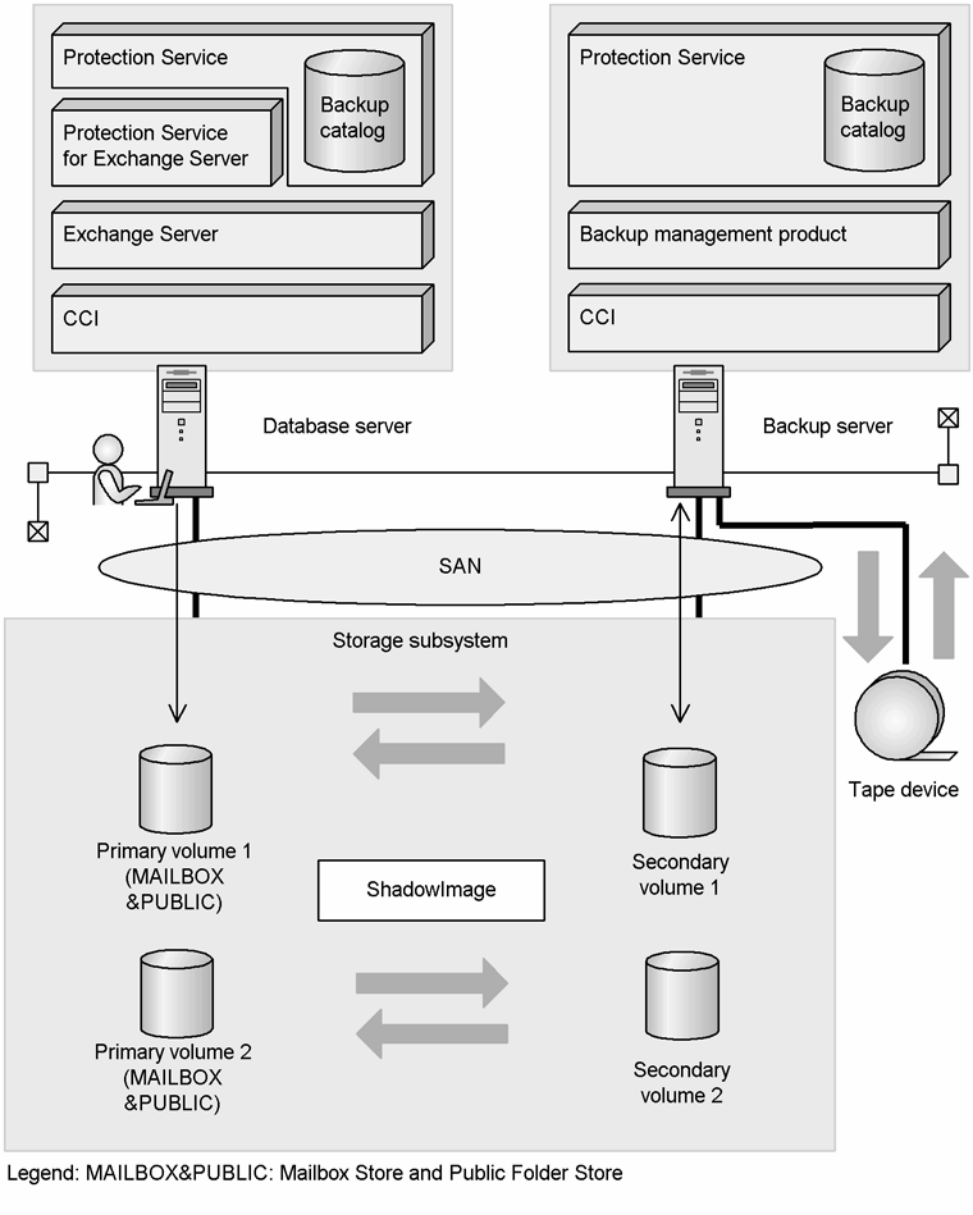



**Figure 5.10 System Configuration: Online Tape Backup and Restoration (Exchange)**

The following assumptions are used:

- The primary volumes are formatted with NTFS.
- Different volumes are used for the information store and transaction log file.
- The primary and secondary volumes are mirrored (as set by the volume replication function and CCI).
- A backup management product is installed on the backup server.
- Parameters for the backup management product have been registered with the drmtapeinit command.
- The primary and secondary volumes are configured as described in Table 5.1.

**Table 5.1 Correspondence of Primary and Secondary Volumes (online backup on storage groups)**

| Primary Volume (mount drive) | Object to be Stored | Secondary Volume (mount drive) |
|---|---|---|
| Primary volume 1 (**D:**) | Mailbox store and public folder store of storage group **STR1** | Secondary volume 1 (**W:**) |
| Primary volume 2 (**F:**) | Mailbox store and public folder store of storage group **STR2** | Secondary volume 2 (**Y:**) |

### 5.8.1 Backing Up Storage Groups (Exchange Server online backup)

This section explains how to perform online backup of storage groups onto tape. First, you perform online backup of data from the primary volume to the secondary volume, and then you back up the data from the secondary volume to tape. A new backup is possible only after the backup data has been stored onto tape.

In this example, storage groups **STR1** and **STR2** are backed up in order.

To perform an online backup of storage groups to tape:

1. Before backing up storage group **STR1**, clear the system cache on the backup server. To clear the system cache, first mount and then unmount the secondary volume.

```
PROMPT> drmmount -copy_group EXG001,B001 -mount_pt W:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = W:
KAVX0401-I Mounting has finished.
           Mount point = W:
KAVX0002-I The drmmount command will now end.
PROMPT> drmumount -copy_group EXG001,B001
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = W:
KAVX0407-I Unmounting has finished.
           Mount point = W:
KAVX0002-I The drmumount command will now end.
```

2. Back up storage group **STR1** online. To perform the backup, use the **drmexgbackup** command.

```
PROMPT> drmexgbackup -mode online -target STR1
KAVX0001-I The drmexgbackup command will now start.
KAVX1600-I Backup processing will now start.
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000001
KAVX1601-I Backup processing has finished.
KAVX0002-I The drmexgbackup command will now end.
```

   When you execute this command, the backup information is registered into the backup catalog on the database server under a new backup ID (the next unused ID). The following assumes that the new backup ID is **0000000001**.

3. Check the results of the backup operation performed on storage group **STR1**. To confirm that backup to the secondary volume finished successfully, execute the **drmexgcat** command.

```
PROMPT> drmexgcat -target STR1
STORAGEGROUP: STR1
BACKUP-ID:0000000001 BACKUP-MODE: ONLINE STORAGEGROUP: STR1 ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:01:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.edb       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.stm       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.edb        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.stm        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
```

4. Before backing up storage group **STR2**, clear the system cache on the backup server. To clear the system cache, first mount and then unmount the secondary volume.

```
PROMPT> drmmount -copy_group EXG001,B002 -mount_pt Y:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = Y:
KAVX0401-I Mounting has finished.
           Mount point = Y:
KAVX0002-I The drmmount command will now end.
PROMPT> drmumount -copy_group EXG001,B002
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = Y:
KAVX0407-I Unmounting has finished.
           Mount point = Y:
KAVX0002-I The drmumount command will now end.
```

5. Back up storage group **STR2** online. To perform the backup, use the **drmexgbackup** command.

```
PROMPT> drmexgbackup -mode online -target STR2
KAVX0001-I The drmexgbackup command will now start.
KAVX1600-I Backup processing will now start.
KAVX0040-I The backup ID has been assigned as follows.
Backup ID = 0000000002
KAVX1601-I Backup processing has finished.
KAVX0002-I The drmexgbackup command will now end.
```

   When you execute this command, the backup information is registered into the backup catalog on the database server under a new backup ID (the next unused ID). The following assumes that the new backup ID is **0000000002**.

6. Check the results of backing up storage group **STR2**. To confirm that backup to the secondary volume finished successfully, execute the **drmexgcat** command.

```
PROMPT> drmexgcat -target STR2
STORAGEGROUP: STR2
BACKUP-ID:0000000002 BACKUP-MODE: ONLINE STORAGEGROUP: STR2 ORIGINAL-ID:0000000002
START-TIME:2002/06/01 10:30:00 END-TIME: 2002/06/01 10:31:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.edb       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.stm       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.edb        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.stm        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
```

7. Export the backup information from storage groups **STR1** and **STR2** to temporary files. To back up from the secondary volumes to tape, you must copy to the backup server the information pertaining to the operations performed in backing up from the primary volumes to the secondary volumes. Execute the **drmdbexport** command to export the backup information of **STR1** to **C:\temp\0000000001.drm**, and the backup information of **STR2** to **C:\temp\0000000002.drm**.

```
PROMPT> drmdbexport 0000000001 -f C:\temp\0000000001.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
PROMPT> drmdbexport 0000000002 -f C:\temp\0000000002.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
```

8. Transfer the exported temporary files from the database server to the backup server. Use the **ftp** command to transfer the exported temporary files **C:\temp\0000000001.drm** and **C:\temp\0000000002.drm** from the database server to the backup server. The following assumes that the FTP root folder is **C:\FTP_ROOT**, and that the temporary files will be transferred to the backup server as **C:\FTP_ROOT\0000000001.drm** and **C:\FTP_ROOT\0000000002.drm**, respectively.

```
PROMPT> ftp backup-server-name
ftp> Username: (logon-name)
ftp> password: (password)
ftp> put C:\temp\0000000001.drm
ftp> put C:\temp\0000000002.drm
ftp> quit
```

9. Import the temporary file of storage group **STR1** into the backup catalog on the backup server. To import temporary file **C:\FTP_ROOT\0000000001.drm** (transferred from the database server in step 8) into the backup catalog on the backup server, execute the **drmdbimport** command on the backup server.

```
PROMPT> drmdbimport -f C:\FTP_ROOT\0000000001.drm
KAVX0001-I The drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
          Imported backup ID = 0000000001
KAVX0002-I The drmdbimport command will now end.
```

10. Check the results of importing the temporary file of storage group **STR1**. To confirm that the import finished successfully, execute the **drmexgcat** command on the backup server.

```
PROMPT> drmexgcat -target STR1
STORAGEGROUP: STR1
BACKUP-ID:0000000001 BACKUP-MODE: ONLINE STORAGEGROUP: STR1 ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:01:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.edb       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.stm       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.edb        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.stm        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
```

11. Import the temporary file of storage group **STR2** into the backup catalog on the backup server. To import the temporary file **C:\FTP_ROOT\0000000002.drm** (transferred from the database server in step 8) into the backup catalog on the backup server, execute the **drmdbimport** command on the backup server.

```
PROMPT> drmdbimport -f C:\FTP_ROOT\0000000001.drm
KAVX0001-I The drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000001
KAVX0002-I The drmdbimport command will now end.
```

12. Check the results of importing the temporary file of storage group **STR2**. To confirm that the import finished successfully, execute the **drmexgcat** command on the backup server.

```
PROMPT> drmexgcat -target STR2
STORAGEGROUP: STR2
BACKUP-ID:0000000002 BACKUP-MODE: ONLINE STORAGEGROUP: STR2 ORIGINAL-ID:0000000002
START-TIME:2002/06/01 10:30:00 END-TIME: 2002/06/01 10:31:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.edb       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.stm       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.edb        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.stm        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
```

13. Mount the secondary volume that contains storage group **STR1** onto the backup server. Specify the backup ID **0000000001** assigned during importing.

```
PROMPT> drmmount 0000000001 -mount_pt W:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = W:
KAVX0401-I Mounting has finished.
           Mount point = W:
KAVX0002-I The drmmount command will now end.
```

14. Check the consistency of the Exchange database for the storage group **STR1**. Specify the backup ID **0000000001** assigned during importing.

```
PROMPT> drmexgverify 0000000001
KAVX0001-I The drmexgverify command will start.
KAVX1650-I The checksum of the Exchange database file was confirmed.
           Storage group name = STR1
KAVX0002-I The drmexgverify command will now end.
```

15. Back up the backup data of storage group **STR1** from the secondary volume to tape. To back up, execute the **drmmediabackup** command on the backup server.

```
PROMPT> drmmediabackup 0000000001
KAVX0001-I The drmmediabackup command will now start.
KAVX0402-I Backup processing will now start.
           To see more details on backup progress, use the monitoring method of
the backup management product.
           Source = W:
KAVX0403-I Backup processing has finished.
           Source = W:
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000003
KAVX0002-I The drmmediabackup command will now end.
```

    When backup is performed, information pertaining to the backup operations is registered into the backup catalog under the new backup ID **0000000003**.

16. Check the results of backing up storage group **STR2** to tape. To confirm that the backup finished successfully, execute the **drmtapecat** command on the backup server.

```
PROMPT> drmtapecat –backup_id 0000000003
BACKUP-ID   BACKUP-OBJECT    SNAPSHOT TIME        EXPIRATION TIME
BACKUP-MEDIA
0000000003  MSEXCHANGE       2002/06/01 11:00:00  2002/06/02 11:00:00  MEDIA1
```

17. Unmount the secondary volume. To unmount the secondary volume, specify the backup ID used when mounting **0000000001**.

```
PROMPT> drmumount 0000000001
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = W:
KAVX0407-I Unmounting has finished.
           Mount point = W:
KAVX0002-I The drmumount command will now end.
```

18. Mount the secondary volume that contains storage group **STR2** onto the backup server. Specify the backup ID **0000000002** assigned during importing.

```
PROMPT> drmmount 0000000002
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = Y:
KAVX0401-I Mounting has finished.
           Mount point = Y:
KAVX0002-I The drmmount command will now end.
```

19. Check the consistency of the Exchange database for the storage group **STR2**. Specify the backup ID **0000000002** assigned during importing.

```
PROMPT> drmexgverify 0000000002
KAVX0001-I The drmexgverify command will start.
KAVX1650-I The checksum of the Exchange database file was confirmed.
           Storage group name = STR2
KAVX0002-I The drmexgverify command will now end.
```

20. Back up the backup data of storage group **STR2** from the secondary volume to tape. To back up, execute the **drmmediabackup** command on the backup server.

```
PROMPT> drmmediabackup 0000000002
KAVX0001-I The drmmediabackup command will now start.
KAVX0402-I Backup processing will now start.
           To see more details on backup progress, use the monitoring method of
the backup management product.
           Source = Y:
KAVX0403-I Backup processing has finished.
           Source = Y:
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000004
KAVX0002-I The drmmediabackup command will now end.
```

When backup is performed, information pertaining to the backup operations is registered into the backup catalog under the new backup ID **0000000004**.

21. Check the results of backing up storage group **STR2**. To confirm that the backup finished successfully, execute the **drmtapecat** command on the backup server.

```
PROMPT> drmtapecat -backup_id 0000000004
BACKUP-ID   BACKUP-OBJECT    SNAPSHOT TIME        EXPIRATION TIME
BACKUP-MEDIA
0000000004  MSEXCHANGE       2002/06/02 11:00:00  2002/06/03 11:00:00  MEDIA2
```

22. Unmount the secondary volume. To unmount the secondary volume, specify the backup ID used when mounting **0000000002**.

```
PROMPT> drmumount 0000000002
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = Y:
KAVX0407-I Unmounting has finished.
           Mount point = Y:
KAVX0002-I The drmumount command will now end.
```

### 5.8.2 Restoring and Recovering Storage Groups (Exchange Server online backup)

This section explains how to restore data that has been backed up to tape online. To do so, you first restore the data from tape to the secondary volume, resynchronize the secondary volume to the primary volume and restore the secondary volume, and then recover the storage groups.

To restore storage groups from tape:

1. Check the backup ID of the backup data. To check the backup ID of the backup data to be used to restore, execute the **drmtapecat** command on the backup server.

```
PROMPT> drmtapecat
BACKUP-ID   BACKUP-OBJECT    SNAPSHOT TIME        EXPIRATION TIME
BACKUP-MEDIA
0000000003  MSEXCHANGE       2002/06/01 11:00:00  2002/06/02 11:00:00  MEDIA1
0000000004  MSEXCHANGE       2002/06/02 11:00:00  2002/06/03 11:00:00  MEDIA2
```

2. Mount the secondary volume that contains storage group **STR1** onto the backup server. Specify the backup ID **0000000003** used on tape.

```
PROMPT> drmmount 0000000003 -mount_pt W:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = W:
KAVX0401-I Mounting has finished.
           Mount point = W:
KAVX0002-I The drmmount command will now end.
```

3. Restore the backup data of storage group **STR1** from tape to the secondary volume. To restore, execute the **drmmediarestore** command on the backup server.

```
PROMPT> drmmediarestore 0000000003
KAVX0001-I The drmmediarestore command will now start.
KAVX0404-I Restoration will now start.
           To see more details on restoration progress, use the monitoring method
of the backup management product.
           Source = W:
           Target = W:
KAVX0405-I Restoration has finished.
           Source = W:
           Target = W:
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000005
KAVX0002-I The drmmediarestore command will now end.
```

When the restoration is performed, information pertaining to the restoration operation is registered into the backup catalog on the backup server, under the new backup ID **0000000005**. At this point, because the status of the secondary volume will be updated, backup ID **0000000001**, which was used to manage the status of the secondary volume before the update, is deleted from the backup catalog on the backup server.

4. Check the results of restoring storage group **STR1** from tape to the secondary volume. To confirm that restoration finished successfully, execute the **drmexgcat** command on the backup server.

```
PROMPT> drmexgcat -target STR1
STORAGEGROUP: STR1
BACKUP-ID:0000000005 BACKUP-MODE: ONLINE STORAGEGROUP: STR1 ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:01:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.edb       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.stm       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.edb        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.stm        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
```

5. Unmount the secondary volume. To unmount the secondary volume, specify the backup ID used when mounting **0000000003**.

```
PROMPT> drmumount 0000000003
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = W:
KAVX0407-I Unmounting has finished.
           Mount point = W:
KAVX0002-I The drmumount command will now end.
```

6. Mount the secondary volume that contains storage group **STR2** onto the backup server. Specify the backup ID **0000000004** used on tape.

```
PROMPT> drmmount 0000000004 -mount_pt Y:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = Y:
KAVX0401-I Mounting has finished.
           Mount point = Y:
KAVX0002-I The drmmount command will now end.
```

7. Restore the backup data of storage group **STR2** from tape to the secondary volume. To restore, execute the **drmmediarestore** command on the backup server.

```
PROMPT> drmmediarestore 0000000004
KAVX0001-I The drmmediarestore command will now start.
KAVX0404-I Restoration will now start.
           To see more details on restoration progress, use the monitoring method
of the backup management product.
           Source = Y:
           Target = Y:
KAVX0405-I Restoration has finished.
           Source = Y:
           Target = Y:
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000006
KAVX0002-I The drmmediarestore command will now end.
```

When restoration is performed, information pertaining to the restoration operation is registered into the backup catalog on the backup server under the new backup ID **0000000006**. At this point, because the status of the secondary volume will be updated, backup ID **0000000002**, which was used to manage the status of the secondary volume before the update, is deleted from the backup catalog on the backup server.

8. Check the results of restoring storage group **STR2** from tape to the secondary volume. To confirm that restoration finished successfully, execute the **drmexgcat** command on the backup server.

```
PROMPT> drmexgcat -target STR2
STORAGEGROUP: STR2
BACKUP-ID:0000000006 BACKUP-MODE: ONLINE STORAGEGROUP: STR2 ORIGINAL-ID:0000000002
START-TIME:2002/06/01 10:30:00 END-TIME: 2002/06/01 10:31:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.edb       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.stm       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.edb        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.stm        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
```

9. Unmount the secondary volume. To unmount the secondary volume, specify the backup ID used when mounting **0000000004**.

```
PROMPT> drmumount 0000000004
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = Y:
KAVX0407-I Unmounting has finished.
           Mount point = Y:
KAVX0002-I The drmumount command will now end.
```

10. Export the backup information of storage groups **STR1** and **STR2** to temporary files. To restore from the secondary volumes to the primary volumes, you must copy to the database server the information pertaining to the operations performed in restoring from the primary volumes to the secondary volumes. Execute the **drmdbexport** command to export the backup information of **STR1** and **STR2** to the FTP root folder. The following assumes that the FTP root folder is **C:\FTP_ROOT**, that the backup information of **STR1** is exported to **C:\FTP_ROOT\0000000005.drm**, and that the backup information of **STR2** is exported to **C:\FTP_ROOT\0000000006.drm**.

```
PROMPT> drmdbexport 0000000005 -f C:\FTP_ROOT\0000000005.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
PROMPT> drmdbexport 0000000006 -f C:\FTP_ROOT\0000000006.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
```

11. Use the **ftp** command to transfer the temporary files **C:\FTP_ROOT\0000000005.drm** and **C:\FTP_ROOT\0000000006.drm** (exported from the backup server in step 10) to the database server. The temporary files will be stored in the current directory. The following assumes that the current directory is **C:**.

```
PROMPT> ftp backup-server-name
ftp> Username: (logon-name)
ftp> password: (password)
ftp> get 0000000005.drm
ftp> get 0000000006.drm
ftp> quit
```

12. Import the temporary file of storage group **STR1** into the backup catalog on the database server. To import the temporary file **C:\0000000005.drm** (transferred from the backup server in step 11), execute the **drmdbimport** command on the database server.

```
PROMPT> drmdbimport -f C:\0000000005.drm
KAVX0001-I The drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000003
KAVX0002-I The drmdbimport command will now end.
```

13. Check the results of importing the temporary file of storage group **STR1**. To confirm that the import finished successfully, execute the **drmexgcat** command on the database server.

```
PROMPT> drmexgcat -target STR1
STORAGEGROUP: STR1
BACKUP-ID:0000000003 BACKUP-MODE: ONLINE STORAGEGROUP: STR1 ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:01:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.edb       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.stm       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.edb        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.stm        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
```

14. Import the temporary file of storage group **STR2** into the backup catalog on the database server. To import the temporary file **C:\0000000006.drm** (transferred from the backup server in step 11), execute the **drmdbimport** command on the database server.

```
PROMPT> drmdbimport -f C:\0000000006.drm
KAVX0001-I The drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000004
KAVX0002-I The drmdbimport command will now end.
```

15. Check the results of importing the temporary file of storage group **STR2**. To confirm that the import finished successfully, execute the **drmexgcat** command on the database server.

```
PROMPT> drmexgcat -target STR2
STORAGEGROUP: STR2
BACKUP-ID:0000000004 BACKUP-MODE: ONLINE STORAGEGROUP: STR2 ORIGINAL-ID:0000000002
START-TIME:2002/06/01 10:30:00 END-TIME: 2002/06/01 10:31:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.edb       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.stm       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.edb        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.stm        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
```

16. Restore the data of the secondary volumes to the primary volumes, and recover the storage groups. Resynchronize and restore the primary and secondary volumes. In addition, apply the transaction logs to recover the storage groups. To restore and recover the storage groups, execute the **drmexgrestore** command on the database server.

```
PROMPT> drmexgrestore 0000000003 -resync -recovery
KAVX0001-I The drmexgrestore command will now start.
KAVX1805-I The information store will now be dismounted.
           Storage group name = STR1
KAVX1700-I Restore processing will now start.
KAVX1701-I Restore processing has finished.
KAVX1806-I The information store will not be mounted.
           Storage group name = STR1
KAVX0002-I The drmexgrestore command will now end.
PROMPT> drmexgrestore 0000000004 -resync -recovery
KAVX0001-I The drmexgrestore command will now start.
KAVX1805-I The information store will now be dismounted.
           Storage group name = STR2
KAVX1700-I Restore processing will now start.
KAVX1701-I Restore processing has finished.
KAVX1806-I The information store will not be mounted.
           Storage group name = STR2
KAVX0002-I The drmexgrestore command will now end.
```

## 5.9 Backing Up, Restoring, and Recovering Storage Groups (cold backup to tape)

This section explains by way of examples how to perform cold backup of storage groups to tape, how to restore that data to a database server, and how to recover that data from the database. These explanations assume the system configuration shown in Figure 5.11.

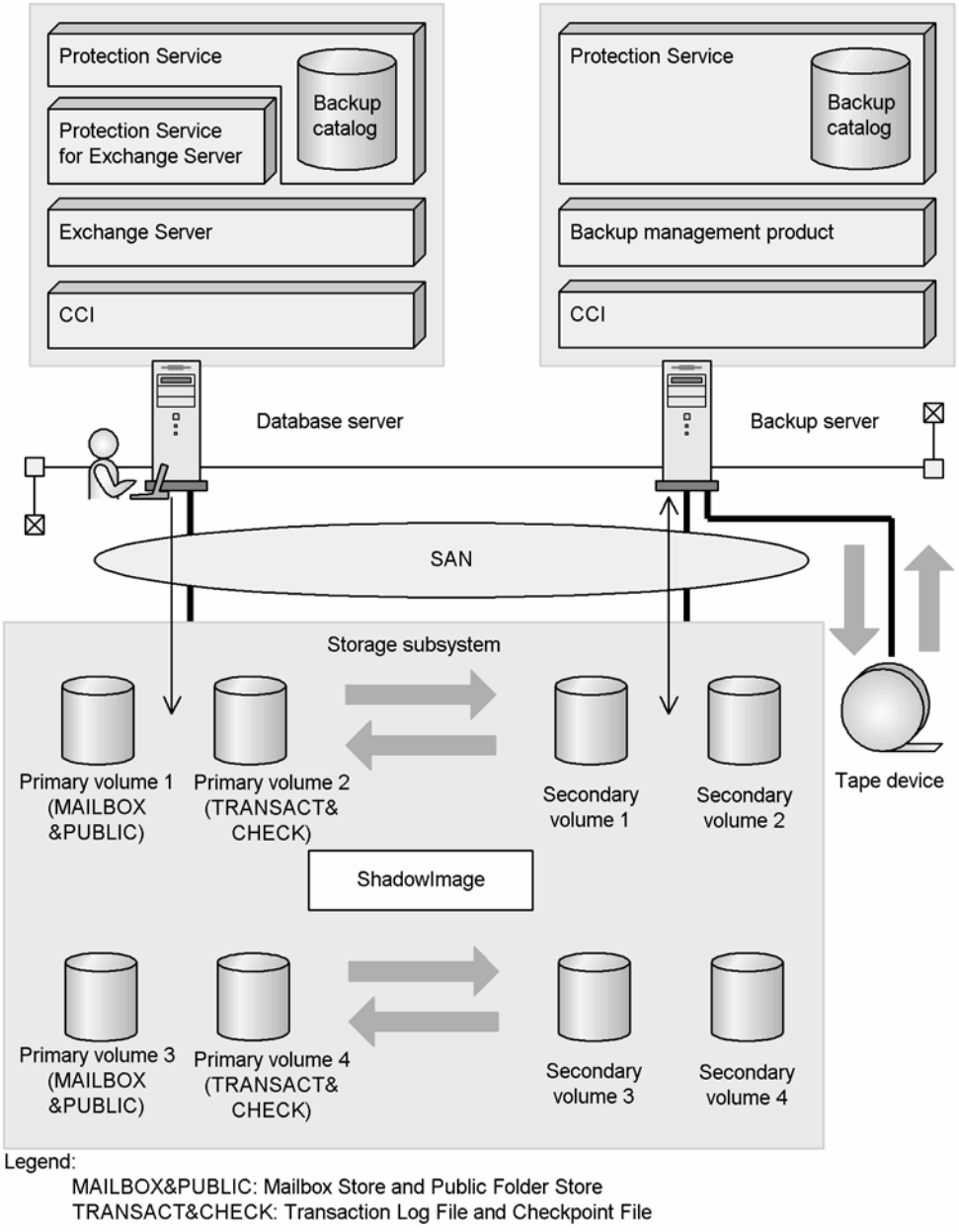



**Figure 5.11 System Configuration: Cold Backup to Tape and Restoration (Exchange)**

The following are assumed:

- The primary volume is formatted as NTFS.
- Different volumes are used for the information store and transaction log file.
- The primary volume and secondary volume are mirrored (as set by the volume replication function and CCI).
- A backup management product is installed on the backup server.
- Parameters for the backup management product have been registered using the **drmtapeinit** command.
- The primary and secondary volumes configured are in the structure shown in Table 5.2.

**Table 5.2 Correspondence of Primary Volume and Secondary Volume (cold backup on storage groups)**

| Primary Volume (mount drive) | Object to be Stored | Secondary Volume (mount drive) |
|---|---|---|
| Primary volume 1 (D:) | Mailbox store and public folder store of storage group STR1 | Secondary volume 1 (W:) |
| Primary volume 2 (E:) | Transaction log file and checkpoint file of storage group STR1 | Secondary volume 2 (X:) |
| Primary volume 3 (F:) | Mailbox store and public folder store of storage group STR2 | Secondary volume 3 (Y:) |
| Primary volume 4 (G:) | Transaction log file and checkpoint file of storage group STR2 | Secondary volume 4 (Z:) |

### 5.9.1 Backing Up Storage Groups (Exchange Server cold backup)

This section explains how to perform cold backup of storage groups onto tape. First, you perform cold back up of data from the primary volume to the secondary volume, and then you back up the data from the secondary volume to tape. A new backup is possible only after the backup data has been stored onto a tape.

In this example, storage groups **STR1** and **STR2** are backed up in this order.

To perform a cold backup of storage groups to tape:

1. Before backing up storage group **STR1**, clear the system cache of the backup server. To clear the system cache, mount the secondary volume and then unmount it.

```
PROMPT> drmmount -copy_group EXG001,B001 -mount_pt W:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = W:
KAVX0401-I Mounting has finished.
           Mount point = W:
KAVX0002-I The drmmount command will now end.
PROMPT> drmumount -copy_group EXG001,B001
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = W:
KAVX0407-I Unmounting has finished.
           Mount point = W:
KAVX0002-I The drmumount command will now end.
PROMPT> drmmount -copy_group EXG002,B001 -mount_pt X:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = X:
KAVX0401-I Mounting has finished.
           Mount point = X:
KAVX0002-I The drmmount command will now end.
PROMPT> drmumount -copy_group EXG002,B001
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = X:
KAVX0407-I Unmounting has finished.
           Mount point = X:
KAVX0002-I The drmumount command will now end.
```

2. Back up storage group **STR1** offline. To perform backup, execute the **drmexgbackup** command.

```
PROMPT> drmexgbackup -target STR1
KAVX0001-I The drmexgbackup command will now start.
KAVX1805-I The information store will now be dismounted.
           Storage group name = STR1
KAVX1600-I Backup processing will now start.
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000001
KAVX1601-I Backup processing has finished.
KAVX1806-I The information store will now be mounted.
           storage-group-name = STR1
KAVX0002-I The drmexgbackup command will now end.
```

When this command is executed, the backup information is registered in the backup catalog of the database server, using a new backup ID (an unused, consecutive ID). In this example, the new backup ID is **0000000001**.

3. Check the backup result of storage group **STR1**. To confirm that backup to the secondary volume finished successfully, execute the **drmexgcat** command:

```
PROMPT> drmexgcat -target STR1
STORAGEGROUP: STR1
BACKUP-ID:0000000001 BACKUP-MODE: COLD STORAGEGROUP: STR1 ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:01:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.edb       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.stm       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.edb        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.stm        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
T TRANSACT     -                    E:\STR1\E00.log         E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
T TRANSACT     -                    E:\STR1\E000001.log     E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
T TRANSACT     -                    E:\STR1\E000002.log     E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
T TRANSACT     -                    E:\STR1\E000003.log     E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
C CHECKPOINT   -                    E:\STR1\E00.chk         E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
PROMPT>
```

4. Before backing up storage group **STR2**, clear the system cache of the backup server. To clear the system cache, mount the secondary volume and then unmount it.

```
PROMPT> drmmount -copy_group EXG001,B002 -mount_pt Y:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = Y:
KAVX0401-I Mounting has finished.
           Mount point = Y:
KAVX0002-I The drmmount command will now end.
PROMPT> drmumount -copy_group EXG001,B002
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = Y:
KAVX0407-I Unmounting has finished.
           Mount point = Y:
KAVX0002-I The drmumount command will now end.
PROMPT> drmmount -copy_group EXG002,B002 -mount_pt Z:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = Z:
KAVX0401-I Mounting has finished.
           Mount point = Z:
KAVX0002-I The drmmount command will now end.
PROMPT> drmumount -copy_group EXG002,B002
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = Z:
KAVX0407-I Unmounting has finished.
           Mount point = Z:
KAVX0002-I The drmumount command will now end.
```

5. Back up storage group **STR2** offline. To perform backup, execute the **drmexgbackup** command.

```
PROMPT> drmexgbackup -target STR2
KAVX0001-I The drmexgbackup command will now start.
KAVX1805-I The information store will now be dismounted.
           Storage group name = STR2
KAVX1600-I Backup processing will now start.
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000002
KAVX1601-I Backup processing has finished.
KAVX1806-I The information store will now be mounted.
           Storage group name = STR2
KAVX0002-I The drmexgbackup command will now end.
PROMPT>
```

When this command is executed, the backup information is registered in the backup catalog of the database server, using a new backup ID (an unused, consecutive ID). In this example, the new backup ID is **0000000002**.

6. Check the backup result of storage group **STR2**. To confirm that backup to the secondary volume finished successfully, execute the **drmexgcat** command.

```
PROMPT> drmexgcat -target STR2
STORAGEGROUP: STR2
BACKUP-ID:0000000002 BACKUP-MODE: COLD STORAGEGROUP: STR2 ORIGINAL-ID:0000000002
START-TIME:2002/06/01 10:30:00 END-TIME: 2002/06/01 10:31:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.edb       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.stm       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.edb        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.stm        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
T TRANSACT     -                    G:\STR2\E00.log         G:          -
Harddisk4    EXG002,B002
- -             -                    -                       -           -       -
EXG002,B002
T TRANSACT     -                    G:\STR2\E000001.log     G:          -
Harddisk4    EXG002,B002
- -             -                    -                       -           -       -
EXG002,B002
C CHECKPOINT   -                    G:\STR2\E00.chk         G:          -
Harddisk4    EXG002,B002
- -             -                    -                       -           -       -
EXG002,B002
PROMPT>
```

7. Export the backup information of storage groups **STR1** and **STR2** to temporary files. To back up the secondary volume to tape, you will need to take the information pertaining to the operations performed during backup from the primary volume to the secondary volume, and copy it to the backup server. Execute the **drmdbexport** command to export the backup information of **STR1** to **C:\temp\0000000001.drm**, and the backup information of **STR2** to **C:\temp\0000000002.drm**.

```
PROMPT> drmdbexport 0000000001 -f C:\temp\0000000001.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
PROMPT> drmdbexport 0000000002 -f C:\temp\0000000002.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
PROMPT>
```

8. Transfer the exported temporary files **C:\temp\0000000001.drm** and **C:\temp\0000000002.drm** from the database server to the backup server by executing the **ftp** command. In this case, the FTP root folder is **C:\FTP_ROOT**. Temporary files will be transferred to the backup server as **C:\FTP_ROOT\0000000001.drm** and **C:\FTP_ROOT\0000000002.drm** respectively.

```
PROMPT> ftp backup-server-name
ftp> Username: (logon-name)
ftp> password: (password)
ftp> put C:\temp\0000000001.drm
ftp> put C:\temp\0000000002.drm
ftp> quit
PROMPT>
```

9. Import the temporary file of storage group **STR1**, which was transferred from the database server, to the backup catalog of the backup server. Take the temporary file **C:\FTP_ROOT\0000000001.drm**, which was transferred from the database server, and import it into the backup catalog of the backup server. To import the file, execute the **drmdbimport** command on the backup server.

```
PROMPT> drmdbimport -f C:\FTP_ROOT\0000000001.drm
KAVX0001-I The drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000001
KAVX0002-I The drmdbimport command will now end.
PROMPT>
```

10. Check the import result of the temporary file of storage group **STR1**. To confirm that the import finished successfully, execute the **drmexgcat** command on the backup server.

```
PROMPT> drmexgcat -target STR1
STORAGEGROUP: STR1
BACKUP-ID:0000000001 BACKUP-MODE: COLD STORAGEGROUP: STR1 ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:01:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.edb       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.stm       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.edb        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.stm        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
T TRANSACT     -                    E:\STR1\E00.log         E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
T TRANSACT     -                    E:\STR1\E000001.log     E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
T TRANSACT     -                    E:\STR1\E000002.log     E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
T TRANSACT     -                    E:\STR1\E000003.log     E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
C CHECKPOINT   -                    E:\STR1\E00.chk         E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
PROMPT>
```

11. Import the temporary file **C:\FTP_ROOT\0000000002.drm**, which was transferred from the database server, into the backup catalog of the backup server. To import the file, execute the **drmdbimport** command on the backup server.

```
PROMPT> drmdbimport -f C:\FTP_ROOT\0000000002.drm
KAVX0001-I The drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000002
KAVX0002-I The drmdbimport command will now end.
PROMPT>
```

12. Check the import result of the temporary file of storage group **STR2**. To confirm that the import finished successfully, execute the **drmexgcat** command on the backup server.

```
PROMPT> drmexgcat -target STR2
STORAGEGROUP: STR2
BACKUP-ID:0000000002 BACKUP-MODE: COLD STORAGEGROUP: STR2 ORIGINAL-ID:0000000002
START-TIME:2002/06/01 10:30:00 END-TIME: 2002/06/01 10:31:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.edb       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.stm       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.edb        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.stm        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
T TRANSACT     -                    G:\STR2\E00.log         G:          -
Harddisk4    EXG002,B002
- -             -                    -                       -           -       -
EXG002,B002
T TRANSACT     -                    G:\STR2\E000001.log     G:          -
Harddisk4    EXG002,B002
- -             -                    -                       -           -       -
EXG002,B002
C CHECKPOINT   -                    G:\STR2\E00.chk         G:          -
Harddisk4    EXG002,B002
- -             -                    -                       -           -       -
EXG002,B002
PROMPT>
```

13. Mount the secondary volume that contains storage group **STR1** onto the backup server. Specify the backup ID **0000000001** assigned during importing.

```
PROMPT> drmmount 0000000001 -mount_pt W:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = W:
KAVX0401-I Mounting has finished.
           Mount point = W:
KAVX0400-I Mounting will now start.
           Mount point = X:
KAVX0401-I Mounting has finished.
           Mount point = X:
KAVX0002-I The drmmount command will now end.
```

14. Back up the backup data of storage group **STR1** from the secondary volume to tape. To back up, execute the **drmmediabackup** command on the backup server.

```
PROMPT> drmmediabackup 0000000001
KAVX0001-I The drmmediabackup command will now start.
KAVX0402-I Backup processing will now start.
           To see more details on backup progress, use the monitoring method of
the backup management product.
           Source = W:
KAVX0402-I Backup processing will now start.
           To see more details on backup progress, use the monitoring method of
the backup management product.
           Source = X:
KAVX0403-I Backup processing has finished.
           Source = W:
KAVX0403-I Backup processing has finished.
           Source = X:
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000003
KAVX0002-I The drmmediabackup command will now end.
```

When backup is performed, information pertaining to the backup operations is registered in the backup catalog, using the new backup ID **0000000003**.

15. Check the backup result of storage group **STR1** to the tape. To confirm that backup finished successfully, execute the **drmtapecat** command on the backup server.

```
PROMPT> drmtapecat -backup_id 0000000003
BACKUP-ID   BACKUP-OBJECT    SNAPSHOT TIME        EXPIRATION TIME
BACKUP-MEDIA
0000000003  MSEXCHANGE       2002/06/01 11:00:00  2002/06/02 11:00:00  MEDIA1
PROMPT>
```

16. Unmount the secondary volume. To unmount the secondary volume, specify the backup ID used when mounting **0000000001**.

```
PROMPT> drmumount 0000000001
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = W:
KAVX0407-I Unmounting has finished.
           Mount point = W:
KAVX0406-I Unmounting will now start.
           Mount point = X:
KAVX0407-I Unmounting has finished.
           Mount point = X:
KAVX0002-I The drmumount command will now end.
```

17. Mount the secondary volume that contains storage group **STR2** onto the backup server. Specify the backup ID **0000000002** assigned during importing.

```
PROMPT> drmmount 0000000002 -mount_pt Y:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = Y:
KAVX0401-I Mounting has finished.
           Mount point = Y:
KAVX0400-I Mounting will now start.
           Mount point = Z:
KAVX0401-I Mounting has finished.
           Mount point = Z:
KAVX0002-I The drmmount command will now end.
```

18. Back up the backup data of storage group **STR2** from the secondary volume to tape. To back up, execute the **drmmediabackup** command on the backup server.

```
PROMPT> drmmediabackup 0000000002
KAVX0001-I The drmmediabackup command will now start.
KAVX0402-I Backup processing will now start.
           To see more details on backup progress, use the monitoring method of
the backup management product.
           Source = Y:
KAVX0402-I Backup processing will now start.
           To see more details on backup progress, use the monitoring method of
the backup management product.
           Source = Z:
KAVX0403-I Backup processing has finished.
           Source = Y:
KAVX0403-I Backup processing has finished.
           Source = Z:
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000004
KAVX0002-I The drmmediabackup command will now end.
```

    When backup is performed, information pertaining to the backup operations is registered in the backup catalog using a new backup ID of **0000000004**.

19. Check the backup result of storage group **STR2** to the tape. To confirm that backup finished successfully, execute the **drmtapecat** command on the backup server.

```
PROMPT> drmtapecat -backup_id 0000000004
BACKUP-ID   BACKUP-OBJECT    SNAPSHOT TIME        EXPIRATION TIME
BACKUP-MEDIA
0000000004  MSEXCHANGE       2002/06/02 11:00:00  2002/06/03 11:00:00  MEDIA2
PROMPT>
```

20. Unmount the secondary volume. To unmount the secondary volume, specify the backup ID used when mounting **0000000001**.

```
PROMPT> drmumount 0000000001
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = Y:
KAVX0407-I Unmounting has finished.
           Mount point = Y:
KAVX0406-I Unmounting will now start.
           Mount point = Z:
KAVX0407-I Unmounting has finished.
           Mount point = Z:
KAVX0002-I The drmumount command will now end.
```

### 5.9.2 Restoring and Recovering Storage Groups (Exchange Server cold backup)

This section explains how to restore data that has been backed up to tape cold. To do so, you first restore the data from a tape to the secondary volume, resynchronize the secondary volume to the primary volume and restore the secondary volume, and then recover storage groups.

To restore storage groups from a tape:

1. Check the backup ID of the backup data. To check the backup ID of the backup data to be used for the restoration, execute the **drmtapecat** command on the backup server.

```
PROMPT> drmtapecat
BACKUP-ID   BACKUP-OBJECT    SNAPSHOT TIME        EXPIRATION TIME
BACKUP-MEDIA
0000000003  MSEXCHANGE       2002/06/01 11:00:00  2002/06/02 11:00:00  MEDIA1
0000000004  MSEXCHANGE       2002/06/02 11:00:00  2002/06/03 11:00:00  MEDIA2
PROMPT>
```

2. Mount the secondary volume that contains storage group STR1 onto the backup server. Specify the backup ID 0000000003 used on tape.

```
PROMPT> drmmount 0000000003 -mount_pt W:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = W:
KAVX0401-I Mounting has finished.
           Mount point = W:
KAVX0400-I Mounting will now start.
           Mount point = X:
KAVX0401-I Mounting has finished.
           Mount point = X:
KAVX0002-I The drmmount command will now end.
```

3. Restore the backup data of storage group STR1 from the tape to the secondary volume. To restore, execute the drmmediarestore command on the backup server.

```
PROMPT> drmmediarestore 0000000003
KAVX0001-I The drmmediarestore command will now start.
KAVX0404-I Restoration will now start.
           To see more details on restoration progress, use the monitoring method
of the backup management product.
           Source = W:
           Target = W:
KAVX0404-I Restoration will now start.
           To see more details on restoration progress, use the monitoring method
of the backup management product.
           Source = X:
           Target = X:
KAVX0405-I Restoration has finished.
           Source = W:
           Target = W:
KAVX0405-I Restoration has finished.
           Source = X:
           Target = X:
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000005
KAVX0002-I The drmmediarestore command will now end.
```

When the restoration is performed, the restoring operation information is registered in the backup catalog of the backup server, using a new backup ID 0000000005. The status of the secondary volume is updated, and the backup ID 0000000001, which was used to manage the status of the secondary volume before its update, will then be deleted from the backup catalog of the backup server.

4. Check the restoration result of storage group STR1 from the tape to the secondary volume. To confirm that the restoration finished successfully, execute the drmexgcat command on the backup server.

```
PROMPT> drmexgcat -target STR1
STORAGEGROUP: STR1
BACKUP-ID:0000000005 BACKUP-MODE: COLD STORAGEGROUP: STR1 ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:01:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.edb       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.stm       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.edb        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.stm        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
T TRANSACT     -                    E:\STR1\E00.log         E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
T TRANSACT     -                    E:\STR1\E000001.log     E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
T TRANSACT     -                    E:\STR1\E000002.log     E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
T TRANSACT     -                    E:\STR1\E000003.log     E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
C CHECKPOINT   -                    E:\STR1\E00.chk         E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
PROMPT>
```

5. Unmount the secondary volume. To unmount the secondary volume, specify the backup ID specified when mounting 0000000003.

```
PROMPT> drmmount 0000000003
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = W:
KAVX0407-I Unmounting has finished.
           Mount point = W:
KAVX0406-I Unmounting will now start.
           Mount point = X:
KAVX0407-I Unmounting has finished.
           Mount point = X:
KAVX0002-I The drmumount command will now end.
```

6. Mount the secondary volume that contains storage group STR2 onto the backup server. Specify the backup ID 0000000004 used on tape.

```
PROMPT> drmmount 0000000004 -mount_pt Y:
KAVX0001-I The drmmount command will now start.
KAVX0400-I Mounting will now start.
           Mount point = Y:
KAVX0401-I Mounting has finished.
           Mount point = Y:
KAVX0400-I Mounting will now start.
           Mount point = Z:
KAVX0401-I Mounting has finished.
           Mount point = Z:
KAVX0002-I The drmmount command will now end.
```

7. Restore the backup data of storage group STR2 from the tape to the secondary volume. To restore, execute the drmmediarestore command on the backup server.

```
PROMPT> drmmediarestore 0000000004
KAVX0001-I The drmtaperestore command will now start.
KAVX0404-I Restoration will now start.
           To see more details on restoration progress, use the monitoring method
of the backup management product.
           Source = Y:
           Target = Y:
KAVX0404-I Restoration will now start.
           To see more details on restoration progress, use the monitoring method
of the backup management product.
           Source = Z:
           Target = Z:
KAVX0405-I Restoration has finished.
           Source = Y:
           Target = Y:
KAVX0405-I Restoration has finished.
           Source = Z:
           Target = Z:
KAVX0040-I The backup ID has been assigned as follows.
           Backup ID = 0000000006
KAVX0002-I The drmmediarestore command will now end.
```

When the restoration is performed, the restoring operation information is registered in the backup catalog of the backup server using a new backup ID 0000000006. The status of the secondary volume is updated, and the backup ID 0000000002, which was used to manage the status of the secondary volume before its update, will then be deleted from the backup catalog of the backup server.

8. Check the restoration result of storage group STR2 from the tape to the secondary volume. To confirm that the restoration finished successfully, execute the drmexgcat command on the backup server.

```
PROMPT> drmexgcat -target STR2
STORAGEGROUP: STR2
BACKUP-ID:0000000006 BACKUP-MODE: COLD STORAGEGROUP: STR2 ORIGINAL-ID:0000000002
START-TIME:2002/06/01 10:30:00 END-TIME: 2002/06/01 10:31:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.edb       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.stm       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.edb        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.stm        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
T TRANSACT     -                    G:\STR2\E00.log         G:          -
Harddisk4    EXG002,B002
- -             -                    -                       -           -       -
EXG002,B002
T TRANSACT     -                    G:\STR2\E000001.log     G:          -
Harddisk4    EXG002,B002
- -             -                    -                       -           -       -
EXG002,B002
C CHECKPOINT   -                    G:\STR2\E00.chk         G:          -
Harddisk4    EXG002,B002
- -             -                    -                       -           -       -
EXG002,B002
PROMPT>
```

9. Unmount the secondary volume. To unmount the secondary volume, specify the backup ID specified when mounting 0000000004.

```
PROMPT> drmumount 0000000004
KAVX0001-I The drmumount command will now start.
KAVX0406-I Unmounting will now start.
           Mount point = Y:
KAVX0407-I Unmounting has finished.
           Mount point = Y:
KAVX0406-I Unmounting will now start.
           Mount point = Z:
KAVX0407-I Unmounting has finished.
           Mount point = Z:
KAVX0002-I The drmumount command will now end.
```

10. Export the backup information of storage groups STR1 and STR2 to temporary files. To restore data from the secondary volume to the primary volume, the information on the operations used to restore data from the tape to the secondary volume must be copied to the database server. Export the backup information of STR1 and STR2 to the FTP root folder by executing the drmdbexport command. In this case, the FTP folder will be C:\FTP_ROOT. Execute the drmdbexport command to export the backup information of STR1 to C:\FTP_ROOT\0000000005.drm, and the backup information of STR2 to C:\FTP_ROOT\0000000006.drm.

```
PROMPT> drmdbexport 0000000005 -f C:\FTP_ROOT\0000000005.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
PROMPT> drmdbexport 0000000006 -f C:\FTP_ROOT\0000000006.drm
KAVX0001-I The drmdbexport command will now start.
KAVX0002-I The drmdbexport command will now end.
PROMPT>
```

11. Collect temporary files exported from the backup server on the database server. Collect temporary files C:\FTP_ROOT\0000000005.drm and C:\FTP_ROOT\0000000006.drm, which were exported from the backup server, on the database server by executing the ftp command. Temporary files will be stored in the current directory. In this case, the current directory will be C:\.

```
PROMPT> ftp backup-server-name
ftp> Username: (logon-name)
ftp> password: (password)
ftp> get 0000000005.drm
ftp> get 0000000006.drm
ftp> quit
PROMPT>
```

12. Import temporary file C:\0000000005.drm, which was collected from storage group STR2, to the backup catalog of the database server by executing the drmdbimport command on the database server.

```
PROMPT> drmdbimport -f C:\0000000005.drm
KAVX0001-I The drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000003
KAVX0002-I drmdbimport command will now end.
PROMPT>
```

13. Check the import result of the temporary file of storage group STR1. To confirm that the import finished successfully, execute the drmexgcat command on the database server.

```
PROMPT> drmexgcat -target STR1
STORAGEGROUP: STR1
BACKUP-ID:0000000003 BACKUP-MODE: COLD STORAGEGROUP: STR1 ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:01:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.edb       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.stm       D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.edb        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.stm        D:          -
Harddisk1    EXG001,B001
- -             -                    -                       -           -       -
EXG001,B001
T TRANSACT     -                    E:\STR1\E00.log         E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
T TRANSACT     -                    E:\STR1\E000001.log     E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
T TRANSACT     -                    E:\STR1\E000002.log     E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
T TRANSACT     -                    E:\STR1\E000003.log     E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
C CHECKPOINT   -                    E:\STR1\E00.chk         E:          -
Harddisk2    EXG002,B001
- -             -                    -                       -           -       -
EXG002,B001
PROMPT>
```

14. Import temporary file C:\0000000006.drm, which was collected from storage group STR2, to the backup catalog of the database server by executing the drmdbimport command on the database server.

```
PROMPT> drmdbimport -f C:\0000000006.drm
KAVX0001-I drmdbimport command will now start.
KAVX0418-I Backup information from the specified file was imported into the backup
catalog.
           Imported backup ID = 0000000004
KAVX0002-I The drmdbimport command will now end.
PROMPT>
```

15. Check the import result of the temporary file of storage group STR2. To confirm that the import finished successfully, execute the drmexgcat command on the database server.

```
PROMPT> drmexgcat -target STR2
STORAGEGROUP: STR2
BACKUP-ID:0000000004 BACKUP-MODE: COLD STORAGEGROUP: STR2 ORIGINAL-ID:0000000002
START-TIME:2002/06/01 10:30:00 END-TIME: 2002/06/01 10:31:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.edb       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
M MAILBOXSTORE MAILBOX1(STR2)       F:\STR2\priv1.stm       F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.edb        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
P PUBLICSTORE  PUBLIC1(STR2)        F:\STR2\pub1.stm        F:          -
Harddisk3    EXG001,B002
- -             -                    -                       -           -       -
EXG001,B002
T TRANSACT     -                    G:\STR2\E00.log         G:          -
Harddisk4    EXG002,B002
- -             -                    -                       -           -       -
EXG002,B002
T TRANSACT     -                    G:\STR2\E000001.log     G:          -
Harddisk4    EXG002,B002
- -             -                    -                       -           -       -
EXG002,B002
C CHECKPOINT   -                    G:\STR2\E00.chk         G:          -
Harddisk4    EXG002,B002
- -             -                    -                       -           -       -
EXG002,B002
PROMPT>
```

16. Restore the data of the secondary volume to the primary volume, and recover storage groups. Resynchronize and restore the primary and secondary volumes. You should also apply the transaction log to recover storage groups. To restore and recover the storage groups, execute the drmexgrestore command on the database server.

```
PROMPT> drmexgrestore 0000000003 -resync -recovery
KAVX0001-I The drmexgrestore command will now start.
KAVX1805-I The information store will now be dismounted.
           Storage group name = STR1
KAVX1700-I Restore processing will now start.
KAVX1701-I Restore processing has finished.
KAVX1806-I The information store will now be mounted.
           Storage group name = STR1
KAVX0002-I The drmexgrestore command will now end.
PROMPT> drmexgrestore 0000000004 -resync -recovery
KAVX0001-I The drmexgrestore command will now start.
KAVX1805-I The information store will now be dismounted.
           Storage group name = STR2
KAVX1700-I Restore processing will now start.
KAVX1701-I Restore processing has finished.
KAVX1806-I The information store will now be mounted.
           Storage group name = STR2
KAVX0002-I The drmexgrestore command will now end.
PROMPT>
```

# Chapter 6 Commands

This chapter describes the commands that Protection Services provides.

6.1 Overview of Commands

6.2 Requirements for Executing Commands for SQL Server

6.3 Before Reading the Command Descriptions

6.4 Copy Controller Command Specifications

6.5 SQL Server Command Specifications

## 6.1 Overview of Commands

Table 6.1 lists the commands provided by Protection Services – Copy Controller.
Table 6.2 lists the commands provided by Protection Services for SQL Server.

In UNIX, you can use the **man** command to display descriptions of Protection Services commands. In Windows, you can execute the command specifying the **-h** option after the command name to display the command format.

**Table 6.1 List of Commands (Copy Controller)**

| Command Name | Function Summary | Possible to run with other commands? |
|---|---|---|
| drmcgctl | ▪ Locks copy groups.<br>▪ Unlocks copy groups.<br>▪ Displays a list of copy groups. | No *1 |
| drmclusinit | Registers the parameters of the cluster product. | Yes |
| drmdbexport | Exports backup information to a file. | No |
| drmdbimport | Imports backup information from a file. | No |
| drmfsbackup | Backs up a file system to a disk. | No |
| drmfscat | Displays a listing of the backup information for a file system. | Yes |
| drmfsdisplay | ▪ Displays a listing of file system information.<br>▪ Updates the dictionary map file to the latest status. | No *2 |
| drmfsrestore | Restores a file system. | No |
| drmlicense | Displays or updates license information. | Yes |
| drmmediabackup | Backs up the backup data to tape. | No |
| drmmediarestore | Restores backup data from tape. | No |
| drmmount | Mounts a disk volume. | No |
| drmresync | Resynchronizes copy groups and deletes the backup data. | No |
| drmtapebackup | Copies the backup data to tape. | No |
| drmtapecat | Displays a listing of backup information for a tape. | Yes |
| drmtapeinit | Registers the parameters for a backup management product. | Yes |
| drmtaperestore | Restores data from a backup on tape. | No |
| drmumount | Unmounts a disk volume. | No |

***Notes:***

1. You can execute other commands simultaneously with the copy group display command.
2. The **drmfsdisplay** command cannot be executed with other commands when the **-refresh** option is specified. This command can be executed with other commands when other options are specified.

**Table 6.2 List of Commands (SQL Server only)**

| Command Name | Function Summary | Possible to run with other commands? |
|---|---|---|
| drmsqlbackup | Backs up an SQL Server database to a disk. | No |
| drmsqlcat | Displays a listing of the backup information for an SQL Server database. | Yes |
| drmsqldisplay | ▪ Displays a listing of SQL Server database information.<br>▪ Updates the SQL Server database information in the dictionary map file. | No * |
| drmsqlinit | Registers SQL Server parameters. | Yes |
| drmsqllogbackup | Backs up the SQL Server transaction log file. | No |
| drmsqlrecover | Recovers a restored SQL Server database. | No |
| drmsqlrecovertool | Recovers a restored SQL Server database using a GUI. | No |
| drmsqlrestore | Restores an SQL Server database. | No |

* The **drmsqldisplay** command cannot be executed with other commands when the **-refresh** option is specified. This command can be executed with other commands when other options are specified.

**Table 6.3 List of Commands (Exchange Server only)**

| Command Name | Function Summary | Possible to run with other commands? |
|---|---|---|
| drmexgbackup | Backs up an Exchange Server database to a disk. | No |
| drmexgcat | Displays a listing of the backup information for an Exchange Server database. | Yes |
| drmexgdisplay | ▪ Displays a listing of Exchange Server database information.<br>▪ Updates the Exchange Server database information in the dictionary map file. | No * |
| drmexgrestore | Restores an Exchange Server database. | No |
| drmexgverify | Verifies the integrity between a storage group and backup information. | No |

* The **drmexgdisplay** command cannot be executed with other commands when the **-refresh** option is specified. This command can be executed with other commands when other options are specified.

### 6.1.1 Preventing the System from Indefinitely Executing a Command

While a command is executing, if a user attempts to execute another command that cannot be executed concurrently with the executing command, the system will attempt to execute the latter command indefinitely until the former command terminates. To prevent the system from attempting to execute such a command indefinitely, you need to edit the **init.conf** file.

The location of the **init.conf** file (in UNIX): **/opt/drm/conf/init.conf**

The location of the **init.conf** file (in Windows):
***Protection-Services-installation-directory*\conf\init.conf**

File format of **init.conf**:
**COM_RETRY_TIME=*number-of-retry-attempts***
**COM_RETRY_WAIT=*duration-between-retry-attempts***

The following values are available:

- Number of retry attempts: 0 to 3,600, with 0 representing indefinite retries.
- Duration between retry attempts: 0 to 3,600 between each retry attempt (in ten-second intervals).

In a cluster configuration of the Active-Active type, commands that cannot be executed concurrently on a system might be executed at the same time if failover occurs due to a system failure. If commands that cannot be executed concurrently are executed, the second command is retried indefinitely until the first command finishes. If you want to stop the indefinite retry, edit the configuration file (**init.conf**).

### 6.1.2 Executing Commands in a Cluster Environment

In a cluster environment, you need to set the environment variable **DRM_HOSTNAME** before executing the command. The following shows an example:

**PROMPT> set DRM_HOSTNAME=*virtual-server-name***

## 6.2 Requirements for Executing Commands for SQL Server

When executing commands to operate the SQL Server database, you need to consider the status of the SQL Server service, the status of the database, and the database type. The following sections explain the requirements for executing Protection Services commands.

### 6.2.1 Relationship between Service Status and Commands

Table 6.4 explains the relationship between the status of the SQL Server service (running or stopped) and the Protection Services commands.

**Table 6.4 Relationship between Service Status and Commands (SQL Server)**

| Command | Service Status | |
|---|---|---|
| | Running | Stopped |
| drmsqlbackup | Executable | (Not applicable) |
| drmsqlcat | Executable | Executable |
| drmsqldisplay<br>(when the **-refresh** option is specified) | Executable | (Not applicable) |
| drmsqldisplay<br>(when the **-refresh** option is not specified) | Executable | (Not applicable) |
| drmsqlinit | Executable | (Not applicable) |
| drmsqllogbackup | Executable | (Not applicable) |
| drmsqlrecover | Executable | (Not applicable) |
| drmsqlrecovertool | Executable | (Not applicable) |
| drmsqlrestore<br>(when the system database is included) | Executable | Executable |
| drmsqlrestore<br>(when the system database is not included) | Executable | (Not applicable) |

### 6.2.2 Relationship between Database Status and Commands

Table 6.5 explains the relationship between the status of the SQL Server database (online, offline, reading, read-only, or unconfirmed) and the Protection Services commands.

**Table 6.5 Relationship between Database Status and Commands (SQL Server)**

| | Database Status | | | | |
|---|---|---|---|---|---|
| **Command** | **Online** | **Offline** | **Reading** | **Read-only** | **Unconfirmed** |
| drmsqlbackup | Yes (DB) | No | No | No | No |
| drmsqlcat | Yes | Yes | Yes | Yes | Yes |
| drmsqldisplay (when the **-refresh** option is specified) | Yes (DB) | Yes (DB) | Yes (DB) | Yes (DB) | Yes (DB) |
| drmsqldisplay (when the **-refresh** option is not specified) | Yes | Yes | Yes | Yes | Yes |
| drmsqlinit | Yes | Yes | Yes | Yes | Yes |
| drmsqllogbackup | Yes (DB) | No | No | No | No |
| drmsqlrecover (when the **-undo** option is specified) | Yes (DB) | No | Yes (DB) (becomes read-only) | Yes (DB) | No |
| drmsqlrecover (when the **-undo** option is not specified) | Yes (DB) | No | Yes (DB) (becomes online) | Yes (DB) (becomes online) | No |
| drmsqlrecovertool | No | No | Yes (DB) (becomes online) | Yes (DB) (becomes online) | No |
| drmsqlrestore (when the **-undo** option is not specified) | Yes (DB) (becomes read-only) | Yes (DB) (becomes read-only) | Yes (DB) (becomes read-only) | Yes (DB) (becomes read-only) | Yes (DB) (becomes read-only) |
| drmsqlrestore (when the **-undo** option is not specified) | Yes (DB) (becomes reading) | Yes (DB) (becomes reading) | Yes (DB) (becomes reading) | Yes (DB) (becomes reading) | Yes (DB) (becomes reading) |

***Legend:***

**Yes (DB)**: The command can be executed, and the operations are performed on the database. The database status after the operations is displayed in parentheses.

**Yes**: The command can be executed; however, no operation is performed on the database.

**No**: The command cannot be executed.

### 6.2.3 Relationship between Database Type and Commands

Table 6.6 explains the relationship between the type of SQL Server database (master, msdb, model, tempdb, user database) and the Protection Services commands.

**Table 6.6 Relationship between Database Status and Commands (SQL Server)**

| Command | SQL Server System Database | | | | SQL Server User Database |
|---|---|---|---|---|---|
| | master | msdb | model | tempdb | |
| drmsqlbackup | Yes (DB) | Yes (DB) | Yes (DB) | No (abnormal termination) | Yes (DB) |
| drmsqlcat | Yes | Yes | Yes | Yes | Yes |
| drmsqldisplay | Yes | Yes | Yes | Yes | Yes |
| drmsqlinit | Yes | Yes | Yes | Yes | Yes |
| drmsqllogbackup | No (No operation is performed) *1 | No (No operation is performed) *1 | No (No operation is performed) *1 | No (No operation is performed) *1 | Yes (DB) *2 |
| drmsqlrecover | No (No operation is performed) | No (No operation is performed) | No (No operation is performed) | No (abnormal termination) | Yes (DB) |
| drmsqlrecovertool | No (No operation is performed) | No (No operation is performed) | No (No operation is performed) | No (abnormal termination) | Yes (DB) |
| drmsqlrestore | Yes (DB) | Yes (DB) | Yes (DB) | Yes | Yes (DB) |

***Legend:***

**Yes (DB)**: The command can be executed, and the operations are performed on the database. The database status after the operations is displayed in parentheses.

**Yes**: The command can be executed; however, no operation is performed on the database.

**No**: The command cannot be executed. The command behavior is displayed in parentheses.

***Notes:***

1. When the **-target** option or **-t** option is specified, the command terminates abnormally.
2. The command is executable only when the recovery type of the database is Full or Bulk_Logged.

## 6.3 Before Reading the Command Descriptions

Note the important information in the following sections before reading the command descriptions.

***Caution:*** Do not finish the command being operated forcibly. If you finish the command being operated forcibly, the pair status of the copy group or the backup catalog might be in an unexpected status.

### 6.3.1 Usage Precautions

- **drmtapecat** command

  ***Caution:*** Backed up data which already expired will be deleted on the first execution of the **drmtapecat** command with non **-delete** options after expiration date.

  If backed up data is lost, you cannot restore the data from tape using the **drmtaperestore** or **drmmediarestore** command. Therefore, specify the expiration period of the backup information longer than the media protection period.

### 6.3.2 Command Path

Commands are stored in the following directory:

In UNIX: **/opt/drm/bin/**

In Windows: ***Protection-Services-installation-directory*\bin**

### 6.3.3 Conventions in Syntax Explanations for Command Arguments

The syntax explanations for command arguments use the conventions described in Table 6.7. To display the command format, execute the command specifying the **-h** option after the command name.

**Table 6.7 Conventions in Syntax Explanations for Arguments**

| Symbol | Description |
|---|---|
| \| (vertical bar) | Only one of the options separated by a vertical bar can be used at one time.<br>Example: **log number \| all**<br>Either **log number** or **all** can be specified. |
| [ ] (brackets) | An item or items enclosed in brackets are optional. If two or more items separated by a vertical bar (\|) are enclosed, you can specify one or none of them.<br>Example: **[ -a \| -b ]**<br>This means that you specify nothing, or **-a**, or **-b**. |
| { } (braces) | An item enclosed in braces must be specified. If two or more items are enclosed, any one of them must be specified.<br>Example: **{ lock \| unlock }**<br>This means that you must select **lock** or **unlock** (but not both). |

### 6.3.4 Conventions for Creating a Target Definition File

When you want to specify two or more target objects (files, directories, databases, or storage groups) in a command option, you can specify them all at one time by using a *target definition file*. A target definition file contains a list of the desired target objects and must be created beforehand.

- **Commands that support a target definition file.** You can use a target definition file with the commands shown in Table 6.8.

**Table 6.8 Commands that Support a Target Definition File**

| Copy Controller | SQL Server | Exchange Server | Oracle |
|---|---|---|---|
| drmfsbackup<br>drmfscat<br>drmfsdisplay<br>drmfsrestore | drmsqlbackup<br>drmsqlcat<br>drmsqldisplay<br>drmsqlrecover<br>drmsqlrestore<br>drmsqllogbackup | drmexgbackup<br>drmexgcat<br>drmexgdisplay<br>drmexgrestore | |

- **File name.** Use alphanumeric characters to specify the file name.
- **Contents of the file.** The contents of the file must follow these conventions:
  - Each parameter (file name, directory name, database name, storage group name) must be specified on one line.
  - A database name or storage group name must be left justified with no leading spaces. Any space before and after the database name is identified as a part of the database name.
  - Lines beginning with **#** are assumed to be comment lines, unless the **#** is the beginning of a database or storage group name, in which case the characters will be assumed to be a database or storage group name.
  - The file names and directory names must be specified using absolute path names.
- **Example of entries in a target definition file (in UNIX):**

```
# Example of specifying files
/data1/batch_0001/Tokyo_output_dir
/data1/batch_0001/Osaka_output_dir
/data1/transact.log
```

- **Example of entries in a target definition file (in Windows):**

```
# Example of specifying files
D:\data1\batch_0001\Tokyo_output_dir
D:\data1\batch_0001\Osaka_output_dir
D:\data1\transact.log
```

### 6.3.5 Coding Rules for Creating a Transaction Log Target Definition File

A transaction log target definition file, when specified as an option of the **drmsqlrecover** command, specifies the order in which transaction log files are to be applied during recovery.

- **File name:**

  Use alphanumeric characters to specify the file name.

- **File contents:**

  The contents of the file must follow these coding rules:

  - Enter the name of the database, followed by the name of the transaction log file.
  - Enclose the name of the database in square brackets "**[**" and "**]**".
  - Enter the transaction log files for each database in the order in which they are to be applied.
  - Each transaction log file name must be specified using absolute path names.
  - A transaction log file name must be left justified with no leading spaces.
  - Lines beginning with **#** are assumed to be comment lines.

- **Example of entries in a target definition file:**

```
# Protection Service 01-04
# Log Backup Files
[SQLDB001]
C:\MSSQL\BackupLog\SQLDBLog001.bak
C:\MSSQL\BackupLog\SQLDBLog002.bak
C:\MSSQL\BackupLog\SQLDBLog003.bak

[SQLDB002]
C:\MSSQL\BackupLog\SQLDB2Log001.bak
C:\MSSQL\BackupLog\SQLDB2Log002.bak
C:\MSSQL\BackupLog\SQLDB2Log003.bak
```

## 6.4 Copy Controller Command Specifications

### 6.4.1 drmcgctl (lock or unlock a copy group)

**Format:**

To list copy groups:

```
drmcgctl
```

To lock or unlock a copy group by specifying a copy group name:

```
drmcgctl -copy_group copy-group-name -mode { lock | unlock }
```

To lock or unlock a copy group by specifying a backup ID:

```
drmcgctl -backup_id backup-ID -mode { lock | unlock }
```

**Description:**

The **drmcgctl** command locks copy groups that contain backup data so that they are not overwritten when the next backup is performed. This command also unlocks these copy groups. A lock on a copy group is valid only on the server where this command was executed. Operations from this server to the copy group cannot be performed until the copy group is unlocked.

When you execute this command with no option specified, a list of copy groups will be displayed. This allows you to check the following:

- The lock status of the copy group
- The backup ID (if a backup has been made)

**Arguments:**

**-copy_group *copy-group-name***

Specify the name of the copy group you want to lock or unlock.

When using UNIX and handling copy groups with multiple generations, you will need to place all copy groups of the same generation that belong to the same logical volume in the same locked status. If these lock statuses differ, backup cannot be performed normally (and an error will occur when you try to perform restoration).

You can check whether or not the logical volumes are the same by using the **drmfsdisplay** command (the **LVM-DEVICE** item displayed).

**-mode { lock | unlock }**

Specify whether to lock or unlock the copy group. To lock the copy group, specify **-mode lock**. To unlock the copy group, specify **-mode unlock**.

**-backup_id** ***backup-ID***

Specify the backup ID associated with the copy groups you want to lock or unlock. By specifying a backup ID, you can lock or unlock all the copy groups used for the backup identified by the specified ID at one time. Specify the backup ID created when the backup was performed from the primary volume to the secondary volume.

To check backup IDs, execute one of the following commands, according to what was backed up:

- **drmfscat** command (when a file system was backed up)
- **drmsqlcat** command (when an SQL Server database was backed up)
- **drmexgcat** command (when a storage group was backed up)

You cannot specify a backup ID that was created when a backup was performed from the secondary volume to tape. (You can use the **drmtapecat** command to check such a backup ID.) If you specify such a backup ID, the command terminates abnormally.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples:**

- The following command displays a listing of lock information for each copy group:

```
PROMPT> drmcgctl
COPY GROUP                LOCK STATUS  BACKUP-ID
VG01,dev01                LOCKED       0000000001
VG01,dev02                LOCKED       0000000001
VG01,dev03                UNLOCKED
VG02,dev01                UNLOCKED
```

- The following command locks the copy group **VG01,dev01**:

```
PROMPT> drmcgctl -copy_group VG01,dev01 -mode lock
```

- The following command unlocks the copy group **VG01,dev01**:

```
PROMPT> drmcgctl -copy_group VG01,dev01 -mode unlock
```

- The following command locks the copy groups used for the backup identified by the backup ID **0000000001**:

```
PROMPT> drmcgctl -backup_id 0000000001 -mode lock
```

- The following command unlocks the copy groups used for the backup identified by the backup ID **0000000001**:

```
PROMPT> drmcgctl -backup_id 0000000001 -mode unlock
```

### 6.4.2 drmclusinit (register the parameters for a cluster product)

**Format:**

To register the parameters for a cluster product:

```
drmclusinit cluster-product-name
```

To view the parameters registered for a cluster product:

```
drmclusinit -v cluster-product-name
```

**Description:**

For a cluster configuration, the **drmclusinit** command uses an interactive format to register the parameters necessary to control a cluster product.

The parameters registered using this command are stored in the following location:

In UNIX: **/opt/drm/conf/cluster/*cluster-name*.dat**

In Windows: ***Protection-Services-installation-directory*\conf\cluster*cluster-name*.dat**

Table 6.9 shows the parameters registered using the **drmclusinit** command:

**Table 6.9 Parameters of the Cluster Product**

| Registered Item | Description |
|---|---|
| Virtual server name (required) | Enter the name of the virtual server managed by the cluster product. |
| Instance name (required) | Enter the name of the instance managed by the cluster product. |
| Resource group name (required) | Enter a string to differentiate the management resource group name of the cluster product. |
| Resource type (optional) | Enter a string to differentiate the type of the resource managed by the cluster product. For a service resource, enter S. For a disk resource, enter D. |
| Service name (required when S has been specified for the resource type) | Enter the name of the service resource managed by the cluster product. Always specify this item when S has been specified as the resource type. |
| Disk name (required when D has been specified for the resource type) | Enter the name of the disk resource managed by the cluster product. Always specify this item when D has been specified as the resource type. |
| Resource name (optional) | Enter a string to differentiate the management resource name of the cluster product. If you choose not to specify this item, press the Return key, and do not enter anything. |

**Arguments:**

**-v**

Specify this to display the registered parameters.

***cluster-product-name***

Specify the keyword that identifies the cluster product being used.

You do not need to register parameter information when using the following products:

- Solaris: VERITAS Cluster Server
- HP-UX: MC/ServiceGuard
- Windows: Microsoft Cluster Service

The specified cluster product name is stored in the following file:

- UNIX: **/opt/drm/conf/cluster/DEFAULT.dat**
- Windows: ***Protection-Services-installation-directory*\conf\cluster\DEFAULT.dat**

### 6.4.3 drmdbexport (export backup information to a file)

**Format:**

```
drmdbexport backup-ID -f export-destination-file-name
```

**Description:**

The **drmdbexport** command exports backup information recorded in the backup catalog to a file. By using the **drmdbimport** command, you can import this exported backup information into a backup catalog on another server.

Note that you cannot export a backup record created by using one of the following commands:
**drmmediabackup**
**drmmediarestore**
**drmtapebackup**
**drmtaperestore**

**Arguments:**

***backup-ID***

Specify the backup ID of the backup record you want to export. To check backup IDs, one of the following commands according to what was backed up:

- **drmfscat** command. (when a file system was backed up)
- **drmsqlcat** command (when an SQL Server database was backed up)
- **drmexgcat** command (when a storage group was backed up)

**-f *export-destination-file-name***

Specify the absolute path name of the file to which you want to export the backup information. Use a maximum of 511 bytes for a file name. If the specified export destination file already exists, the existing file is overwritten.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Example (in UNIX):**

- The following command exports the backup information of the backup ID **0000000001** to the file **/tmp/0000000001.drm**:

```
PROMPT> drmdbexport 0000000001 -f /tmp/0000000001.drm
```

**Example (in Windows):**

- The following command exports the backup information of the backup ID **0000000001** to the file **D:\tmp\0000000001.drm**:

```
PROMPT> drmdbexport 0000000001 -f D:\temp\0000000001.drm
```

### 6.4.4 drmdbimport (import backup information from a file)

**Format:**

```
drmdbimport -f import-source-file
```

**Description:**

The **drmdbimport** command imports, into a backup catalog, backup information from a file that was exported by the **drmdbexport** command. Protection Services manages backup information based on copy groups, which are used as a key. If a backup record of the same copy group exists when you attempt to import the backup record, the old backup record is overwritten.

**Arguments:**

**-f *import-source-file-name***

Specify the absolute path name of the file whose backup information is to be imported into the backup catalog. Use a maximum of 511 bytes for a file name.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Example (in UNIX):**

- The following command imports the backup information from the file **/tmp/0000000001.drm**:

```
PROMPT> drmdbimport -f /tmp/0000000001.drm
```

**Example (in Windows):**

- The following command imports the backup information from the file **D:\tmp\0000000001.drm**:

```
PROMPT> drmdbimport -f D:\temp\0000000001.drm
```

### 6.4.5 drmfsbackup (back up a file system to a secondary volume)

**Format:**

To perform an online backup:

```
drmfsbackup mount-point-directory-name |
mount-point-directory-target-definition-file-name[ -mode online ]
            [ -target file-or-directory-name(s)
            | -f target-definition-file-name ]
```

To perform a cold backup:

```
drmfsbackup mount-point-directory-name |
mount-point-directory-name-target-definition-file-name -mode cold
```

**Description:**

The **drmfsbackup** command backs up the volume that contains the file system for the specified mount point to the secondary volume. You can back up an entire file system or only some files and directories in a file system. You can also back up more than one file system at a time. If the file system for the mount point consists of more than one volume, all the primary volumes are backed up to the secondary volumes.

Before executing this command, the following operations are required:

- All the application programs using the volume to be backed up must be ended. The volume being used by the operating system cannot be backed up.
- The system cache of the secondary volume must be cleared. Mount or unmount the secondary volume on the backup server to clear the system cache.

**Arguments:**

***mount-point-directory-name***

Specify the name of the mount point directory for the file system you want to back up. You must specify the mount point directory/drive letter for a mounted file system or the absolute path from the drive letter. If the specified mount point directory belongs to a file system that is not mounted, this command will terminate abnormally.

**In UNIX.** The mount point directory name must satisfy the following:

- Maximum number of characters: 255 bytes
- Characters: Characters that can be used for directory names in the operating system.

  If a path does not end with **/**, the command assumes **/** at the end of it. For example, **/mnt** and **/mnt/** are assumed to be the same directory.

**In Windows.** The mount point directory name must satisfy the following:

- Maximum number of characters: 128 bytes
- Characters: Characters that can be used for folder names in Windows (you cannot use a space character)

  If a path does not end with \, the command assumes \ at the end of them. For example, **D:** and **D:** are assumed to be the same drive. **D:\MOUNTDIR** and **D:\MOUNTDIR** are assumed to be the same directory.

***mount-point-directory-target-definition-file-name***

Specify the name of the batch file which lists the mount point directories for multiple file systems to be backed up. To specify this file, you must specify the file name alone. The following shows where the target definition file for mount point directories is stored and gives examples of entries in the file.

The location of the file (in Windows):
*Protection-Services-installation-directory*\conf\fs

Example of entries in the file (in Windows):
```
D:
E:
F:\MNT
```

The location of the file (in UNIX):
```
/opt/drm/conf/fs
```

Example of entries in the file (in UNIX):
```
/mntpt1
/mntpt2
/fs/mntpt2
```

**-mode online**

Specify this to perform an online backup. This will perform a backup without unmounting the file system.

If you specify an online backup for a file system other than VxFS, only resynchronization processing for the file system will be performed, before the online backup. If applications using the file system are not prevented from updating data, the validity of the backed-up data cannot be guaranteed.

**-target** ***file-or-directory-name(s)***

Specify this option to back up a file system containing the specific files or directories.

Note that, in this option, you must specify the names of the files or directories that exist in the file system specified in ***mount-point-directory-name***. If you specify a file or directory that exists in another file system, the command does not back up the file or directory. Use absolute path names to specify the file names or directory names. To back up two or more files or directories all at one time, use commas to separate each of the file names or directory names you specify.

The file names or directory names specified in this option are registered in the backup catalog. You can use the **drmfscat** command to check them.

If you specify neither this option nor the **-f** option, the command backs up the entire file system specified by ***mount-point-directory-name***.

**-f** ***target-definition-file-name***

Like the **-target** option, this option performs a backup related to specific files or directories (that is, the backup includes the content of such files and directories, and related information). Unlike the **-target** option, this option lets you specify a target definition file that collectively specifies all the files and directories for which backup is to be performed. The target definition file containing the list of absolute paths of the files or directories must be created before you attempt to use this option. Use an absolute path name to specify the target definition file name.

If you specify neither this option nor the **-target** option, the command backs up the entire file system specified by ***mount-point-directory-name***.

**-mode cold**

To perform a cold backup, specify **cold**.

You can perform a cold backup only for a mounted file system. The command unmounts the file system and performs an offline backup for the volume(s) containing the file system. When the backup terminates, the command mounts the file system again. If the command cannot unmount the file system, the command displays an error message and cancels the backup processing. If the volume to be backed up has been unmounted, the command cancels the backup processing.

When the command is executed on the server in a cluster configuration, instead of unmounting the file system, the disk resource to be backed up is placed offline to back up the volume. The disk resource is placed online after backup.

The backup processing is canceled even if the command is executed when either of the following cases applies:

- When operations to place the disk resource offline failed
- When the disk resource is placed offline from the beginning

When this option is not specified, an online backup is performed.

**Notes:**

- In Windows, make sure that another volume is not mounted on the directory of the volume to be backed up when performing an online backup. If so, online backup will fail.
- The backup information in the backup catalog is managed based on the copy group used as a key. Depending on the backup method, you might not be able to perform restoration, even though the backup data exists on the secondary volume.

  The example is described below using the two files, which are located on separate volumes:

  – File system A (copy group: **VG01,dev01**)

  – File system B (copy group: **VG01,dev02**)

  Use the following backup method to back up the file systems:

  1. Back up file system A and file system B concurrently. Backup ID **0000000001** is created.
  2. Back up file system A only. Backup ID **0000000002** is created.

  When you use backup method 2, backup ID **0000000002** is created, and the old backup information (backup ID: **0000000001**) about the copy group **VG01,dev01** on file system A is deleted from the backup catalog. In other words, since the backup information about file system B, which is included in backup ID **0000000001**, is also deleted from the backup catalog, file system B cannot be restored even though the backup data exists in the secondary volume. When you restore file system B, restore the backup data obtained by using backup method 1 from tape to the secondary volume, and then restore the backup data from the secondary volume to the primary volume.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples (in UNIX):**

- The following command performs a cold backup for the entire mount point directory **/mnt**:

```
PROMPT> drmfsbackup /mnt -mode cold
```

- The following command performs an online backup for the files **file01** and **file02** in the file system mounted under the mount point directory **/mnt**:

```
PROMPT> drmfsbackup /mnt -target /mnt/file01,/mnt/file02
```

- The following command performs an online backup for the files that are placed in the file system mounted under the mount point directory **/mnt** and that are specified in the target definition file **/tmp/FILELIST.txt**:

```
PROMPT> drmfsbackup /mnt -f /tmp/FILELIST.txt
```

- The following command performs an online backup concurrently for the mount point directories **/app1**, **/app2**, and **/app/mntpt2** specified in the mount point directory target definition file **APP1**.

  ```
  PROMPT> drmfsbackup APP1
  ```

  The location of the mount point directory target definition file:

  ```
  /opt/drm/conf/fs/APP1
  ```

  Contents of the mount point directory target definition file:

  ```
  /app1
  /app2
  /app/mntpt2
  ```

**Examples (in Windows):**

- The following command performs a cold backup for the entire **D** drive:

  ```
  PROMPT> drmfsbackup D: –mode cold
  ```

- The following command performs an online backup concurrently for the mount point directories **D:**, **E:**, and **F:\MNT** specified in the mount point directory target definition file **APP1**:

  ```
  PROMPT> drmfsbackup APP1
  ```

  The location of the target definition file for the mount point directory is:

  ```
  Protection-Services-installation-directory\conf\fs\APP1
  ```

  Contents of the target definition file for the mount point directory are:

  ```
  D:
  E:
  F:\MNT
  ```

### 6.4.6 drmfscat (display backup information for a file system)

**Format:**

```
drmfscat mount-point-directory-name |
mount-point-directory-target-definition-file-name
         [ -target file-or-directory-name(s)
         | -f target-definition-file-name ]
         [ -device device-file-name ][ -l ][ -v ]
         [ -backup_id backup-ID ][ -hostname host-name ]
```

**Description:**

The **drmfscat** command displays information about the backups performed for the file system. You can also display information about the backup performed for more than one file system.

Table 6.10 lists and describes the displayed items. Each item is separated by a space. A hyphen (-) is displayed for any item that cannot be displayed. If none of the items can be displayed, an error message is displayed.

**Table 6.10 Items Displayed by the drmfscat Command**

| Displayed Item | Description |
|---|---|
| INSTANCE | Mount point directory name |
| BACKUP-ID | Backup ID |
| BACKUP-MODE | Backup mode (**COLD** or **ONLINE**) |
| INSTANCE | Mount point directory name |
| ORIGINAL-ID | Original backup ID obtained by the **drmfsbackup** command |
| START-TIME | Start time of a snapshot backup |
| END-TIME | End time of a snapshot backup |
| HOSTNAME | Server name where the snapshot backup was performed |
| T | Object type (**F**, which indicates a file, is displayed.) |
| FILE | File name |
| FS | Mount point directory name |
| FSTYPE | File system type (**NTFS**, **vxfs**, **ufs**, or **hfs**) |
| DG | Disk group name<br>In Windows, a hyphen (**-**) is displayed. |
| LVM-DEVICE | Logical device file name (In Windows, a GUID is displayed.) |
| DEVICE *1 | Physical device file name (raw device file name) or **Harddisk*n*** (where ***n*** is an integer) |
| COPY-GROUP | Copy group name (CCI volume group name and device name) |
| PORT# | Port name on the server host side |
| TID# | Target ID on the server host side |
| LUN# | Logical unit number on the server host side |
| MU# | Pair identifier |
| LDEV# | Logical device number across RAID devices |
| P/S | Letter to identify whether the volume is primary or secondary:<br>**P**: Primary volume of a pair.<br>**S**: Secondary volume of a pair. |
| SERIAL# | Serial number across RAID devices |
| VIRTUAL-SERVERNAME *2 | Virtual server name (value of the **DRM_HOSTNAME** environment variable) |
| DB-PATH *2 | Name of the directory storing the backup catalog |
| CATALOG-UPDATE-TIME *2 | Time when the backup catalog was created |

***Notes:***

1. If this command is executed with the **-device** option, this information will be displayed after **T**.
2. The command executed with the **-v** option displays this information.

**Arguments:**

***mount-point-directory-name***

Specify the name of the mount point directory or drive letter of the file system for which you want to display backup information, or specify the absolute path from the drive letter.

In UNIX, if a path does not end with **/**, the command assumes **/** at the end of it. For example, **/mnt** and **/mnt/** are assumed to be the same directory.

In Windows, if a path does not end with ****, the command assumes **** at the end of it. For example, **D:** and **D:** are assumed to be the same drive. **D:\MOUNTDIR** and **D:\MOUNTDIR** are assumed to be the same directory.

***mount-point-directory-target-definition-file-name***

Specify the name of the target definition file that specifies the mount point directories for the file systems for which you want to display backup information. To specify this file, you must specify the file name alone. The following shows where the target definition file for mount point directories is stored and gives examples of entries in the file.

The location of the file (in Windows):
*Protection-Services-installation-directory*\conf\fs

Example of entries in the file (in Windows):
```
D:
E:
F:\MNT
```

The location of the file (in UNIX):
```
/opt/drm/conf/fs
```

Example of entries in the file (in UNIX):
```
/mntpt1
/mntpt2
/fs/mntpt2
```

**-target** ***file-name(s) or directory-name(s)***

Displays backup information for specific files or directories in the file system specified by the ***mount-point-directory-name*** option. You can only specify the names of the files or directories that exist in the file system specified by the ***mount-point-directory-name*** option. If you specify a file or directory that does not exist in the specified file system, the backup information of the file or directory is not displayed.

Use absolute path names to specify the file names or directory names. To display information for two or more files or directories all at one time, use commas to separate each of the file names or directory names you specify. Be sure that the name of each individual folder or file is the same as the path returned by the **drmfsbackup** command. If these names are not in complete agreement, the correct backup information will not be displayed.

If you specify neither this option nor the **-f** option, the command displays information for the entire file system specified by ***mount-point-directory-name***.

**-f** ***target-definition-file-name***

Displays backup information for specific files or directories in the file system specified by the ***mount-point-directory-name*** option. Unlike **-target**, this option lets you specify a target definition file that specifies all the files or directories for which you want to display information. The target definition file containing the list of absolute paths of the files or directories must be created before you attempt to use this option. Use an absolute path name to specify the target definition file name. Be sure that the name of each individual folder or file is the same as the path returned by the **drmfsbackup** command. If these names are not in complete agreement, the correct backup information will not be displayed.

If you specify neither this option nor the **-target** option, the command displays information for the entire file system specified by ***mount-point-directory-name***.

**-device** ***device-file-name***

Displays only the file system information, physical disk information, and logical-volume configuration information about a specific device file.

**-l**

Specify this option to display information in the long format.

**-v**

Specify this option to display information for the backup catalog. The following information is displayed:

- Name of the directory storing the backup catalog

  Displays the path that is set in **DRM_DB_PATH** in the environment setup file (**init.conf**). If **DRM_DB_PATH** has not been set, the product installation path appears.

- Virtual server name (value of the **DRM_HOSTNAME** environment variable)

  If the **DRM_HOSTNAME** environment variable has not been set, a hyphen (**-**) appears.

- Time when the backup catalog was created

  For each backup ID, displays the time when the backup catalog was created.

**-backup_id** ***backup-ID***

Specify this argument when you want to display only the backup information of a specific backup ID. A backup ID uniquely identifies backup data and is registered in the backup catalog when a backup is performed.

**-hostname** ***host-name***

Specify this argument to display only information pertaining to a specific host.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples (in UNIX):**

- The following command displays the backup information for the file system specified by the mount point **/mnt**:

```
PROMPT> drmfscat /mnt
INSTANCE: /mnt
BACKUP-ID:0000000001 BACKUP-MODE: COLD INSTANCE: /mnt ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE   FS        DG      DEVICE     COPY-GROUP
F -      /mnt      vg00    c0t0d0     VG01,dev01
F -      -         -       -          VG01,dev01
```

- The following command displays the backup information, in the long format, for the file system specified by the mount point **/mnt**:

```
PROMPT> drmfscat /mnt -target /mnt/file1 -l
INSTANCE: /mnt
BACKUP-ID: 0000000001 BACKUP-MODE: COLD INSTANCE: /mnt ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE         FS    FSTYPE    DG        LVM-DEVICE       DEVICE
COPY-GROUP   PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
F /mnt/file1   /mnt  vxfs      vg00      lvol1            c0t0d0
VG01,dev01   CL1-A  2    10   0   10000 P   15044
F -            -     -         -         -                -
VG01,dev01   CL1-A  2    11   0   10001 P   15044

INSTANCE: /mnt
BACKUP-ID: 0000000002 BACKUP-MODE: ONLINE INSTANCE: /mnt ORIGINAL-ID:0000000002
START-TIME:2002/06/01 10:30:00 END-TIME: 2002/06/01 10:33:00 HOSTNAME: FILESERV1
T FILE         FS    FSTYPE    DG        LVM-DEVICE       DEVICE
COPY-GROUP   PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
F /mnt/file1   /mnt  vxfs      vg00      lvol1            c0t0d0
VG01,dev01   CL1-A  2    10   0   10000 P   15044
F -            -     -         -         -                -
VG01,dev01   CL1-A  2    11   0   10001 P   15044
```

- The following command displays the file system backup information, in the long format, about the disk volume **/dev/rdsk/c0t0d0**:

```
PROMPT> drmfscat /mnt -device c0t0d0 -l
INSTANCE: /mnt
BACKUP-ID: 0000000001 BACKUP-MODE: COLD INSTANCE: /mnt ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T DEVICE             FILE           FS      FSTYPE    DG        LVM-DEVICE
COPY-GROUP   PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
F c0t0d0             /mnt/file1     /mnt      vxfs    vg00      lvol1
VG01,dev01   CL1-A  2    10   0   10000 P   15044
F -                  -              -         -       -         -
VG01,dev01   CL1-A  2    11   0   10001 P   15044

INSTANCE: /mnt
BACKUP-ID: 0000000002 BACKUP-MODE: ONLINE INSTANCE: /mnt ORIGINAL-ID:0000000002
START-TIME:2002/06/01 10:30:00 END-TIME: 2002/06/01 10:33:00 HOSTNAME: FILESERV1
T DEVICE             FILE           FS     FSTYPE    DG        LVM-DEVICE
COPY-GROUP   PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
F c0t0d0             /mnt/file1     /mnt    vxfs      vg00      lvol1
VG01,dev01   CL1-A  2    10   0   10000 P   15044
F -                  -              -       -         -         -
VG01,dev01   CL1-A  2    11   0   10001 P   15044
```

- The following command displays the backup information in the mount point **/mnt**. The host name is **FILESERV1**.

```
PROMPT> drmfscat /mnt -hostname FILESERV1
INSTANCE: /mnt
BACKUP-ID:0000000001 BACKUP-MODE: COLD INSTANCE: /mnt ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE       FS            DG      DEVICE         COPY-GROUP
F -          /mnt          vg00    c0t0d0         VG01,dev01
F -          -             -       -              VG01,dev01
```

- The following command displays backup information for the file system specified by the mount point **/mnt** and management information for the backup catalog:

```
PROMPT> drmfscat /mnt –v
VIRTUAL-SERVERNAME: host1
DB-PATH: /var/opt/drm/db2
INSTANCE: /mnt
BACKUP-ID: 0000000001 BACKUP-MODE: COLD INSTANCE: /mnt ORIGINAL-ID:0000000001
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
CATALOG-UPDATE-TIME: 2002/06/01 10:02:00
T FILE   FS        DG      DEVICE     COPY-GROUP
F -      /mnt      vg00    c0t0d0     VG01,dev01
F -      -         -       -          VG01,dev01
```

- The following command concurrently displays the backup information for the file systems under the mount point directories **/app1**, **/app2**, and **/app/mntpt2** specified in the mount point directory target definition file **APP1**:

```
PROMPT> drmfscat APP1
INSTANCE: APP1
BACKUP-ID:0000000001 BACKUP-MODE: COLD INSTANCE: APP1 ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE FS          DG   DEVICE COPY-GROUP
F -    /app/mntpt2 vg00 c0t0d0 VG01,dev01
F -    /app1       vg00 c0t0d1 VG01,dev02
F -    /app2       vg00 c0t0d2 VG01,dev03
```

**Examples (in Windows):**

- The following command displays the backup information for the file system under the **D** drive:

```
PROMPT> drmfscat D:
INSTANCE: D:
BACKUP-ID:0000000001 BACKUP-MODE: COLD INSTANCE: D: ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE  FS  DG  DEVICE      COPY-GROUP
F -     D:  -   Harddisk1   VG01,dev01
F -     -   -   -           VG01,dev01
```

- The following command displays backup information, in the long format, about the file system related to the disk volume **Harddisk1**:

```
PROMPT> drmfscat D: -device Harddisk1 -l
INSTANCE: D:
BACKUP-ID: 0000000001 BACKUP-MODE: COLD INSTANCE: D: ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE              FS FSTYPE DG LVM-DEVICE
DEVICE    COPY-GROUP PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
F Harddisk1 D:\temp\file1.txt D: NTFS   -
\\?\Volume{df66a5b0-5583-12d5-a410-806d6172696f}\ harddisk1 VG01,dev01 CLI-A  2
10   0   10000 P   15044
F -                 -  -      -  -
-         VG01,dev01 CLI-A  2    11   0   10001 P   15044

INSTANCE: D:
BACKUP-ID: 0000000002 BACKUP-MODE: ONLINE INSTANCE: D: ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:30:00 END-TIME: 2002/06/01 10:33:00 HOSTNAME: FILESERV1
T FILE              FS FSTYPE DG LVM-DEVICE
DEVICE    COPY-GROUP PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
F Harddisk1 D:\temp\file1.txt D: NTFS   -
\\?\Volume{df66a5b0-5583-12d5-a410-806d6172696f}\ harddisk1 VG01,dev01 CLI-A  2
10   0   10000 P   15044
F -                 -  -      -  -
-         VG01,dev01 CLI-A  2    11   0   10001 P   15044
```

- The following command displays the backup information about the file system of the **D** drive. The host name is **FILESERV1**:

```
PROMPT> drmfscat D: -hostname FILESERV1
INSTANCE: D:
BACKUP-ID:0000000001 BACKUP-MODE: COLD INSTANCE: D: ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE   FS  DG    DEVICE      COPY-GROUP
F -      D:  -     Harddisk1   VG01,dev01
F -      -   -     -           VG01,dev01
```

- The following command displays backup information for the file system under the **D** drive and management information for the backup catalog:

```
PROMPT> drmfscat D: -v
VIRTUAL-SERVERNAME: host1
DB-PATH: D:\Program Files\Hitachi\DRM\db2
INSTANCE: D:
BACKUP-ID:0000000001 BACKUP-MODE: COLD INSTANCE: D: ORIGINAL-ID:0000000001
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
CATALOG-UPDATE-TIME: 2002/06/01 10:02:00
T FILE  FS  DG  DEVICE      COPY-GROUP
F -     D:  -   Harddisk1   VG01,dev01
F -     -   -   -           VG01,dev01
```

- The following command displays backup information for the file system under the **D** drive and management information for the backup catalog (when a backup is not performed):

```
PROMPT> drmfscat D: -v
VIRTUAL-SERVERNAME: host1
DB-PATH: D:\Program Files\Hitachi\DRM\db2
KAVX0024-E The specified backup data does not exist.
```

-

- The following command displays backup information for the file system specified by the mount point **D:\MNT**:

```
PROMPT> drmfscat D:\MNT
INSTANCE: D:\MNT
BACKUP-ID:0000000001 BACKUP-MODE: COLD INSTANCE: D:\MNT ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE  FS      DG  DEVICE      COPY-GROUP
F -     D:\MNT  -   Harddisk1   VG01,dev02
F -     -       -   -           VG01,dev02
```

- The following command concurrently displays the backup information for the file systems in the mount point directories **D:**, **E:**, and **F:\MNT** specified in the mount point directory target definition file **APP1**:

```
PROMPT> drmfscat APP1
INSTANCE: APP1
BACKUP-ID:0000000001 BACKUP-MODE: COLD INSTANCE: APP1 ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME:
FILESERV1
T FILE  FS       DG       DEVICE     COPY-GROUP
F -     D:       -        Harddisk1  VG01,dev01
F -     E:       -        Harddisk2  VG01,dev02
F -     F:\MNT   -        Harddisk3  VG01,dev03
```

### 6.4.7 drmfsdisplay (display or update file system information)

**Format:**

To display file system information:

```
drmfsdisplay [ mount-point-directory-name ]
             [ -target file-or-directory-name(s)
             | -f target-definition-file-name ]
             [ -device device-file-name ][ -l ] [ -v ]
```

To update the information in the dictionary map file:

```
drmfsdisplay -refresh
```

**Description:**

The **drmfsdisplay** command has the following three functions:

1. Displays the resource information for the file system on the server where the command is executed.
2. Displays the information about a desired file system in the system where the command is executed, in units of mount point directory name.
3. Updates the file system information for the dictionary map file. Execute this command before performing a backup.

Table 6.11 lists the items displayed by the above functions 1 and 2. Each item is separated by a space. A hyphen (-) is displayed for any item that cannot be displayed. If none of the items can be displayed, an error message is displayed.

**Table 6.11 Items Displayed by the drmfsdisplay Command**

| Displayed Item | Description |
|---|---|
| INSTANCE | Mount point directory name |
| T | Object type (**F**, which indicates a file, is displayed.) |
| FILE | File name |
| FS | Mount point directory name |
| FSTYPE | File system type (**NTFS**, **vxfs**, **ufs**, or **hfs**) |
| DG | Disk group name (In Windows, a hyphen (**-**) is displayed.) |
| LVM-DEVICE | Logical device file name (In Windows, a GUID is displayed.) |
| DEVICE *1 | Physical device file name (raw device file name) or **Harddisk*n*** (where ***n*** is an integer) |
| COPY-GROUP | Copy group name (CCI volume group name and device name) |
| PORT# | Port name on the server host side |
| TID# | Target ID on the server host side |
| LUN# | Logical unit number on the server host side |
| MU# | Pair identifier |
| LDEV# | Logical device number across RAID devices |
| P/S | Letter to identify whether the volume is primary or secondary:<br>**P**: Primary volume of a pair.<br>**S**: Secondary volume of a pair. -: A volume that is not part of a pair. |
| SERIAL# | Serial number across RAID devices |
| VIRTUAL-SERVERNAME *2 | Virtual server name (value of the **DRM_HOSTNAME** environment variable) |
| DB-PATH *2 | Name of the directory storing the dictionary map file |
| CORE-MAPFILE-UPDATE-TIME *2 | Update time for the core map file |
| APP.-MAPFILE-UPDATE-TIME *2 | Update time for the application map file |

***Notes:***

1. If this command is executed with the **-device** option , this will be displayed after **T**.
2. The command executed with the **-v** option displays this information.

**Arguments:**

***mount-point-directory-name***

Specify the name of the mount point directory or drive letter as the file system for which you want to display information, or specify the absolute path.

In UNIX, if a path does not end with **/**, the command assumes **/** at the end of it. For example, **/mnt** and **/mnt/** are assumed to be the same directory.

In Windows, if a path does not end with ****, the command assumes **** at the end of them. For example, **D:** and **D:** are assumed to be the same drive. **D:\MOUNTDIR** and **D:\MOUNTDIR** are assumed to be the same directory.

If this argument is not specified, this command targets all file systems.

**-target** ***file-or-directory-name(s)***

Displays information about specific files or directories. Use absolute path names to specify the file names or directory/path names. To display the information for two or more files or directories, use commas to separate each of the file names or directory names you specify.

**-f** ***target-definition-file-name***

Displays information about specific files or directories. Unlike **-target**, this option lets you specify a target definition file that collectively specifies all the files or directories for which you want to display information. The target definition file containing the list of absolute paths of the files or directories must be created before you use this option. Use an absolute path name to specify the target definition file.

**-device** ***device-file-name***

Displays information about the specific device file only. With this option specified, the command displays the information about the specified device file for the file system specified in the ***mount-point-directory-name*** option. If you do not specify this option, the command displays the information about the specified device file for all the file systems.

**-l**

Specify this option to display information in the long format.

**-v**

Specify this option to display management information for the dictionary map file. The following information is displayed:

- Name of the directory storing the dictionary map file

  Displays the path that is set in **DRM_DB_PATH** in the environment setup file (**init.conf**).

  If **DRM_DB_PATH** has not been set, the product installation path appears.

- Virtual server name (value of the **DRM_HOSTNAME** environment variable)

  If the **DRM_HOSTNAME** environment variable has not been set, a hyphen (**-**) appears.

- Update time for the dictionary map file

  Displays the update time separately for the core map file and the application map file.

**-refresh**

Updates the information in the dictionary map file to the latest state. If you do not specify the ***mount-point-directory-name*** option, the command updates the information in the dictionary map file for all file systems. When the ***mount-point-directory-name*** option is specified, the command updates the information in the dictionary map file for the specified file system.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples (in UNIX):**

- The following command outputs the information about the file system specified by the mount point **/mnt**:

```
PROMPT> drmfsdisplay /mnt
INSTANCE: /mnt
T FILE                FS                  DG      DEVICE              COPY-GROUP
F -                   /mnt                vg00    c0t0d0              VG01,dev01
```

- The following command outputs information, in the long format, about the file **file1** on the file system specified by the mount point **/mnt**:

```
PROMPT> drmfsdisplay /mnt -target /mnt/file1 -l
INSTANCE: /mnt
T FILE                FS           FSTYPE    DG        LVM-DEVICE   DEVICE
COPY-GROUP   PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
F /mnt/file1          /mnt         vxfs      vg00      lvol1         c0t0d0
VG01,dev01   CL1-A  0    0    0   10000 P   15044
```

- The following command outputs file system information, in the long format, about the disk volume **/dev/rdsk/c0t0d0**:

```
PROMPT> drmfsdisplay -device c0t0d0 -l
INSTANCE: /mnt
T DEVICE              FILE           FS      FSTYPE    DG        LVM-DEVICE
COPY-GROUP   PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
F c0t0d0              /mnt/file1     /mnt    vxfs      vg00      lvol1
VG01,dev01   CL1-A  0    0    0   10000 P   15044
```

- The following command displays information about the file system specified by the mount point **/mnt** and management information for the dictionary map file:

```
PROMPT> drmfsdisplay /mnt -v
VIRTUAL-SERVERNAME: host1
DB-PATH: /var/opt/drm/db2
INSTANCE: /mnt
CORE-MAPFILE-UPDATE-TIME: 2002/06/01 10:00:00
APP.-MAPFILE-UPDATE-TIME: 2002/06/01 10:00:00
T FILE                FS                  DG      DEVICE              COPY-GROUP
F -                   /mnt                vg00    c0t0d0              VG01,dev01
```

- The following command displays information about the file system specified by the mount point **/mnt** and management information for the dictionary map file (when the dictionary map file does not exist):

```
PROMPT> drmfsdisplay /mnt -v
VIRTUAL-SERVERNAME: host1
DB-PATH: /var/opt/drm/db2
KAVX0039-E The core map file(s) cannot be found.
```

**Examples (in Windows):**

- The following command outputs information about the file system on the **D** drive:

```
PROMPT> drmfsdisplay D:
INSTANCE: D:
T FILE      FS        DG        DEVICE              COPY-GROUP
F -         D:        -         Harddisk1           VG01,dev01
```

- The following command outputs information about the file system in the mount point **D:\MNT**:

```
PROMPT> drmfsdisplay D:\MNT
INSTANCE: D:\MNT
T FILE      FS            DG        DEVICE              COPY-GROUP
F -         D:\MNT        -         Harddisk1           VG01,dev01
```

- The following command outputs file system information, in the long format, about the file **D:\temp\file1.txt** on the **D** drive:

```
PROMPT> drmfsdisplay D: -target D:\temp\file1.txt -l
INSTANCE: D:
T FILE                FS  FSTYPE  DG  LVM-DEVICE
DEVICE    COPY-GROUP PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
F D:\temp\file1.txt   D:  NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk1 VG01,dev01 CL1-A  0
0    0   10000 P   15044
```

- The following command outputs file system information, in the long format, about the disk volume **Harddisk1**:

```
PROMPT> drmfsdisplay -device Harddisk1 -l
INSTANCE: D:
T DEVICE    FILE                FS   FSTYPE  DG  LVM-DEVICE
COPY-GROUP PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
F Harddisk1 D:\temp\file1.txt   D:   NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\ VG01,dev01 CL1-A  0    0    0
10000 P   15044
```

- The following command displays backup information for the file system on the **D** drive and management information for the dictionary map file:

```
PROMPT> drmfsdisplay D: -v
VIRTUAL-SERVERNAME: host1
DB-PATH: D:\Program Files\Hitachi\DRM\db2
INSTANCE: D:
CORE-MAPFILE-UPDATE-TIME: 2002/06/01 10:00:00
APP.-MAPFILE-UPDATE-TIME: 2002/06/01 10:00:00
T FILE      FS        DG        DEVICE             COPY-GROUP
F -         D:        -         Harddisk1          VG01,dev01
```

- The following command displays backup information for the file system on the **D** drive and management information for the dictionary map file (when the dictionary map file does not exist):

```
PROMPT> drmfsdisplay D: -v
VIRTUAL-SERVERNAME: host1
DB-PATH: D:\Program Files\Hitachi\DRM\db2
KAVX0039-E The core map file(s) cannot be found.
```

### 6.4.8 drmfsrestore (restore a file system from a backup to a primary volume)

**Format:**

```
drmfsrestore backup-ID -resync [ -force ]
                       [ -target file-or-directory-name(s)
                       | -f target-definition-file-name ]
```

**Description:**

The **drmfsrestore** command performs disk resynchronization to restore data to the primary volume from the secondary volume. The backup data used for restoration is specified by a backup ID.

On file systems that consist of multiple physical volumes, all volumes will be restored.

The following explains the command processing for restoration by disk resynchronization and restoration:

1. When the file system to be restored has been mounted, the command automatically unmounts the file system. If the file system cannot be unmounted, the command displays an error message, and the restoration processing will terminate abnormally.

   When the file system has already been unmounted, the command processing goes to the next step.

2. The command makes sure that the file system has been unmounted, and then performs disk resynchronization to restore the backup data from the secondary volume to the primary volume.

3. The command mounts the file system.

The following explains the command processing for restoration in a cluster configuration:

1. The command automatically places the disk resource offline when the disk resource in the file system to be restored is placed online. If operations to place the disk resource offline fail, the command displays an error message and the restoration processing fails.

   When the disk resource has already been placed offline, go on to the next step.

2. The command makes sure that the disk resource is placed offline successfully and then performs disk resynchronization to restore the backup data from the secondary volume to the primary volume.

3. The command places the disk resource online.

Restoration overwrites the entire primary volume with the entire secondary volume that contains a backup of the primary volume. Therefore, additions and changes to the primary volume after the backup was created are not applied.

Before executing this command, all the application programs using the volume to be restored must be ended. The volume being used by the operating system cannot be restored.

This command should not be used when data from the secondary volume is being backed up to tape with the **drmtapebackup** or **drmmediabackup** command, when data from tape is being restored to the secondary volume with the **drmtaperestore** or **drmmediarestore** command, or when the secondary volume is being mounted with the **drmmount** command.

**Arguments:**

***backup-ID***

Specify the backup ID of the backup data you want to use for restoration. A backup ID uniquely identifies backup data and is registered in the backup catalog during backup. To check backup IDs, execute the **drmfscat** command.

**-resync**

Specifies that the primary and secondary volumes should be restored by disk resynchronization. The backup data in the secondary volume is synchronized to the primary volume.

**-force**

Specify this option to perform restoration by forced resynchronization of the primary and secondary volumes.

With this option, perform forced resynchronization if the copy group name of the primary volume obtained when the backup processing was performed on the file server corresponds with the information on the file server, even though the LDEV number and the SERIAL number do not correspond with the LDEV number and the SERIAL number when the backup processing was performed. Specify this option only if restoration by resynchronization could not be performed with the **-resync** option, such as when the LDEV number changes when the volume is replaced. If this option is specified under a normal restoration, data might be corrupted.

**-target** ***file-or-directory-name(s)***

Restores the file system containing the specific files or directories. File names and directory names need to be registered in the backup catalog specified by the backup ID, but even if they are not registered in the catalog, specified files and directories can be restored if they are backed up.

Use absolute path names to specify the file names or directory names. Make sure that the name of each individual folder or file is the same as the path returned by the **drmfsbackup** command with the **-target** or **-f** option. If these names are not in complete agreement, the correct backup information will not be displayed. To restore two or more files or directories all at one time, use commas to separate each of the file names or directory names you specify.

If you specify neither this option nor the **-f** option, the command restores the entire file system specified by ***mount-point-directory-name***.

**-f** ***target-definition-file-name***

Like the **-target** option, specify this option to restore a file system containing the specific files or directories. Unlike the **-target** option, this option lets you specify a target definition file that collectively specifies all the files and directories to be restored. The target definition file containing the list of absolute paths of the files or directories must be created before you attempt to use this option. Use an absolute path name to specify the target definition file name. Be sure that the name of each individual folder or file is the same as the path returned by the **drmfsbackup** command with the **-target** or **-f** option. If these names are not in complete agreement, the correct backup information will not be displayed.

If you specify neither this option nor the **-target** option, the command restores the entire file system specified by ***mount-point-directory-name***.

**Notes:**

The backup information in the backup catalog is managed based on the copy group used as a key. Depending on the backup method, you might not be able to perform restoration, even though the backup data exists on the secondary volume.

The example is described below using the two files, which are located on separate volumes:

- File system A (copy group: **VG01,dev01**)
- File system B (copy group: **VG01,dev02**)

Use the following backup method to back up the file systems:

1. Back up the file system A and the file system B concurrently. The backup ID **0000000001** is created.
2. Back up the file system A only. The backup ID **0000000002** is created.

When you use the backup method 2, the backup ID **0000000002** is created, and the old backup information (backup ID: **0000000001**) about the copy group **VG01,dev01** on the file system A is deleted from the backup catalog. In other words, since the backup information about the file system B, which is included in the backup ID **0000000001**, is also deleted from the backup catalog, the file system B cannot be restored even though the backup data exists in the secondary volume. When you restore the file system B, restore the backup data obtained by using the backup method 1 from tape to the secondary volume, and then restore the backup data from the secondary volume to the primary volume.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Example (in UNIX):**

- The following command performs disk resynchronization for restoration from the backup identified by the backup ID **0000000001**:

```
PROMPT> drmfsrestore 0000000001 –resync
```

**Example (in Windows):**

- The following command performs disk resynchronization for restoration from the backup identified by the backup ID **0000000001**:

```
PROMPT> drmfsrestore 0000000001 –resync
```

### 6.4.9 drmlicense (display or update license information)

**Format:**

To display license information:
`drmlicense` *`product-code`* `-l`

To update the existing license:
`drmlicense` *`product-code`* `-k` *`license-key`*

**Description:**

The ***drmlicense*** command displays and updates license information for Protection Services.

**Arguments:**

***product-code***

Specify the model number of Protection Services for which you want to display license information.

**-l**

Specify this option to display license information for Protection Services.

**-k *license-key***

Specify this option to update the existing license.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples:**

- The following command updates the license for Protection Services (**P-9D13-Y6211**) to the new license (**1234567890ABC**):
```
PROMPT> drmlicense P-9D13-Y6211 -k 1234567890ABC
```
- The following command displays the license information for Protection Services (**P-9D13-Y6211**).

  When the permanent license (**Permanent**) is used:
```
PROMPT> drmlicense P-9D13-Y6211 -l
License Information
License Type: Permanent
Capacity:      1 TB
```

  When the temporary license (**Temporary**) is used:
```
PROMPT> drmlicense P-9D13-Y6211 -l
License Information
License Type: Temporary
Term Of Validity: MM/DD/YYYY
```

  When the emergency license (**Emergency**) is used:
```
PROMPT> drmlicense P-9D13-Y6211 -l
License Information
License Type: Emergency
Term Of Validity: MM/DD/YYYY
```

### 6.4.10 drmmediabackup (back up data from a secondary volume to tape)

**Format:**

```
drmmediabackup backup-ID [ -raw ]
```

**Description:**

The **drmmediabackup** command backs up data to tape based on the backup information specified by the backup ID. Before executing this command, you must execute the **drmmount** command to mount the secondary volume to the specified mount point directory on the backup server. After executing the **drmmediabackup** command, you must also execute the **drmumount** command to unmount the secondary volume.

Both the **drmtaperestore** command and the **drmmediarestore** command can restore the data backed up by the **drmmediabackup** command.

Before executing the **drmmediabackup** command, make sure of the following:

- The volume is linked to the backup management product.
- The copy group including the secondary volume to be backed up is locked to prevent servers other than a backup server from performing operations on that secondary volume.
- A definition file for the tape backup has been created.
- The secondary volume is not in the mirror status.
- The **drmmount** command has been executed and the secondary volume has been mounted on the specified mount point directory.

If an error occurs during execution of the **drmmediabackup** command, check the contents of the trace log of the backup management product that is provided by Protection Services. Then, take actions for the error according to what was output to the log.

For VERITAS NetBackup: The trace log is output to the following file:

In UNIX
`/var/opt/drm/log/drm_nbu_backup.log`

In Windows
*Protection Services-installation-directory*`\log\drm_nbu_backup.log`

For VERITAS Backup Exec: Protection Services does not provide trace logs for VERITAS Backup Exec. If an error occurred, check the log provided by VERITAS Backup Exec, or use the GUI to check the status, and then take actions for the error.

**Arguments:**

***backup-ID***

Specify the backup ID for the secondary volume that contains the backup data to be copied to tape. A backup ID uniquely identifies backup data and is registered in the backup catalog during backup.

Use the backup ID which was used for the previous **drmmount** command. To check backup IDs, execute one of the following commands according to what was backed up:

- **drmfscat** command (when a file system was backed up)
- **drmsqlcat** command (when an SQL Server database was backed up)
- **drmexgcat** command (when a storage group was backed up)

**-raw**

Specify this option to back up the secondary volume as a raw device. This backs up data per logical volume.

In Windows, you can specify this option only for VERITAS NetBackup.

**Note:**

When you use the **drmmediabackup** command, start the **drmmount** command by backup ID specification in advance. The **drmmediabackup** command cannot be used when the **drmmount** command is started by copy group name specification.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Example ( in UNIX):**

- The following commands mount the secondary volume to the directory **/tmp**, and then copy the backup data identified by the backup ID **0000000002** from the secondary volume to tape.

```
PROMPT> drmmount 0000000002 -mount_pt /tmp
PROMPT> drmmediabackup 0000000002
PROMPT> drmumount 0000000002
```

**Example (in Windows):**

- The following commands mount the secondary volume to the **D** drive, and then copy the backup data identified by the backup ID **0000000002** from the secondary volume to tape:

```
PROMPT> drmmount 0000000002 -mount_pt D:
PROMPT> drmmediabackup 0000000002
PROMPT> drmumount 0000000002
```

### 6.4.11 drmmediarestore (restore data from tape to the secondary volume)

**Format:**

```
drmmediarestore backup-ID [ -raw ]
```

**Description:**

The **drmmediarestore** command restores data from tape to the secondary volume according to the backup information specified by the backup ID. Before executing this command, you must execute the **drmmount** command to mount the secondary volume to the specified mount point directory on the backup server. After executing the **drmmediarestore** command, you must also execute the **drmumount** command to unmount the secondary volume.

The **drmmediarestore** command can restore data that is backed up by the **drmmediabackup** command or the **drmtapebackup** command.

This command requires a supported backup management product.

To restore backed up data from tape in the environment that uses VERITAS Backup Exec, use the Protection Services commands in the VERITAS Backup Exec windows.

When you set **BENT** or **BEWS** in the **drmtapeinit** command for working with VERITAS Backup Exec, the **drmmediarestore** command mounts the secondary volume for restoration, and then displays the following message. Use the VERITAS Backup Exec windows to restore the data according to the instructions shown in the message.

When the restore operation terminates, enter one of the following keywords:

- **YES** (If restoration terminated successfully.)
- **NO** (If restoration terminated abnormally.)
- **CANCEL** (To cancel operations.)

Enter the correct keyword after the restoration operation with VERITAS Backup Exec has finished.

Before executing the **drmmediarestore** command, make sure of the following:

- The copy group including the secondary volume for restoration is locked to prevent servers other than a backup server from performing operations on that secondary volume.
- The secondary volume is not in the mirror status.

If an error occurs during execution of the **drmmediarestore** command, check the contents of the trace log of the backup management product that is provided by Protection Services. Then, take actions for the error according to what was output to the log.

For VERITAS NetBackup

The trace log is output to the following file:

In UNIX: **/var/opt/drm/log/drm_nbu_restore.log**
In Windows: ***Protection-Services-installation-directory*\log\drm_nbu_restore.log**

For VERITAS Backup Exec

Protection Services does not provide trace logs for VERITAS Backup Exec. If an error occurred, check the log provided by VERITAS Backup Exec, or use the GUI to check the status, and then take actions for the error.

**Arguments:**

***backup-ID***

Specify the backup ID of the backup data to be restored. A backup ID uniquely identifies backup data and is registered in the backup catalog during backup. To check backup IDs, execute the **drmtapecat** command.

**-raw**

Indicates that the backup data specified by the backup ID has been backed up as a raw device with the **-raw** option specified. Even if you do not specify this option, the command restores data normally no matter whether the **-raw** option was specified for the backup. However, if you specify this option to restore the data that was backed up without the **-raw** option specified, the command outputs a message and terminates abnormally.

In Windows, you can specify this option only for VERITAS NetBackup.

**Note:**

When you use the **drmmediarestore** command, start the **drmmount** command by backup ID specification in advance. The **drmmediarestore** command cannot be used when the **drmmount** command is started by copy group name specification.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Example (in UNIX):**

- The following commands mount the secondary volume to the directory **/tmp**, and restore the backup data identified by the backup ID **0000000002** from tape:

```
PROMPT> drmmount 0000000002 -mount_pt /tmp
PROMPT> drmmediarestore 0000000002
PROMPT> drmumount 0000000002
```

**Example (in Windows):**

- The following commands mount the secondary volume to the **D** drive, and restore the backup data identified by the backup ID **0000000002** from tape:

```
PROMPT> drmmount 0000000002 -mount_pt D:
PROMPT> drmmediarestore 0000000002
PROMPT> drmumount 0000000002
```

### 6.4.12 drmmount (mount a secondary volume)

**Format:**

To perform mount by specifying the name of a copy group (in Windows):

```
drmmount -copy_group copy-group-name
         [ -mount_pt mount-point-directory-name ]
```

To perform mount by specifying the name of a backup ID:

```
drmmount backup-ID [ -mount_pt mount-point-directory-name ][ -raw ][ -force ]
```

**Description:**

The **drmmount** command mounts volumes for the following reasons.

- To clear system cache
- To execute the **drmmediabackup** and **drmmediarestore** command
- To mount volumes being unmounted after executing backup or restoration

If backup ID is specified with the **drmmount** command, this command locks the copy group corresponding to the specified backup ID. The copy group locked by this command can be unlocked using the **drmumount** command. You must use the **drmumount** command to unmount secondary volumes when you mounted the secondary volumes using the **drmmount** command.

A secondary volume that is not formatted as a file system or that is in the mirror status cannot be mounted.

The command outputs a message and terminates abnormally without mounting the secondary volume if one of the following occurs:

- You execute this command on a host that cannot reference the secondary volume.
- The primary volume's copy group name, LDEV number and DKC serial number that were acquired when the backup was executed does not match the information on the current backup server.
- You execute this command on the secondary volume in the paired status (PAIR).

**Arguments:**

**-copy_group** ***copy-group-name*** (in Windows):

Specify the name of the copy group to mount. The system cache must be cleared before a data backup when using Windows systems. Specify the copy group from the backup server to mount the secondary volume and then unmount the secondary volume by using the **drmumount** command to clear the system cache.

To check the name of a copy group, execute either the **drmfscat** command or the **drmfsdisplay** command.

**-mount_pt** ***mount-point-directory-name***

Specifies the name of the mount point directory in which to mount the secondary volume.

**In UNIX:** Use an absolute path to specify the name of the mount point directory. The mount point directory name must satisfy the following:

- Maximum number of characters: 255 bytes
- Characters: Characters that can be used for directory names in the operating system
- The directory must be created before you execute the command.

If a path does not end with **/**, the command assumes **/** at the end of it. For example, **/mnt** and **/mnt/** are assumed to be the same directory.

If a slant (**/**) is specified for a mount point directory name, the command mounts the secondary volume to the mount point where the primary volume was mounted.

**In Windows:** Specify the drive letter of the name of the mount point directory or specify the absolute path from the drive letter. The mount point directory name must satisfy the following:

- Maximum number of characters: 64 bytes
- Characters: Characters that can be used for folder names in Windows (you cannot use a space character)

If you specify a drive for the mount point directory name, the command searches for unused drive names in alphabetical order beginning from the specified drive, and then mounts the secondary volume on the first found drive.

If you specify the absolute path from the drive letter as the mount point directory name, the command mounts the secondary volume on the following location:

Mounting the secondary volume by specifying the copy group name
*absolute-path-specified-for-mount-point-directory-name*

Mounting the secondary volume by specifying the backup ID
*absolute-path-specified-for-mount-point-directory-name\primary-volume-drive-letter\prim*

If a drive letter or absolute path does not end with ****, the command assumes **** at the end of it. For example, **D:** and **D:** are assumed to be the same drive. **D:\MOUNTDIR** and **D:\MOUNTDIR** are assumed to be the same directory.

When this option is omitted, the following mount point will be used:

**In UNIX:**

```
/var/opt/drm/mnt/primary-volume-mount-point
/var/opt/drm/mnt
```

**In Windows:**

The unused drives that can be selected are assigned in alphabetical order when the **drmmount** command is executed.

***backup-ID***

Specify the backup ID associated with the copy groups you want to mount. When two or more copy groups were used for the backup identified by the specified backup ID, the secondary volumes of all the copy groups are mounted.

To check backup IDs, execute one of the following commands according to what was backed up:

- **drmfscat** command (when a file system was backed up)
- **drmsqlcat** command (when an SQL Server database was backed up)
- **drmexgcat** command (when a storage group was backed up)

**-raw**

Specify this option to mount the secondary volume as a raw device. You must specify this option when you specify the **-raw** option for the **drmmediabackup** command to back up data.

When you mount the data that was backed up by the **drmmediabackup** command with the **-raw** option specified, the secondary volume is processed as a raw device even if the **-raw** option is omitted.

If you specify this option to mount the data that was backed up by the **drmmediabackup** command without the **-raw** option specified, the command outputs a message and terminates abnormally.

**-force**

Specify this option to forcibly mount a secondary volume. If the copy group name of the target volume matches the specified backup ID, the command forcibly mounts that volume even if its LDEV number or DKC serial number does not match the specification.

**Note:**

The **-force** option causes the command to mount the secondary volume without checking its LDEV number. This may damage the data.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples (in UNIX):**

- The following command mounts the secondary volume identified by the backup ID **0000000001**:
  ```
  PROMPT> drmmount 0000000001
  ```
  For the above command, if several secondary volumes are backed up to the backup ID **0000000001**, they will be mounted at the following mount point.
  /var/opt/drm/mnt/*primary-volume-mount-point*

  You can use the **drmfscat** command to check the mount point of the primary volume.

- The following command mounts the secondary volume associated with the backup ID **0000000001** to the mount point specified in the **-mount_pt** option:
  ```
  PROMPT> drmmount 0000000001 -mount_pt /mnt
  ```
  /mnt/*primary-volume-mount-point*

  You can use the **drmfscat** command to check the mount point of the primary volume.

**Example (in Windows):**

- The following command mounts the secondary volume identified by the backup ID **0000000001** to **D:**.
  ```
  PROMPT> drmmount 0000000001 -mount_pt D:
  ```
  If several secondary volumes have been backed up with the backup ID **0000000001**, the command searches for an unused drive in alphabetical order beginning from the **D** drive, and mounts the secondary volume to the first found drive.

- The following command mounts the secondary volume identified by the backup ID **0000000001** to **E:\SVOLMNT**.
  ```
  PROMPT> drmmount 0000000001 -mount_pt E:\SVOLMNT
  ```
  The following shows the example of mounting the paths by using the **drmmount** command. If the configuration of the mount point of the primary volume is as follows,
  ```
  P:
  P:\MNT
  Q:
  ```
  then, the **drmmount** command mounts the secondary volume to the following paths:
  ```
  E:\SVOLMNT\P
  E:\SVOLMNT\P\MNT
  E:\SVOLMNT\Q
  ```

### 6.4.13 drmresync (resynchronize copy groups)

**Format:**

To resynchronize a copy group:
`drmresync -copy_group` *`copy-group-name`*

To resynchronize the copy groups associated with a backup ID:
`drmresync -backup_id` *`backup-ID`*

**Description:**

The **drmresync** command resynchronizes either the specified copy group or the copy groups related to the specified backup ID, and returns them to the mirrored status. When you execute this command, the corresponding backup information will be deleted from the backup catalog. Also, since the primary volume will be synchronized to the secondary volume, the backup on the secondary volume will be lost. We recommend that you use this command only after copying the data on the secondary volume to another backup medium, such as tape.

This command should not be used when data from the secondary volume to tape is being backed up with the **drmtapebackup** or **drmmediabackup** command, when data from tape to the secondary volume is being restored with the **drmtaperestore** or **drmmediarestore** command, or when the secondary volume is being mounted with the **drmmount** command.

**Arguments:**

**-copy_group** ***copy-group-name***

Specify the name of the copy group you want to resynchronize.

To check the copy group name, execute one of the following commands according to what was backed up:

- **drmfscat** command (when a file system was backed up)
- **drmsqlcat** command (when an SQL Server database was backed up)
- **drmexgcat** command (when a storage group was backed up)

**-backup_id** ***backup-ID***

Specify the backup ID associated with the copy groups you want to resynchronize. By specifying a backup ID, you can resynchronize all the copy groups used for the backup identified by the specified ID at one time.

To check backup IDs, execute one of the following commands according to what was backed up:

- **drmfscat** command (when a file system was backed up)
- **drmsqlcat** command (when an SQL Server database was backed up)
- **drmexgcat** command (when a storage group was backed up)

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples:**

- The following command resynchronizes the copy group **VG01,dev01**:
  ```
  PROMPT> drmresync -copy_group VG01,dev01
  ```
- The following command locks the copy groups used in the backup identified by the backup ID **0000000001**:
  ```
  PROMPT> drmresync -backup_id 0000000001
  ```

### 6.4.14 drmtapebackup (back up data from a secondary volume to tape)

**Format (in UNIX):**

To back up data from the secondary volume to tape by specifying a backup ID:
```
drmtapebackup backup-ID [ -mount_pt mount-point-directory-name
```

To back up the secondary volume as a raw device:
```
drmtapebackup backup-ID -raw
```

**Format (in Windows):**
```
drmtapebackup backup-ID [ -mount_pt mount-point-directory-name ][ -raw ]
```

**Description:**

The **drmtapebackup** command mounts a secondary volume to the specified mount point directory on the backup server, and backs up data from the backup server to tape based on the backup information of the specified backup ID. After the data is backed up to tape, the secondary volume is automatically unmounted.

Both the **drmtaperestore** command and the **drmmediarestore** command can restore the data backed up by the **drmtapebackup** command.

Before executing the **drmtapebackup** command, make sure of the following:

- The volume is linked to a backup management product.
- The copy group including the secondary volume to be backed up is locked so that the secondary volume to be backed up cannot be operated from a server other than backup servers.
- The configuration file for the tape backup has been created.
- The secondary volume is not in the mirror status.

If an error occurs during execution of the **drmtapebackup** command, check the contents of the trace log of the backup management product that is provided by Protection Services, and then respond to the error according to what was output to the log.

For VERITAS NetBackup:

The trace log is output to the following file:

In UNIX:
`/var/opt/drm/log/drm_nbu_backup.log`

In Windows:
*`Protection Services-installation-directory`*`\log\drm_nbu_backup.log`

For VERITAS Backup Exec:

Protection Services does not provide trace logs for VERITAS Backup Exec. If an error occurred, check the log provided by VERITAS Backup Exec, or activate the GUI to check the status, and then respond to the error.

**Arguments:**

***backup-ID***

Specify the backup ID for the secondary volume that contains the backup data to be copied to tape. A backup ID uniquely identifies backup data, and is registered in the backup catalog during the backup processing.

To check backup IDs, execute one of the following commands according to what was backed up:

- **drmfscat** command (when a file system was backed up)
- **drmsqlcat** command (when an SQL Server database was backed up)
- **drmexgcat** command (when a storage group was backed up)

**-mount_pt** ***mount-point-directory-name***

Use an absolute path to specify the name of the mount point directory in which to mount the secondary volume. The secondary volume is mounted on the specified mount point. The data in the secondary volume is backed up to tape by using the backup management product.

In UNIX

The mount point directory name must satisfy the following:

- Maximum number of characters: 255 bytes
- Characters: Characters that can be used for directory names in the operating system
- The directory must be created before you execute the command.

If a path does not end with **/**, the command assumes **/** at the end of it. For example, **/mnt** and **/mnt/** are assumed to be the same directory.

If a slant (**/**) is specified for a mount point directory name, the command mounts the secondary volume to the mount point where the primary volume was mounted.

In Windows

Specify the drive letter of the name of the mount point directory in which to mount the secondary volume or specify the absolute path from the drive letter.

The mount point directory name must satisfy the following:

- Maximum number of characters: 64 bytes
- Characters: Characters that can be used for folder names in Windows (you cannot use a space character)

If the drive is specified as the mount point directory name, the unused drive is searched in alphabetical order and then mounted.

If you specify the absolute path from the drive letter as the mount point directory name, the command mounts the secondary volume on the following location:
*absolute-path-specified-for-mount-point-directory-name\primary-volume-drive-letter\primary-volume-mount-point*

If a path does not end with \, the command assumes \ at the end of it. For example, **D:** and **D:** are assumed to be the same drive. **D:\MOUNTDIR** and **D:\MOUNTDIR** are assumed to be the same directory.

Specify the name of the mount point directory to which you want to mount the secondary volume. The secondary volume will be mounted on the specified mount point, and the backup management product will back up the secondary volume to the tape.

When this option is omitted, the following mount point will be used:

In UNIX:
`/var/opt/drm/mnt`

In Windows:

Any drive not being used when the **drmtapebackup** command is executed.

**-raw**

Use this option to perform backup of the secondary volume as a raw device. When backup as a raw device is performed, the secondary volume is not unmounted, and backup is performed per logical volume.

In Windows, you can specify this option only for VERITAS NetBackup.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Example (in UNIX):**

- The following command mounts the secondary volume to the directory **/tmp**, and copies the backup data identified by the backup ID **0000000002** from the secondary volume to tape.

```
PROMPT> drmtapebackup 0000000002 -mount_pt /tmp
```

**Example (in Windows):**

- The following command mounts the secondary volume to the **D** drive, and copies the backup data identified by the backup ID **0000000002** from the secondary volume to tape.

```
PROMPT> drmtapebackup 0000000002 –mount_pt D:
```

### 6.4.15 drmtapecat (display or delete backup information in a backup catalog)

**Format:**

To display information for the backup performed from the secondary volume to tape:

```
drmtapecat [ backup-ID ][ -l ][ -hostname host-name ] [ -v ]
```

To display information for the backup performed from the primary volume to the secondary volume:

Copy Controller:

```
drmtapecat -o FILESYSTEM mount-point-or-drive-name |
mount-point-directory-target-definition-file-name[ drmfscat-command-options ]
```

SQL Server:

```
drmtapecat –o MSSQL instance-name [ drmsqlcat-command-options ]
```

Exchange Server:

```
drmtapecat –o MSEXCHANGE [ drmexgcat-command-options ]
```

To delete the backup information:

```
drmtapecat backup-ID –delete
```

**Description:**

The **drmtapecat** command lists the backup information about tape backups, which is stored in the backup catalog on the server where the command was executed.

Table 6.12 lists the displayed items. Each item is separated by a space. A hyphen (-) is displayed for any item that cannot be displayed. If none of the items can be displayed, an error message is displayed.

**Table 6.12 Items displayed by the drmtapecat command**

| Displayed Item | Description |
|---|---|
| BACKUP-ID | Backup ID (10 characters) |
| ORIGINAL-ID *1 | Original backup ID obtained by the **drmtapebackup** command |
| HOSTNAME *1 | Server name where the snapshot backup was performed |
| BACKUP-OBJECT | Snapshot backup object type |
| INSTANCE *1 | Name of the instance that was backed up:<br>▪ When a file system was backed up, the mount point directory name is displayed.<br>▪ When an SQL Server database was backed up, the name of the SQL Server instance is displayed.<br>▪ When an Exchange database was backed up, - is displayed. |
| SNAPSHOT-TIME | Time when a snapshot backup was performed |
| EXPIRATION-TIME | Duration of the backup data on tape |
| BACKUP-MEDIA | Name of the medium label that the backup management product used when backing up data to tape |
| VIRTUAL-SERVERNAME *2 | Virtual server name (value of the **DRM_HOSTNAME** environment variable) |
| DB-PATH *2 | Name of the directory storing the backup catalog |
| CATALOG-UPDATE-TIME *3 | Time when the backup catalog was created |

***Notes:***

1. When the **-l** option is specified, these items are displayed.
2. When the **-v** option is specified, this information is displayed.
3. When the **-v** and **-o** options are specified, this information is displayed.

**Arguments:**

***backup-ID***

Specify this argument to display the backup information for the specified backup ID, or to delete the backup information for the specified backup ID. A backup ID uniquely identifies backup data, and is registered in the backup catalog during the backup processing.

**-l**

Specify this argument when you want to display the following items acquired by the **drmtapebackup** command:

- ORIGINAL-ID
- HOSTNAME
- INSTANCE

**-hostname** ***host-name***

Specify this argument to display only information pertaining to a specific host. This argument can be used when, for example, backup information executed on multiple servers is imported to the server on which you are executing the command.

**-v**

Specify this option to display information about the backup catalog. The following information is displayed:

- Virtual server name (value of the **DRM_HOSTNAME** environment variable)

  If the **DRM_HOSTNAME** environment variable has not been set, a hyphen (**-**) appears.

- Name of the directory storing the backup catalog

  Displays the path that is set in **DRM_DB_PATH** in the environment setup file (**init.conf**).

  If **DRM_DB_PATH** has not been set, the product installation path appears.

- Time when the backup catalog was created

  For each backup ID, displays the time when the backup catalog was created. This information is displayed only when the **-o** option is specified.

**-o FILESYSTEM**

Specify this option when you want to display the information for a backup from a primary volume to a secondary volume, and the type of backup object is a file system.

**-o MSSQL**

Displays detailed information for the backup that was registered when a snapshot backup was performed for the backup information about the instance for the backup object type.

**-o MSEXCHANGE**

Displays detailed information for the backup that was registered when a snapshot backup was performed for the backup information about the instance for the backup object type.

***mount-point-directory-name***

Specify the name of the mount point directory for the file system for which you want to display backup information.

***mount-point-directory-target-definition-file-name***

Specify the name of the mount point directory target definition file for the file system or drive for which you want to display backup information.

***instance-name***

Specify the instance name for the database for which you want to display backup information.

***drmfscat-command-options*** for Copy Controller
or ***drmsqlcat-command-options*** for SQL Server
or ***drmexgcat-command-options*** for Exchange Server

You can specify the following options for the **drmfscat**, **drmsqlcat**, and **drmexgcat** commands. For details about the functions of the options, see the descriptions of these commands.

**-target**
**-f**
**-device**
**-l**
**-backup_id**
**-hostname**
**-transact_log (SQL Server only)**
**-datafile**
**-metafile (SQL Server only)**
**-v**

**-delete**

Specify this argument to delete the backup information for the backup catalog. By using this option, you can delete a backup record for a tape backup before the record's duration specified by the **drmtapeinit** command expires. You can also delete a backup record that is to be stored permanently.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples (in UNIX):**

- The following command displays the backup information for tape backups performed by a backup management product:

```
PROMPT> drmtapecat
BACKUP-ID   BACKUP-OBJECT  SNAPSHOT-TIME        EXPIRATION-TIME     BACKUP-MEDIA
0000000001  FILESYSTEM     2002/02/01 10:00:00  2002/02/02 10:00:00 MEDIA1
0000000002  FILESYSTEM     2002/02/01 11:00:00  2002/02/02 11:00:00 MEDIA2
```

- The following command displays the backup information of the backup ID **0000000002**:

```
PROMPT> drmtapecat 0000000002
BACKUP-ID   BACKUP-OBJECT  SNAPSHOT-TIME        EXPIRATION-TIME     BACKUP-MEDIA
0000000002  FILESYSTEM     2002/02/01 10:30:00  2002/02/03 10:30:00 MEDIA2
```

- The following command displays detailed information for the backup backed up to tape by the backup management product.

```
PROMPT> drmtapecat -l
BACKUP-ID  ORIGINAL-ID HOSTNAME  BACKUP-OBJECT INSTANCE SNAPSHOT-TIME
EXPIRATION-TIME   BACKUP-MEDIA
0000000001 0000000001  FILESV    FILESYSTEM    /mnt1  2002/02/01 10:00:00
2002/02/02 10:00:00 MEDIA1
0000000002 0000000001  APPSV     FILESYSTEM    /app1  2002/02/01 11:00:00
2002/02/02 11:00:00 MEDIA2
```

- The following command, with the host name **FILESV** specified, displays the detailed information for tape backups performed by the backup management product:

```
PROMPT> drmtapecat -hostname FILESV
BACKUP-ID  ORIGINAL-ID HOSTNAME  BACKUP-OBJECT INSTANCE SNAPSHOT-TIME
EXPIRATION-TIME   BACKUP-MEDIA
0000000001 0000000001  FILESV    FILESYSTEM    /mnt     2002/02/01 10:00:00
2002/02/02 10:10:00 MEDIA1
```

- The following command displays information for the backup performed from the primary volume to the secondary volume:

```
PROMPT> drmtapecat -o FILESYSTEM /mnt
INSTANCE: /mnt
BACKUP-ID:0000000010 BACKUP-MODE: COLD INSTANCE: /mnt ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE   FS        DG      DEVICE     COPY-GROUP
F -      /mnt      vg00    c0t0d0     VG01,dev01
F -      -         -       -          VG01,dev01
```

**Examples (in Windows):**

- The following command displays the backup information for tape backups performed by a backup management product:

```
PROMPT> drmtapecat
BACKUP-ID   BACKUP-OBJECT  SNAPSHOT-TIME        EXPIRATION-TIME     BACKUP-MEDIA
0000000002  FILESYSTEM     2002/02/01 11:00:00  2002/02/02 11:00:00 MEDIA3
0000000003  FILESYSTEM     2002/02/01 11:30:00  2002/02/02 11:30:00 MEDIA4
```

- The following command displays the backup information of the backup ID **0000000002**:

```
PROMPT> drmtapecat -backup_id 0000000002
BACKUP-ID   BACKUP-OBJECT  SNAPSHOT-TIME        EXPIRATION-TIME     BACKUP-MEDIA
0000000002  FILESYSTEM     2002/02/01 10:30:00  2002/02/01 10:00:00 MEDIA2
```

- The following command displays detailed information for the backup backed up to tape by the backup management product.

```
PROMPT> drmtapecat -l
BACKUP-ID  ORIGINAL-ID HOSTNAME  BACKUP-OBJECT INSTANCE SNAPSHOT-TIME
EXPIRATION-TIME   BACKUP-MEDIA
0000000001 0000000001  FILESV    FILESYSTEM    D:     2002/02/01 10:00:00
2002/02/02 10:00:00 MEDIA1
0000000002 0000000001  APPSV     FILESYSTEM    E:     2002/02/01 11:00:00
2002/02/02 11:00:00 MEDIA2
```

-

- The following command, with the host name **FILESV** specified, displays the detailed information for tape backups performed by the backup management product:

```
PROMPT> drmtapecat -l -hostname FILESV
BACKUP-ID  ORIGINAL-ID HOSTNAME  BACKUP-OBJECT INSTANCE SNAPSHOT-TIME
EXPIRATION-TIME   BACKUP-MEDIA
0000000001 0000000001  FILESV    FILESYSTEM     D:      2002/02/01 10:00:00
2002/02/02 10:10:00 MEDIA1
```

- The following command displays the backup catalog information for tape backups performed by a backup management product, and management information for the backup catalogs:

```
PROMPT> drmtapecat –v
VIRTUAL-SERVERNAME: host1
DB-PATH: D:\Program Files\Hitachi\DRM\DB2
BACKUP-ID   BACKUP-OBJECT  SNAPSHOT-TIME        EXPIRATION-TIME     BACKUP-MEDIA
0000000001  FILESYSTEM     2002/02/01 10:00:00  2002/02/02 10:00:00 MEIDA1
0000000002  MSSQL           2002/02/01 11:00:00  2002/02/02 10:00:00 MEDIA3
0000000003  MSEXCHANGE     2002/02/01 11:30:00  2002/02/02 10:30:00 MEDIA4
```

- The following command displays backup catalogs for tape backups performed by a backup management product, and management information for the backup catalogs (when a backup is not performed):

```
PROMPT> drmtapecat –v
VIRTUAL-SERVERNAME: host1
DB-PATH: D:\Program Files\Hitachi\DRM\DB2
KAVX0024-E The specified backup data does not exist.
```

- The following command displays information for the file system backup performed from the primary volume to the secondary volume:

```
PROMPT> drmtapecat –o FILESYSTEM D:
INSTANCE: D:
BACKUP-ID:0000000010 BACKUP-MODE: COLD INSTANCE: D: ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: FILESERV1
T FILE  FS  DG  DEVICE      COPY-GROUP
F -     D:  -   Harddisk1   VG01,dev01
F -     -   -   -           VG01,dev01
```

- The following command displays information for the SQL database backup performed from the primary volume to the secondary volume:

```
PROMPT> drmtapecat –o MSSQL SQL1
INSTANCE: SQL1
BACKUP-ID: 0000000010 BACKUP-MODE: ON-LINE INSTANCE: SQL1 ORIGINAL-ID: 0000000001
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: DB_SVR1
T  DB   OBJECT    FILE              FS  DG  DEVICE     COPY-GROUP
M  DB1  METAFILE  C:\METADIR\Meta1   C:  -   -          -
D  DB1  DATAFILE  D:\SQL\data1.mdf   D:  -   Harddisk2  VG02,dev02
-  -    -         -                 -   -   -          VG02.dev02
T  DB1  TRANSACT  D:\SQL\tlog1.ldf   D:  -   Harddisk2  VG02,dev02
-  -    -         -                 -   -   -          VG02.dev02
M  DB2  METAFILE  C:\METADIR\Meta2   C:  -   -          -
D  DB1  DATAFILE  D:\SQL\data2.mdf   D:  -   Harddisk2  VG02,dev02
-  -    -         -                 -   -   -          VG02.dev02
T  DB1  TRANSACT  D:\SQL\tlog2.ldf   D:  -   Harddisk2  VG02,dev02
-  -    -         -                 -   -   -          VG02.dev02
```

- The following command displays information for the storage group backup performed from the primary volume to the secondary volume:

```
PROMPT> drmtapecat -o MSEXCHANGE STR1
STORAGEGROUP: STR1
BACKUP-ID: 0000000010 BACKUP-MODE: ONLINE STORAGEGROUP: STR1 ORIGINAL-ID:
0000000001
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:01:00 HOSTNAME: EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.edb       D:          -
Harddisk1    VG01-dev01
- -             -                    -                       -           -       -
VG01-dev01
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.stm       D:          -
Harddisk1    VG01-dev01
- -             -                    -                       -           -       -
VG01-dev01
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.edb        D:          -
Harddisk1    VG01-dev01
- -             -                    -                       -           -       -
VG01-dev01
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.stm        D:          -
Harddisk1    VG01-dev01
- -             -                    -                       -           -       -
VG01-dev01
T TRANSACT     -                    E:\STR1\E00.log         E:          -
Harddisk2    VG01-dev02
- -             -                    -                       -           -       -
VG01-dev02
T TRANSACT     -                    E:\STR1\E000001.log     E:          -
Harddisk2    VG01-dev02
- -             -                    -                       -           -       -
VG01-dev02
T TRANSACT     -                    E:\STR1\E000002.log     E:          -
Harddisk2    VG01-dev02
- -             -                    -                       -           -       -
VG01-dev02
T TRANSACT     -                    E:\STR1\E000003.log     E:          -
Harddisk2    VG01-dev02
- -             -                    -                       -           -       -
VG01-dev02
C CHECKPOINT   -                    E:\STR1\E00.chk         E:          -
Harddisk2    VG01-dev02
- -             -                    -                       -           -       -
VG01-dev02
```

### 6.4.16 drmtapeinit (register parameters for a backup management product)

**Format:**

To register the parameters for the backup management product:

```
drmtapeinit
```

To display the parameters registered for the backup management product:

```
drmtapeinit -v
```

**Description:**

The **drmtapeinit** command provides an interactive interface that lets you register the parameters for controlling a backup management product that works with Protection Services.

The following shows the location where the parameters registered by this command are stored.

In UNIX:

```
/opt/drm/conf/tape/DEFAULT.dat
```

In Windows:

*Protection-Services-installation-directory*\conf\tape\DEFAULT.dat

Table 6.13 lists the parameters for backup management products that can be registered by using this command.

**Table 6.13 Parameters for Backup Management Products**

| Registration Item | Description |
|---|---|
| Name of the backup management product | Specify **NBU** when using VERITAS NetBackup.<br>Specify **BENT** when using VERITAS Backup Exec 8.6.<br>Specify **BEWS** when using VERITAS Backup Exec 9.0. |
| Period to store a backup catalog used for backing up to tape | Specify the number of days to store backup records.<br>If you specify 0, the backup information is stored permanently.<br>When 0 is specified, **PERMANENT** is displayed for this item in the parameter display result of the command with the **-v** option specified. |

**Arguments:**

**-v**

Specify this argument to display the settings of the parameters currently registered.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples:**

- The following command registers the parameter settings for working with VERITAS NetBackup:

```
PROMPT> drmtapeinit
KAVX0411-I Enter the backup management product name: NBU
KAVX0417-I Enter the number of days to store the backup catalog: 1
KAVX0414-I Backup parameters were updated.
PROMPT>
```

- The following command displays the parameter settings for working with VERITAS NetBackup:

```
PROMPT> drmtapeinit -v
backup-application-name: NBU
days-to-keep-the-backup-catalog: 1
PROMPT>
```

- The following command registers the parameters for working with VERITAS Backup Exec 8.6:

```
PROMPT> drmtapeinit
KAVX0411-I Enter the backup management product name: BENT
KAVX0417-I Enter the number of days to store the backup catalog: 1
KAVX0414-I Backup parameters were updated.
PROMPT>
```

- The following command displays the parameters for working with VERITAS Backup Exec 8.6:

```
PROMPT> drmtapeinit -v
backup-application-name: BENT
days-to-keep-the-backup-catalog: 1
PROMPT>
```

- The following command changes the parameters for working with VERITAS Backup Exec 9.0:

```
PROMPT> drmtapeinit
KAVX0411-I Enter the backup management product name                    : BEWS
KAVX0417-I Enter the number of days to store the backup catalog: 1
KAVX0414-I Backup parameters were updated
PROMPT>
```

- The following command displays the parameters for working with VERITAS Backup Exec 9.0:

```
PROMPT> drmtapeinit -v
backup-application-name : BEWS
days-to-keep-backup-catalog : 1
PROMPT>
```

**Notes:**

- After the storage period (number of days) for the backup information has passed, the backup information will be deleted when the **drmtapeinit** command is next executed.
- If all backup information is deleted, you cannot use the **drmtaperestore** command to restore a backup from tape. To prevent such a problem, set the period for storing backup information longer than the period for protecting media of the backup management product.
- If you no longer require a configuration definition file defined for the tape backup management product, directly delete the file. You must also delete this file if you need to change the configuration definition.

### 6.4.17 drmtaperestore (restore data from tape to a secondary volume)

**Format:**

```
drmtaperestore backup-ID [ -mount_pt mount-point-directory-name ]
```

**Description:**

The **drmtaperestore** command mounts a secondary volume to the specified mount point directory on the backup server, and restores data from tape to the secondary volume. After the data is restored, the secondary volume is automatically unmounted.

The **drmtaperestore** command can restore data that is backed up by the **drmmediabackup** command or the **drmtapebackup** command.

This command requires a supported backup management product.

To restore backed-up data from tape using VERITAS Backup Exec, use the Protection Services command in the VERITAS Backup Exec windows.

When you set **BENT** or **BEWS** in the **drmtapeinit** command for working with VERITAS Backup Exec, the **drmtaperestore** command mounts the secondary volume for restoration, and then displays the following message. Use the VERITAS Backup Exec windows to restore the data according to the instructions shown in the message.

After the restore operation finishes, enter one of the following keywords:

- **YES** (if the operation ended normally)
- **NO** (if the operation ended abnormally)
- **CANCEL** (to cancel the operation)

After VERITAS Backup Exec is used and the restoration operation finishes, enter the correct keyword.

Before executing the **drmtaperestore** command, make sure of the following:

- The copy group including the secondary volume to be restored is locked so that the secondary volume to be backed up cannot be operated from a server other than backup servers.
- The secondary volume is not in a mirrored status.

If an error occurs during execution of the **drmtaperestore** command, check the contents of the trace log of the backup management product that is provided by Protection Services, and then respond to the error according to what was output to the log.

For VERITAS NetBackup:

The trace log is output to the following file:

In UNIX:

```
/var/opt/drm/log/drm_nbu_restore.log
```

In Windows:

```
Protection Services-installation-directory\log\drm_nbu_restore.log
```

For VERITAS Backup Exec:

Protection Services does not provide trace logs for VERITAS Backup Exec. If an error occurred, check the log provided by VERITAS Backup Exec, or activate the GUI to check the status, and then respond to the error.

**Arguments:**

***backup-ID***

Specify the backup ID of the backup data you want to use for restoration. A backup ID uniquely identifies backup data, and is registered in the backup catalog during the backup processing. To check backup IDs, execute the **drmtapecat** command.

**-mount_pt** ***mount-point-directory-name***

Use an absolute path to specify the name of the mount point directory in which to mount the secondary volume.

In UNIX

The mount point directory name must satisfy the following:

- Maximum number of characters: 255 bytes
- Characters: Characters that can be used for directory names in the operating system
- The directory must be created before you execute the command.

If a path does not end with **/**, the command assumes **/** at the end of it. For example, **/mnt** and **/mnt/** are assumed to be the same directory.

If a slant (**/**) is specified for a mount point directory name, the command mounts the secondary volume to the mount point where the primary volume was mounted.

In Windows

Specify the drive letter of the name of the mount point directory in which to mount the secondary volume or specify the absolute path from the drive letter.

The mount point directory name must satisfy the following:

- Maximum number of characters: 64 bytes
- Characters: Characters that can be used for folder names in Windows (you cannot use a space character)

If the drive is specified as the mount point directory name, the unused drive is searched in alphabetical order and then mounted.

If you specify the absolute path from the drive letter as the mount point directory name, the command mounts the secondary volume on the following location:
*absolute-path-specified-for-mount-point-directory-name\primary-volume-drive-letter\primary-*

If a path does not end with ****, the command assumes **** at the end of them. For example, **D:** and **D:** are assumed to be the same drive. **D:\MOUNTDIR** and **D:\MOUNTDIR** are assumed to be the same directory.

If you do not specify this argument, the data is restored to the same directory as the mount point directory used when the data was backed up to tape.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Example (in UNIX):**

- The following command mounts the secondary volume to the directory **/tmp**, and restores the backup data identified by the backup ID **0000000002** from tape:
```
PROMPT> drmtaperestore 0000000002 -mount_pt /tmp
```

**Example (in Windows):**

- The following command mounts the secondary volume to the **D** drive, and restores the backup data identified by the backup ID **0000000002** from tape:
```
PROMPT> drmtaperestore 0000000002 -mount_pt D:
```

### 6.4.18 drmumount (unmount secondary volume)

**Format:**

To perform unmount by specifying the name of a copy group (in Windows):
```
drmumount -copy_group copy-group-name
```

To perform unmount by specifying the name of a backup ID:
```
drmumount backup-ID
```

**Description:**

The **drmumount** command unmounts the secondary volumes that were mounted by using the **drmmount** command.

If the volume for the specified backup ID or copy group has already been unmounted, the command displays a warning that the target volume has been unmounted, and then continues processing.

If you use the **drmmediabackup** or **drmmedibarestore** command to back up or restore data, you must use this command to unmount the secondary volume.

Before executing this command, all application programs using the secondary volume must be ended. If you execute the following commands during mounting of the secondary volume, you will not be able to unmount the secondary volume using the **drmumount** command.

- **drmdbimport**
- **drmfsbackup**, **drmsqlbackup**, **drmexgbackup**
- **drmresync**
- **drmtaperestore**

If it is not possible to unmount a secondary volume using the **drmumount** command, unlock the copy group corresponding to the backup ID using the **drmcgctl** command. Then unmount the secondary volume using the following procedure:

- In UNIX: Use the **umount** command of the operating system.
- In Windows: Use the unmount functionality of CCI

**Arguments:**

**-copy_group** ***copy-group-name*** (in Windows)

Specify the name of the copy group to be unmounted (a copy group mounted by using the **drmmount** command). The system cache must be cleared before a data backup when using Windows systems. Specify the copy group from the backup server to mount the secondary volume and then unmount the secondary volume by using the **drmumount** command to clear the system cache.

To check the name of a copy group, execute either the **drmfscat** command or the **drmfsdisplay** command.

To check the name of a copy group, execute the **drmfscat** command or **drmfsdisplay** command.

***backup-ID***

Specify the backup ID associated with the copy groups you want to unmount. When two or more copy groups were used for the backup identified by the specified backup ID, the secondary volumes of all the copy groups are unmounted.

To check backup IDs, execute one of the following commands according to what was backed up:

- **drmfscat** command (when a file system was backed up)
- **drmsqlcat** command (when an SQL Server database was backed up)
- **drmexgcat** command (when a storage group was backed up)

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Example:**

- The following command mounts the secondary volume identified by the backup ID **0000000001**:

```
PROMPT> drmumount 0000000001
```

## 6.5 SQL Server Command Specifications

### 6.5.1 drmsqlbackup (back up an SQL Server database to a secondary volume)

**Format:**

To back up the whole instance containing the system database:

```
drmsqlbackup instance-name -system
```

To back up all user databases:

```
drmsqlbackup instance-name
```

To back up a specific database:

```
drmsqlbackup instance-name
             [ -target database-name | -f target-definition-file-name ]
```

**Description:**

The **drmsqlbackup** command takes the volume that contains the specified instance in memory, and backs it up to the secondary volume. If the instance's objects (such as data files and various databases) exist across several volumes, all primary volumes will be backed up to secondary volumes.

When SQL Server instances are backed up, an online backup will be performed. If instances that are not running are specified when executing a command, the command will terminate abnormally.

When a command is executed, SQL Server VDI (Virtual Device Interface) is used to create a snapshot of the database within the instance. Snapshot data (metafiles) are stored in the VDI metafile storage directory registered by the **drmsqlinit** command. The file name is **backup-ID_database-ID.dmp**.

The backup ID used in the metafile is a ten-digit numerical value assigned during command execution. The database ID is a ten-digit numerical value, assigned by the SQL server, that identifies a database.

If you specify an instance that is not running, the command fails. All the user databases included in the instance are to be backed up. The system database for SQL server is not included. When you back up a system database, execute the command with the **-system** option.

The system cache of the secondary volume must be cleared before executing this command. Mount or unmount the secondary volume on the backup server to clear the system cache.

When you execute this command on the copy group in the paired status (**PAIR**), the status of the copy group is changed to **PSUS**.

**Arguments:**

***instance-name***

Specify the database instance to be backed up. If the instance to be backed up is the default (**MSSQLSERVER**), specify **DEFAULT**.

**-system**

Use this option to set the system database (except the **tempdb** database) as the database to be backed up. SQL Server will be stopped for the restoration when this option is specified.

**-target *database-name(s)***

Specify this option to back up an instance containing the specific files or directories.

When specifying multiple databases to be backed up, use a comma to separate each database name. If you specify a database name containing a space character, enclose the database name in double quotations ". Make sure that you specify the database in the instance specified by the instance-name option. If you specify databases in separate instances, those databases will not be backed up.

The database names specified in this option will be registered in the backup catalog, and can be checked using the **drmsqlcat** command.

**-f *target-definition-file-name***

Like the **-target** option, this option performs a backup related to specific databases only. Unlike the **-target** option, this option lets you specify a target definition file that collectively specifies all the databases for which backup is to be performed. The target definition file containing the list of databases must be created before you attempt to use this option. Use an absolute path name to specify the target definition file. If you specify a target definition file name containing a space character, enclose the target definition file name in double quotations ".

The database specified in the target definition file must exist in the instance specified in the instance-name option. If you specify databases in separate instances, those databases will not be backed up.

**Notes:**

- Make sure that another volume is not mounted on the directory of the volume to be backed up when performing an online backup.
- The backup information in the backup catalog is managed based on the copy group used as a key. Depending on the backup method, you might not be able to perform restoration, even though the backup data exists on the secondary volume.

  The example is described below using the two databases, which are located on separate volumes:

  - Database A (copy group: **VG01,sql01**)
  - Database B (copy group: **VG01,sql01**)

  Use the following backup method to back up the databases:

  1. Back up database A and database B concurrently. The backup ID **0000000001** is created.
  2. Back up database A only. The backup ID **0000000002** is created.

When you use backup method 2, the backup ID **0000000002** is created, and the old backup information (backup ID: **0000000001**) about copy group **VG01,sql01** on database A is deleted from the backup catalog. In other words, since the backup information about database B, which is included in the backup ID **0000000001**, is also deleted from the backup catalog, database B cannot be restored even though the backup data exists in the secondary volume. When you restore database B, restore the backup data obtained by using backup method 1 from tape to the secondary volume, and then restore the backup data from the secondary volume to the primary volume.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples:**

- The following command performs online backup of all databases in the instance **SQLDB**:
  ```
  PROMPT> drmsqlbackup SQLDB
  ```
- The following command performs online backup of databases **DB01** and **DB02** in the instance **SQLDB**:
  ```
  PROMPT> drmsqlbackup SQLDB -target DB01,DB02
  ```

### 6.5.2 drmsqlcat (display backup information for a SQL Server database)

**Format:**

```
drmsqlcat instance-name
          [ -target database-name | -f target-definition-file-name ]
          [ -transact_log ][ -datafile ][ -metafile ]
          [ -device device-file-name ][ -l ][ -v ]
          [ -backup_id backup-ID ][ -hostname host-name ]
```

**Description:**

The **drmsqlcat** command displays the backup information of the SQL Server database on the server where the command is executed. Table 6.14 lists and describes the items displayed by the **drmsqlcat** command.

Each item is separated by a space. A hyphen (-) is displayed for any item that cannot be displayed. If none of the items can be displayed, an error message is displayed.

**Table 6.14 Items Displayed by the drmsqlcat Command (continues on the next page)**

| Displayed Item | Description |
|---|---|
| INSTANCE | SQL Server instance name |
| BACKUP-ID | Backup ID |
| BACKUP-MODE | Backup mode (ONLINE) |
| ORIGINAL-ID | Original backup ID obtained by the drmsqlbackup command |

**Table 6.14 Items Displayed by the drmsqlcat Command (continued)**

| Displayed Item | Description |
|---|---|
| START-TIME | Snapshot backup start time |
| END-TIME | Snapshot backup end time |
| HOSTNAME | Server name where the snapshot backup was performed |
| T | Object type: D: Data file T: Transaction log M: Metafile |
| DB | SQL Server database name |
| OBJECT | SQL Server object name:<br>DATAFILE: Data file name<br>TRANSACT: Transaction file name<br>METAFILE: VDI metafile name |
| FILE | File name |
| FS | Mount point directory name |
| FSTYPE | File system type (NTFS) |
| DG | A hyphen (-) is displayed. |
| LVM-DEVICE | A GUID is displayed. |
| DEVICE *1 | Harddiskn (where n is an integer) |
| COPY-GROUP | Copy group name, displayed as follows:<br>CCI volume group name, device name |
| PORT# | Port name on the host server |
| TID# | Target-ID on the host server |
| LUN# | Logical unit number on host server |
| MU# | Pair ID |
| LDEV# | Logical device number inside the RAID device |
| P/S | A letter identifying the primary or secondary volume:<br>P: Primary volume<br>S: Secondary volume<br>-: Others |
| SERIAL# | Serial number inside the RAID device |
| VIRTUAL-SERVERNAME *2 | Virtual server name (value of the DRM_HOSTNAME environment variable) |
| DB-PATH *2 | Name of the directory storing the backup catalog |
| CATALOG-UPDATE-TIME *2 | Time when the backup catalog was created |

***Notes:***

1. When this command is executed with the **-device** option specified, this will be displayed after **OBJECT**.
2. The command executed with the **-v** option displays this information.

**Arguments:**

***instance-name***

Specify the instance name of the database to display the information for backup. If the instance to be recovered is the default (**MSSQLSERVER**), specify **DEFAULT**.

**-target *database-name(s)***

Displays backup information for a specific database:

- File name
- File system information
- Structural information about the logical volume
- Physical disk information

To display the information for multiple storage groups, use a comma to separate each database name. If you specify database name containing a space character, enclose database name in double quotations ".

When both this option and the **-f** option are omitted, all database information about the instance specified by the instance name will be displayed.

**-f *target-definition-file-name***

Specifies that backup information for specific databases is to be referenced. Unlike the **-target** option, this option lets you specify a target definition file that collectively specifies all the databases whose backup information you want to display. The target definition file containing the list of databases must be created before you attempt to use this option. Use an absolute path name to specify the target definition file. If you specify database name containing a space character, enclose database name in double quotations ".

When both this option and the **-target** option are omitted, all information about the instance specified by the instance name will be displayed.

**-transact_log**

Specifies that only information relating to the transaction log file is to be displayed. This option will display the following information:

- The name of the transaction log file
- File system information
- Structural information about the logical volume
- Physical disk information

**-datafile**

Specifies that only information relating to the data file is to be displayed. This option will display the following information.

- The name of the data file
- File system information
- Logical volume structure information
- Physical disk information

**-metafile**

Specifies that only information relating to the metafile is to be displayed. This option will display the following information.

- The name of the metafile
- File system information
- Logical volume structure information
- Physical disk information

**-device *device-file-name***

Specifies that only the information for the specified device files about the instance specified by the ***instance-name*** option is to be displayed. This option will display the following information:

- Database information
- The name of the transaction log file
- Data file information
- File system information
- Physical disk information
- Logical volume structure information

**-l**

Specifies that information is to be displayed in the long format.

**-v**

Specify this option to display information about the backup catalog.

The following information is displayed:

- Name of the directory storing the backup catalog. Displays the path that is set in **DRM_DB_PATH** in the environment setup file (**init.conf**). If **DRM_DB_PATH** has not been set, the product installation path appears.
- Virtual server name (value of the **DRM_HOSTNAME** environment variable). If the **DRM_HOSTNAME** environment variable has not been set, a hyphen (-) appears.
- For each backup ID, displays the time when the backup catalog was created.

**-backup_id *backup-ID***

Specifies that backup information for a certain backup ID is to be displayed. A backup ID, which uniquely identifies a certain piece of backup data, is registered in the backup catalog during backup.

**-hostname *host-name***

Specify this argument to display information pertaining a specific host only.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples:**

- The following command outputs information about the SQL Server database specified in instance **SQL1**:

```
PROMPT> drmsqlcat SQL1
INSTANCE: SQL1
BACKUP-ID: 0000000001 BACKUP-MODE: ON-LINE INSTANCE: SQL1 ORIGINAL-ID: 0000000001
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: DB_SVR1
T DB        OBJECT    FILE                 FS          DG      DEVICE
COPY-GROUP
M DB1       METAFILE  C:\METADIR\Meta1      C:          -       -            -
D DB1       DATAFILE  D:\SQL\data1.mdf     D:          -       Harddisk2
VG02,dev02
- -          -         -                    -           -       -
VG02.dev02
T DB1       TRANSACT  D:\SQL\tlog1.ldf     D:          -       Harddisk2
VG02,dev02
- -          -         -                    -           -       -
VG02.dev02
M DB2       METAFILE  C:\METADIR\Meta2      C:          -       -            -
D DB1       DATAFILE  D:\SQL\data2.mdf     D:          -       Harddisk2
VG02,dev02
- -          -         -                    -           -       -
VG02.dev02
T DB1       TRANSACT  D:\SQL\tlog2.ldf     D:          -       Harddisk2
VG02,dev02
- -          -         -                    -           -       -
VG02.dev02
```

- The following command displays two generations of backup information, in the long format, about the SQL Server database specified in instance **SQL1**:

```
PROMPT> drmsqlcat SQL1 -l
INSTANCE: SQL1
BACKUP-ID: 0000000001 BACKUP-MODE: ON-LINE INSTANCE: SQL1 ORIGINAL-ID: 0000000001
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: DB_SVR1
T DB  OBJECT    FILE             FS FSTYPE  DG  LVM-DEVICE
DEVICE    COPY-GROUP   PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
M DB1 METAFILE  C:\METADIR\Meta1 C: NTFS    -
\\?\Volume{df66a5b0-5583-12d5-a410-806d6172696f}\  Harddisk1 VG11,dev01   CLI-A  2
10   0   10010 P   15044
D DB1 DATAFILE  D:\SQL\data1.mdf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk2 VG12,dev02   CLI-A  2
20   0   10020 P   15044
- -   -         -               -  -       -   -
-         VG12.dev02   CLI-A  2    21   0   10021 S   15044
T DB1 TRANSACT  D:\SQL\tlog1.ldf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk2 VG12,dev02   CLI-A  2
20   0   10020 P   15044
- -   -         -               -  -       -   -
-         VG12.dev02   CLI-A  2    21   0   10021 S   15044
M DB2 METAFILE  C:\METADIR\Meta2 C: NTFS    -
\\?\Volume{df66a5b0-5583-12d5-a410-806d6172696f}\  Harddisk1 VG11,dev01   CLI-A  2
10   0   10010 P   15044
D DB1 DATAFILE  D:\SQL\data2.mdf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk2 VG12,dev02   CLI-A  2
20   0   10020 P   15044
```

```
- -   -         -                -  -       -   -
-         VG12.dev02   CLI-A  2    21   0   10021 S   15044
T DB1 TRANSACT  D:\SQL\tlog2.ldf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk2 VG12,dev02   CLI-A  2
20   0   10020 P   15044
- -   -         -                -  -       -   -
-         VG12.dev02   CLI-A  2    21   0   10021 S   15044

INSTANCE: SQL1
BACKUP-ID: 0000000002 BACKUP-MODE: ON-LINE INSTANCE: SQL1 ORIGINAL-ID: 0000000002
START-TIME: 2002/06/02 10:00:00 END-TIME: 2002/06/02 10:03:00 HOSTNAME: DB_SVR1
T DB  OBJECT    FILE             FS FSTYPE  DG  LVM-DEVICE
DEVICE    COPY-GROUP   PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
M DB1 METAFILE  C:\METADIR\Meta1 C: NTFS    -
\\?\Volume{df66a5b0-5583-12d5-a410-806d6172696f}\  Harddisk1 VG11,dev01   CLI-A  2
10   0   10010 P   15044
D DB1 DATAFILE  D:\SQL\data1.mdf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk2 VG12,dev02   CLI-A  2
20   0   10020 P   15044
- -   -         -                -  -       -   -
-         VG12.dev02   CLI-A  2    21   0   10021 S   15044
T DB1 TRANSACT  D:\SQL\tlog1.ldf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk2 VG12,dev02   CLI-A  2
20   0   10020 P   15044
- -   -         -                -  -       -   -
-         VG12.dev02   CLI-A  2    21   0   10021 S   15044
M DB2 METAFILE  C:\METADIR\Meta2 C: NTFS    -
\\?\Volume{df66a5b0-5583-12d5-a410-806d6172696f}\  Harddisk1 VG11,dev01   CLI-A  2
10   0   10010 P   15044
D DB1 DATAFILE  D:\SQL\data2.mdf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk2 VG12,dev02   CLI-A  2
20   0   10020 P   15044
- -   -         -                -  -       -   -
-         VG12.dev02   CLI-A  2    21   0   10021 S   15044
T DB1 TRANSACT  D:\SQL\tlog2.ldf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk2 VG12,dev02   CLI-A  2
20   0   10020 P   15044
- -   -         -                -  -       -   -
-         VG12.dev02   CLI-A  2    21   0   10021 S   15044
```

- The following command displays information, in the long format, about the SQL server database in the instance **SQL1**. The host name is specified as **DB_SVR1**:

```
PROMPT> drmsqlcat SQL1 -l -hostname DB_SVR1
INSTANCE: SQL1
BACKUP-ID: 0000000001 BACKUP-MODE: ON-LINE INSTANCE: SQL1 ORIGINAL-ID: 0000000001
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: DB_SVR1
T DB  OBJECT    FILE             FS FSTYPE  DG  LVM-DEVICE
DEVICE    COPY-GROUP   PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
M DB1 METAFILE  C:\METADIR\Meta1 C: NTFS    -
\\?\Volume{df66a5b0-5583-12d5-a410-806d6172696f}\  Harddisk1 VG11,dev01   CLI-A  2
10   0   10010 P   15044
D DB1 DATAFILE  D:\SQL\data1.mdf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk2 VG12,dev02   CLI-A  2
20   0   10020 P   15044
- -   -         -                -  -       -   -
-         VG12.dev02   CLI-A  2    21   0   10021 S   15044
T DB1 TRANSACT  D:\SQL\tlog1.ldf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk2 VG12,dev02   CLI-A  2
20   0   10020 P   15044
- -   -         -                -  -       -   -
-         VG12.dev02   CLI-A  2    21   0   10021 S   15044
M DB2 METAFILE  C:\METADIR\Meta2 C: NTFS    -
\\?\Volume{df66a5b0-5583-12d5-a410-806d6172696f}\  Harddisk1 VG11,dev01   CLI-A  2
10   0   10010 P   15044
```

```
D DB1 DATAFILE  D:\SQL\data2.mdf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk2 VG12,dev02   CLI-A  2
20   0   10020 P   15044
- -   -         -               -  -       -   -
-         VG12.dev02   CLI-A  2    21   0   10021 S   15044
T DB1 TRANSACT  D:\SQL\tlog2.ldf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk2 VG12,dev02   CLI-A  2
20   0   10020 P   15044
- -   -         -               -  -       -   -
-         VG12.dev02   CLI-A  2    21   0   10021 S   15044
```

- The following command outputs information about the SQL Server database specified by the instance **SQL1** and management information for the backup catalog:

```
PROMPT> drmsqlcat SQL1 -v
VIRTUAL-SERVERNAME: DB_SVR1
DB-PATH: D:\Program Files\Hitachi\DRM\db2
INSTANCE: SQL1
BACKUP-ID: 0000000001 BACKUP-MODE: ON-LINE INSTANCE: SQL1 ORIGINAL-ID: 0000000001
START-TIME: 2002/06/01 10:00:00 END-TIME: 2002/06/01 10:03:00 HOSTNAME: DB_SVR1
CATALOG-UPDATE-TIME: 2002/06/01 11:00:00
T  DB   OBJECT    FILE              FS  DG  DEVICE     COPY-GROUP
M  DB1  METAFILE  C:METADIR\Meta1   C:  -   -          -
D  DB1  DATAFILE  D:\SQL\data1.mdf  D:  -   Harddisk2  VG02,dev02
-  -    -         -                 -   -   -          VG02.dev02
T  DB1  TRANSACT  D:\SQL\tlog1.ldf  D:  -   Harddisk2  VG02,dev02
-  -    -         -                 -   -   -          VG02.dev02
M  DB2  METAFILE  C:METADIR\Meta2   C:  -   -          -
D  DB1  DATAFILE  D:\SQL\data2.mdf  D:  -   Harddisk2  VG02,dev02
-  -    -         -                 -   -   -          VG02.dev02
T  DB1  TRANSACT  D:\SQL\tlog2.ldf  D:  -   Harddisk2  VG02,dev02
-  -    -         -                 -   -   -          VG02.dev02
```

- The following command outputs information about the SQL Server database specified by the instance **SQL1** and management information for the backup catalog (when a backup is not performed):

```
PROMPT> drmsqlcat SQL1 -v
VIRTUAL-SERVERNAME: DB_SVR1
DB-PATH: D:\Program Files\Hitachi\DRM\db2
KAVX0024-E The specified backup data does not exist.
```

### 6.5.3 drmsqldisplay (display or update information for a SQL Server database)

**Format:**

To display the information for the SQL Server database:

```
drmsqldisplay [ instance-name ]
              [ -target database-name | -f target-definition-file-name ]
              [ -transact_log ][ -datafile ]
              [ -device device-file-name ][ -l ][ -v ]
```

To update the information in the dictionary map file:

```
drmsqldisplay [ instance-name ] -refresh
```

**Description:**

The **drmsqldisplay** command does the following:

1. Displays the resource information of the SQL Server database on the server on which the command was executed.
2. Displays resource information pertaining to optional instances for the system on which the command was executed.
3. Updates the SQL Server database information of the dictionary map file. Execute this command before performing a backup.

**Error! Reference source not found.** lists and describes the items displayed in 1 and 2.

A hyphen (-) will be displayed in columns that contain items that cannot be displayed. An error message will be displayed when none of the items can be displayed.

Each item is separated by space.

**Table 6.15 Items Displayed by the drmsqldisplay Command (continues on the next page)**

| Displayed Item | Description |
|---|---|
| INSTANCE | The name of the SQL server instance |
| T | The object type:<br>D: Data file<br>T: Transaction log |
| DB | The name of the SQL server database |
| OBJECT | The name of the SQL server object:<br>DATAFILE: The name of the data file<br>TRANSACT: The name of the transaction log file |
| FILE | The file name |
| FS | The mount point directory name |
| FSTYPE | The type of file system (NTFS) |
| DG | A hyphen (-) is displayed. |
| LVM-DEVICE | A GUID is displayed. |
| DEVICE *1 | Harddiskn (where n is an integer) |

**Table 6.15 Items Displayed by the drmsqldisplay Command (continued)**

| Displayed Item | Description |
|---|---|
| COPY-GROUP | The copy group name, shown in the following format:<br>The name of the CCI Volume Group, the loop name, and the device name. |
| PORT# | The port name on the host server |
| TID# | The target ID on the host server. |
| LUN# | The logical unit number on the host server. |
| MU# | Paired ID |
| LDEV# | The logical device number within the RAID setup. |
| P/S | A letter to distinguish the primary volume from the secondary volume:<br>P: Primary volume<br>S: Secondary volume<br>-: A volume that is not part of a pair. |
| SERIAL# | The serial number within the RAID device |
| VIRTUAL-SERVERNAME *2 | Virtual server name (value of the DRM_HOSTNAME environment variable) |
| DB-PATH *2 | Name of the directory storing the dictionary map file |
| CORE-MAPFILE-UPDATE-TIME *2 | Update time for the core map file |
| APP.-MAPFILE-UPDATE-TIME *2 | Update time for the application map file |

***Notes:***

1. When this command is executed with the **-device** option specified, this will be displayed after **OBJECT**.
2. The command executed with the **-v** option displays this information.

**Arguments:**

***instance-name***

Specify the name of the SQL Server database instance for which information is to be updated or displayed. If the instance to be backed up is the default (**MSSQLSERVER**), specify **DEFAULT**. If the instance name is omitted, use the **drmsqlinit** command to display information for all registered instances.

**-target *database-name(s)***

Specifies that information is to be displayed or updated regarding specific databases of the instance ***instance-name***. To display or update information for more than one database, separate the database names using commas. If you specify a database name containing a space character, enclose the name in double quotations ".

**-f *target-definition-file-name***

Displays information regarding specific databases of the instance ***instance-name***. Unlike **-target**, this option lets you specify a target definition file that specifies a list of databases for which the information is to be displayed. The target definition file containing the list of databases must be created before you attempt to use this option. Use an absolute path to specify the file name. If you specify a target definition file name containing a space character, enclose the target definition file name in double quotations ".

**-transact_log**

Displays information relating to the transaction log file only. This option will display the following information:

- The name of the transaction log file
- File system information
- Logical volume structure information
- Physical disk information

When you specify this option with the ***instance-name*** option, only the information about the transaction log of the specified instance will be displayed. When the ***instance-name*** option is omitted, information about all instance transaction logs will be displayed.

**-datafile**

Displays only the information about the data file of the specified instance. This option will display the following information:

- The name of the data file
- File system information
- Logical volume structure information
- Physical disk information

When you specify this option with the ***instance-name*** option, the command displays only information about the data file of the specified instance. When the ***instance-name*** option is omitted, information about the data files of all instances will be displayed.

**-device *device-file-name***

Displays information relating to the device file only. This option will display the following information:

- The name of the SQL Server database
- The transaction log
- Data file information
- File system information
- Physical disk information
- Logical volume structure information

When you specify this option with the ***instance-name*** option, the command displays only information about the device files of the specified instance. When the ***instance-name*** option is omitted, information about the device files of all instances will be displayed.

**-l**

Specifies that SQL Server database information is to be displayed in the long format.

**-v**

Specify this option to display management information about the dictionary map file. The following information is displayed:

- Name of the directory storing the backup catalog. Displays the path that is set in **DRM_DB_PATH** in the environment setup file (**init.conf**). If **DRM_DB_PATH** has not been set, the product installation path appears.
- Virtual server name (value of the **DRM_HOSTNAME** environment variable). If the **DRM_HOSTNAME** environment variable has not been set, a hyphen (**-**) appears.
- Update time for the dictionary map file. Displays the update time separately for the core map file and the application map file.

**-refresh**

Updates dictionary map file information to the latest status. When you specify this option with the ***instance-name*** option, only information about the device file will be displayed. When the ***instance-name*** option is omitted, the information for dictionary map files related to the all instances will be updated.

The dictionary map file must be updated to the latest status by using this command when any of the following cases apply:

- When an instance of SQL Server is created
- When the SQL server database configuration has been changed
- When the CCI configuration definition file has been changed and a pair of volumes has been changed
- When the mount point has been changed
- When the disk configuration such as adding or removing a hard disk has been changed
- When the storage location of the dictionary map has been changed by executing the drmdbsetup utility.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples:**

- The following command outputs information about the database **SQL1**:

```
PROMPT> drmsqldisplay SQL1
INSTANCE: SQL1
T DB     OBJECT    FILE                 FS          DG   DEVICE       COPY-GROUP
D DB1    DATAFILE  D:\SQL\data1.mdf     D:          -    Harddisk1    VG01,dev01
- -      -         -                    -           -    -            VG01,dev01
T DB1    TRANSACT  D:\SQL\tlog1.ldf     D:          -    Harddisk1    VG01,dev01
- -      -         -                    -           -    -            VG01,dev01
D DB2    DATAFILE  E:\SQL\data2.mdf     E:          -    Harddisk2    VG02,dev02
- -      -         -                    -           -    -            VG02,dev02
T DB2    TRANSACT  E:\SQL\tlog2.ldf     E:          -    Harddisk2    VG02,dev02
- -      -         -                    -           -    -            VG02,dev02
```

- The following command outputs information, in the long format, about the database **SQL1**:

```
PROMPT> drmsqldisplay SQL1 -l
INSTANCE: SQL1
T DB  OBJECT    FILE             FS FSTYPE  DG  LVM-DEVICE
DEVICE    COPY-GROUP   PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
D DB1 DATAFILE  D:\SQL\data1.mdf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk1 VG01,dev01   CLI-A  2
10   0   10000 P   15044
- -   -         -                -  -       -   -
-         VG01,dev01   CLI-A  2    20   0   10020 S   15044
D DB1 DATAFILE  D:\SQL\data2,mdf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk1 VG01,dev01   CLI-A  2
10   0   10000 P   15044
- -   -         -                -  -       -   -
-         VG01,dev01   CLI-A  2    20   0   10020 S   15044
T DB1 TRANSACT  D:\SQL\tlog1.ldf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk1 VG01,dev01   CLI-A  2
10   0   10000 P   15044
- -   -         -                -  -       -   -
-         VG01,dev01   CLI-A  2    20   0   10020 S   15044
T DB1 TRANSACT  D:\SQL\tlog2.ldf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk1 VG01,dev01   CLI-A  2
10   0   10000 P   15044
- -   -         -                -  -       -   -
-         VG01,dev01   CLI-A  2    20   0   10020 S   15044
D DB2 DATAFILE  E:\SQL\data1.mdf E: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk1 VG02,dev01   CLI-A  2
11   0   10001 P   15044
- -   -         -                -  -       -   -
-         VG02,dev01   CLI-A  2    21   0   10021 S   15044
D DB2 DATAFILE  E:\SQL\data2.mdf E: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk1 VG02,dev01   CLI-A  2
11   0   10001 P   15044
- -   -         -                -  -       -   -
-         VG02,dev01   CLI-A  2    21   0   10021 S   15044
T DB2 TRANSACT  E:\SQL\tlog1.ldf E: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk1 VG02,dev01   CLI-A  2
11   0   10001 P   15044
- -   -         -                -  -       -   -
-         VG02,dev01   CLI-A  2    21   0   10021 S   15044
T DB2 TRANSACT  E:\SQL\tlog2.ldf E: NTFS    -
```

```
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk1 VG02,dev01   CLI-A  2
11   0   10001 P   15044
- -   -         -                -  -       -   -
-         VG02,dev01   CLI-A  2    21   0   10021 S   15044
```

- The following command only outputs information, in the long format, about the data file specified with the instance **SQL1**:

```
PROMPT> drmsqldisplay SQL1 -l -transact_log
INSTANCE: SQL1
T DB  OBJECT    FILE             FS FSTYPE  DG  LVM-DEVICE
DEVICE    COPY-GROUP   PORT#  TID# LUN# MU# LDEV# P/S SERIAL#
T DB1 TRANSACT  D:\SQL\tlog1.ldf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk1 VG01,dev01   CLI-A  2
10   0   10000 P   15044
- -   -         -                -  -       -   -
-         VG01,dev01   CLI-A  2    20   0   10020 S   15044
T DB1 TRANSACT  D:\SQL\tlog2.ldf D: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk1 VG01,dev01   CLI-A  2
10   0   10000 P   15044
- -   -         -                -  -       -   -
-         VG01,dev01   CLI-A  2    20   0   10020 S   15044
T DB2 TRANSACT  E:\SQL\tlog1.ldf E: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk1 VG02,dev01   CLI-A  2
11   0   10001 P   15044
- -   -         -                -  -       -   -
-         VG02,dev01   CLI-A  2    21   0   10021 S   15044
T DB2 TRANSACT  E:\SQL\tlog2.ldf E: NTFS    -
\\?\Volume{df67a5b0-5583-11d5-a410-806d6172696f}\  Harddisk1 VG02,dev01   CLI-A  2
11   0   10001 P   15044
- -   -         -                -  -       -   -
-         VG02,dev01   CLI-A  2    21   0   10021 S   15044
```

- The following command outputs information about the SQL Server database specified by the instance **SQL1** and management information for the dictionary map file:

```
PROMPT> drmsqldisplay SQL1 -v
VIRTUAL-SERVERNAME: host1
DB-PATH: D:\Program Files\Hitachi\DRM\db2
INSTANCE: SQL1
CORE-MAPFILE-UPDATE-TIME: 2002/06/01 10:00:00
APP.-MAPFILE-UPDATE-TIME: 2002/06/01 10:00:00
T DB   OBJECT    FILE              FS  DG  DEVICE     COPY-GROUP
D DB1  DATAFILE  D:\SQL\data1.mdf  D:  -   Harddisk1  VG01,dev01
- -    -         -                 -   -   -          VG01,dev01
T DB1  TRANSACT  D:\SQL\tlog1.ldf  D:  -   Harddisk1  VG01,dev01
- -    -         -                 -   -   -          VG01,dev01
D DB2  DATAFILE  E:\SQL\data2.mdf  E:  -   Harddisk2  VG02,dev02
- -    -         -                 -   -   -          VG02,dev02
T DB2  TRANSACT  E:\SQL\tlog2.ldf  E:  -   Harddisk2  VG02,dev02
- -    -         -                 -   -   -          VG02,dev02
```

- The following command outputs information about the SQL Server database specified by the instance **SQL1** and management information for the dictionary map file (when the dictionary map file does not exist):

```
PROMPT> drmsqldisplay SQL1 -v
VIRTUAL-SERVERNAME: host1
DB-PATH: D:\Program Files\Hitachi\DRM\db2
KAVX0039-E The core map file(s) cannot be found.
```

### 6.5.4 drmsqlinit (register parameters for SQL Server)

**Format:**

To register parameters for SQL Server:
`drmsqlinit` *`instance-name`*

To display the parameters registered for SQL Server:
`drmsqlinit -v` *`instance-name`*

**Description:**

The **drmsqlinit** command provides an interactive interface that lets you register the SQL Server parameters necessary to back up a SQL Server database. You can register parameters for each instance. This command registers the following information.

**Table 6.16 Parameters for the SQL Server**

| Setting | Description |
|---|---|
| VDI metafile storage directory (required) | Use an absolute path to specify the name of the directory for storing a VDI metafile. An existing directory must be specified. Specify an upper case character for the drive letter. |
| VDI generation timeout interval (in seconds) (required) | The timeout interval in seconds, used when a VDI metafile is generated. |
| Undo file storage directory (required) | Use an absolute path to specify the name of the directory for storing an undo file. An existing directory must be specified. |
| Backup file (for transaction logs) storage directory (required) | Specify the backup destination for the transaction log file backed up with the drmsqllogbackup command. Use an absolute path to specify the directory name. Specify a location other than a primary volume containing databases and a secondary volume containing databases. |

Directories in which SQL Server schema definition files (with parameters registered as **instance-name.dat**) are stored cannot be specified as storage directories for VDI metafiles or undo files.

The parameters that this command registers are stored in the following location:

***Protection-Services-installation-directory*\conf\MSSQL*instance-name*.dat**

To delete instances that have registered parameters, delete ***name-of-instance-to-be-deleted*.dat**.

**Arguments:**

**-v**

Displays the registered parameters.

***instance-name***

Specify the name of the SQL Server instance to be backed up. If the instance to be backed up is the default (**MSSQLSERVER**), specify **DEFAULT**.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples:**

- The following command sets up the instance **SQL1**:

```
PROMPT> drmsqlinit SQL1
KAVX1100-I Enter the name of the storage directory for VDI metafiles:
D:\MSSQL\Meta
KAVX1101-I Enter the timeout interval for VDI generation (in seconds, between 0
and 3600): 10
KAVX1102-I Enter the name of the storage directory for undo files: D:\MSSQL\Undo
KAVX1107-I Enter the name of the storage directory for the backup-log files:
D:\MSSQL\tlog
KAVX1103-I SQL Server information has been updated.
PROMPT>
```

- The following command displays the **SQL1** parameters:

```
PROMPT> drmsqlinit -v SQL1
Meta directory name: D:\MSSQL\Meta
VDI timeout sec (0 - 3600): 10
Undo file directory name: D:\MSSQL\Undo
SQL Server backup-log directory name: D:\MSSQL\Log
PROMPT>
```

### 6.5.5 drmsqllogbackup (back up the transaction log of a SQL Server)

**Format:**

To specify the instance and back up the transaction log:

```
drmsqllogbackup instance-name
              [ -target database-name | -f target-definition-file-name ]
```

To specify the backup ID and back up transaction log file backups:

```
drmsqllogbackup backup-ID
```

To specify the instance and view a list of transaction log file backups:

```
drmsqllogbackup instance-name -v
        [ BACKUP-ID | [ -target database-name | -f target-definition-file-name ] ]
```

To specify the backup ID and view a list of transaction log file backups:

```
drmsqllogbackup backup-ID -v
              [ -target database-name | -f target-definition-file-name ]
              [ -s log-backup-ID ] [ -e log-backup-ID ]
```

To delete transaction log file backups:

```
drmsqllogbackup backup-ID -d
              [ -s log-backup-ID ] [ -e log-backup-ID ]
```

**Description:**

Use the **drmsqlbackup** command to back up the transaction log file of a backed-up SQL server database. Use the **drmsqlinit** command to set the directory to which this file is to be backed up. The backup file of the transaction log file will be named as follows:

***database-name_yyyymmddhhmmss_log-backup-ID*.bk**

This backup ID is used to identify the number of times that the transaction log file has been backed up, for the backup data specified by the backup ID. This value is expressed as a four-digit number in decimal format (for example, **0001** or **1000**).

The preconditions to execute this command are as follows:

- The backup catalog acquired by the **drmsqlbackup** command exists.
- The instance to be backed up is running.
- The contents of the transaction log have not been destroyed.
- The recovery model of the database is **Full** or **Bulk_Logged**. (The recovery model Simple of the database is not included.)

**Notes:**

- When the log backup is acquired by Enterprise Manager provided by SQL Server, the log chain breaks and this command cannot be used. Do not truncate the log manually.
- This command cannot be applied to the system databases (**master**, **msdb**, **model**, **tempdb**, and **distribution**).
- Once a database has been restored, the log backup for different recovery paths are mixed and displayed.

**Arguments:**

***instance-name***

Specify the name of the SQL Server instance to be backed up. If the SQL Server to be backed up is the default instance **MSSQLSERVER**, specify **DEFAULT**.

**-v**

Specify this option to display a list of the transaction log files that were backed up. Information on the backups of the transaction log files acquired after the specified backup ID will be displayed. You can take the information displayed by this option, and use it as a transaction log target definition file.

**BACKUP-ID**

Specify **BACKUP-ID** to display the backup IDs of the backups for the specified instance. Specify the latest backup ID.

When the backup catalog that you want to specify is deleted and you cannot specify the backup ID, you can specify an original ID. Add **0:** before the original ID and specify the command arguments as well as the backup ID. The following shows the examples:

- The following command views information on the backups of the transaction log backup files with original ID 0000000001
  ```
  PROMPT> drmsqllogbackup O:0000000001 -v
  ```
- The following command deletes information on the backups of the transaction log backup files with original ID 0000000001
  ```
  PROMPT> drmsqllogbackup O:0000000001 -d
  ```

**-target** ***database-name(s)***

Specify this to display information about the database of the instance specified by ***instance-name***. To display information about multiple databases, separate the name of each database with a comma. If you specify a database name containing a space character, enclose the database name in double quotations ".

**-f** ***target-definition-file-name***

Specify this to display information about the database of the instance specified by ***instance-name***. Unlike the **-target** option, you can use this option to view information about multiple files with one setting, so long as those files are already contained in a configuration file. Make sure that you specify the path of this configuration file as an absolute path. If you specify a target definition file name containing a space character, enclose the target definition file name in double quotations ".

***backup-ID***

When deleting or displaying a transaction log backup file, use this option to specify its backup ID.

**-d**

Specify this option to delete the backups of the acquired transaction log files.

**-s** ***log-backup-ID***

Specify this option to set the start of the range of the transaction log backup files to be deleted or displayed. Use this option together with the **-e** option to specify the start and end of this range. Specifying the **-s** option alone sets the range from the backup ID that was specified with the **-s** option to the last log backup ID.

**-e** ***log-backup-ID***

Specify this option to set the end of the range of the transaction log backup files to be deleted or displayed. Use this option with the **-s** option to specify the start and end of this range. Specifying the **-e** option alone sets the range from the first log backup ID to the log backup ID specified with the **-e** option.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (a message indicating abnormal termination is output to the standard output).

**Examples:**

- The following command backs up the transaction log file of the instance **DEFAULT**:
```
PROMPT> drmsqllogbackup DEFAULT
```

- The following command displays information on the backups of the transaction log backup files with backup ID **0000000020** and with a log backup ID between **0001** and **0003**:
```
PROMPT> drmsqllogbackup 0000000020 -v -s 0001 -e 0003
[userDB1]
C:\LogBackup\userDB1_20021106010101_0001.bk
C:\LogBackup\userDB1_20021106050101_0002.bk
C:\LogBackup\userDB1_20021106090101_0003.bk
[userDB2]
C:\LogBackup\userDB2_20021106010101_0001.bk
C:\LogBackup\userDB2_20021106050101_0002.bk
C:\LogBackup\userDB2_20021106090101_0003.bk
```

- The following command deletes the backups of the transaction log backup files with backup ID **0000000020** and with a log backup ID between **0001** and **0003**:
```
PROMPT> drmsqllogbackup 0000000021 -d -s 0001 -e 0003
```

- The following command displays information on the backups of the transaction log backup files when two databases in the instance default have been backed up at different times with different backup IDs.

  Creating a transaction log target definition file:

  Backup ID for the database **userDB1**: **0000000002**

  Backup ID for the database **userDB2**: **0000000003**
```
PROMPT> drmsqllogbackup DEFAULT -v
# ORIGINAL-ID:0000000002 BACKUP-ID:0000000002 --> This line is handled as a
comment line.
[userDB1]
C:\LogBackup\userDB1_20021106010101_0001.bk
C:\LogBackup\userDB1_20021106050101_0002.bk
C:\LogBackup\userDB1_20021106090101_0003.bk
# ORIGINAL-ID:0000000003 BACKUP-ID:0000000003 -> This line is handled as a comment
line.
[userDB2]
C:\LogBackup\userDB2_20021106010101_0001.bk
C:\LogBackup\userDB2_20021106050101_0002.bk
C:\LogBackup\userDB2_20021106090101_0003.bk
PROMPT>
```

  The following command lists information for the backup IDs for the instance:
```
PROMPT> drmsqllogbackup DEFAULT -v BACKUP-ID
ORIGINAL-ID BACKUP-ID DB
0000000002 0000000002 userDB1
0000000003 0000000003 userDB2
PROMPT>
```

- The following command lists information for the backup IDs when multiple databases have been backed up at one time for the instance **default**.

```
PROMPT> drmsqllogbackup DEFAULT -v BACKUP-ID
ORIGINAL-ID BACKUP-ID DB
0000000002 0000000002 userDB1,userDB2 --> Displays comma-separated information.
0000000003 0000000003 userDB2
PROMPT>
```

### 6.5.6 drmsqlrecover (recover restored SQL Server databases)

**Format:**

```
drmsqlrecover instance-name
              [ -target database-name | -f target-definition-file-name ]
              [ -transact_log_list
              name-of-target-definition-file-for-transaction-logs ]
              [ -undo ]
```

**Description:**

The **drmsqlrestore** command recovers databases that have been restored. This command applies transaction logs that are specified in a target definition file for transaction logs or acquired during backup, and performs roll-forward recovery processing.

During command execution, from another computer such as an application server, you should not connect to the database that was restored. If another server connects to the database during command execution, the command might fail.

**Arguments:**

***instance-name***

Specify the database instance to be recovered. If the instance to be recovered is the default (**MSSQLSERVER**), specify **DEFAULT**.

**-target *database-name(s)***

Specify this option to recover specific databases. When specifying multiple databases to be recovered, use a comma to separate each database name. If you specify a database name containing a space character, enclose the database name in double quotations ".

When both this option and the **-f** option are omitted, the entire instance will be recovered.

**-f *target-definition-file-name***

Like the **-target** option, this option restores specific databases during recovery. Unlike the **-target** option, this option lets you specify a target definition file that collectively specifies all the databases to be restored. The target definition file containing the list of databases must be created before you attempt to use this option. Use an absolute path name to specify the target definition file. If you specify a target definition file name containing a space character, enclose the target definition file name in double quotations ".

Make sure that you specify databases that exist in the instance specified by this option. If you specify databases in separate instances, those databases will not be recovered.

**-transact_log_list** ***name-of-target-definition-file-for-transaction-logs***

Specify the order of the transaction log files to be applied during recovery. The order of these transaction log files is listed in the target definition file. Make sure that you use an absolute path when specifying the file name. If you specify a target definition file name containing a space character, enclose the target definition file name in double quotations ".

The log to be applied differs, depending on the user operation. Confirm the backup log by using the **drmsqllogbackup** command, and then select the log to be applied.

If this option is omitted, recovery processing by roll-forward is not performed, since the transaction log is not applied. Therefore, the database will return to the latest backup status.

**-undo**

Specifies that the database should be put in standby mode, accessed as read-only, after recovery. Temporary files will be created for each database in the undo file storage directory specified by the **drmsqlinit** command.

If this option is omitted, full access to the database will be available once recovery completes.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples:**

- The following command recovers the entire database identified by **SQLIns**:
```
PROMPT> drmsqlrecover SQLIns
```
- The following command recovers only the database **DB01** from within the instance identified by **SQLIns**:
```
PROMPT> drmsqlrecover SQLIns -target DB01
```

### 6.5.7 drmsqlrecovertool (recover restored SQL Server DB through a GUI)

**Format:**

```
drmsqlrecovertool instance-name
```

**Description:**

The **drmsqlrecovertool** command uses a GUI to recover an SQL Server database that has been restored by the **drmsqlrestore** command.

**Arguments:**

***instance-name***

Specify the name of the database instance to be recovered. If the SQL Server instance to be recovered is the existing instance (**MSSQLSERVER**), specify **DEFAULT**.

**GUI description:**

The following describes the **drmsqlrecovertool** dialog box (see Figure 6.1) that is activated when the **drmsqlrecovertool** command is executed.

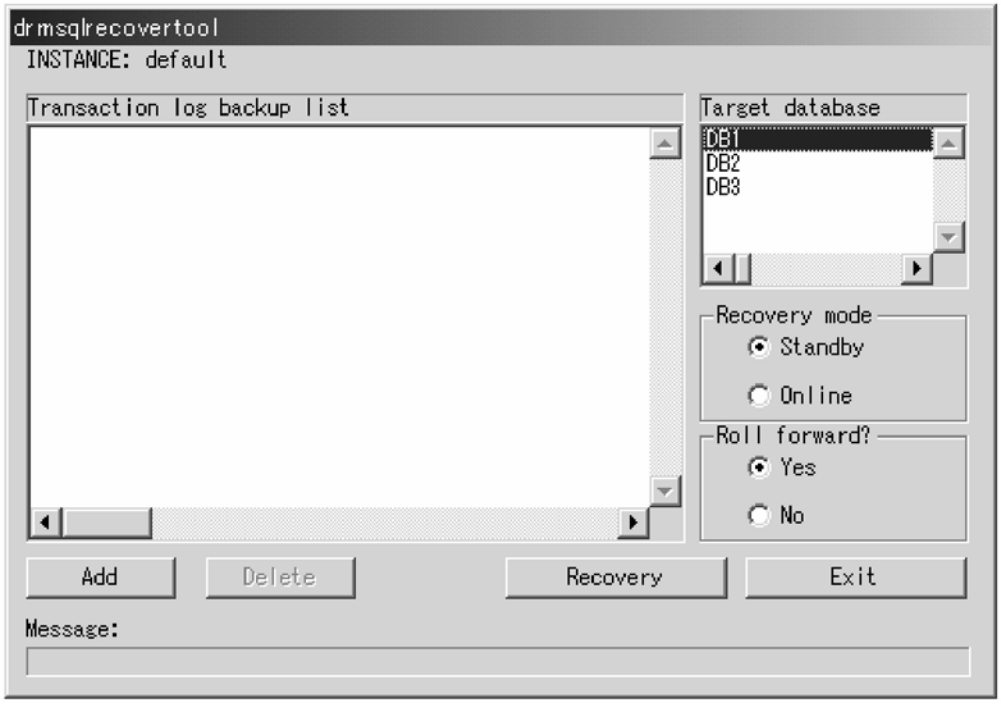



**Figure 6.1 drmsqlrecovertool Dialog Box**

**INSTANCE**

Displays the instance name specified for the **drmsqlrecovertool** command. The command will recover this instance. To change the instance, close the **drmsqlrecovertool** dialog box, and then re-execute the **drmsqlrecovertool** command.

**Transaction log backup list**

Displays a list of transaction log backup files that apply to the database selected in **Target database**. Use the **Add** button to add a file to this list. Use the **Delete** button to delete a file. The files shown in **Transaction log backup list** are sorted each time a new file is added.

A transaction log backup file is displayed in the following format:

**[*]** ***file-name creation-date-and-time*** **(*yyyy/mm/dd hh:mm:ss* format)** ***size*** **(bytes)**

An asterisk (*****) is added at the beginning of the recovered file.

**Target database**

Displays the database for the instance specified for the **drmsqlrecovertool** command. Select the database to which the transaction log backup files apply. You cannot select more than one database.

**Recovery mode**

Select the state of the database after the recovery.

**Standby**: Use the database in the read-only mode.
**Online** : Use the database in the read and write mode.

**Roll forward?**

Select whether or not to perform a roll-forward during recovery.

**Add button**

Choose this button to add a transaction log file to apply. This button adds the selected file to the files selected in **Transaction log backup list**. The files are sorted by name (except file extensions and path names) and added.

You cannot add the following files:

- Network files (files whose path begins with \\)
- Files that already exist in **Transaction log backup list**

**Delete button**

Choose this button to delete a transaction log backup file selected in **Transaction log backup list**. You can select multiple backup files. All the selected files are deleted.

**Recovery button**

Choose this button to perform the roll-forward recovery on the database. Of the transaction log backup files shown in **Transaction log backup list**, the files without an asterisk (*****) will be performed the roll-forward recovery to the database selected in **Target database**, beginning from the top file. The roll-forward recovery is not performed on the files when **No** is selected for **Roll forward?**.

When the recovery finishes, an asterisk (*****) is added to the beginning of all the file names in Transaction log backup list. If a recovery error occurs, the result is output to the message dialog box or **drm_output.log**.

**EXIT button**

Closes the **drmsqlrecovertool** dialog box.

**Message**

Displays the progress of the command execution.

**Return values:**

**0**: All the databases are recovered.

**Other than 0**: Some databases remain unprocessed.

**Example:**

- The following command recovers the transaction log to the database for the instance **SQLIns**:

```
PROMPT> drmsqlrecovertool SQLIns
```

### 6.5.8 drmsqlrestore (restore SQL Server DBs from backups to a primary vol.)

**Format:**

To restore data by disk resynchronization:

```
drmsqlrestore backup-ID -resync [ -force ][ -undo ][ -nochk_host ]
                        [ -target database-name | -f target-definition-file-name ]
```

To apply only the metafile to the primary volume:

```
drmsqlrestore backup-ID -no_resync [ -undo ][ -nochk_host ]
                        [ -target database-name | -f target-definition-file-name ]
```

**Description:**

The **drmsqlrestore** command lets you use the backup data specified by the backup ID to restore data from the secondary volume to the primary volume by disk resynchronization. The snapshot metafile created by the **drmsqlbackup** command is used for restoration processing.

The following explains the operation of this command for restoration by disk resynchronization:

1. If the restored database was attached, the database will be detached. If the detachment of the database fails, an error message will be displayed, and restoration processing will terminate abnormally.
2. The backup data will be restored from the secondary volume to the primary volume by disk resynchronization.
3. The database will be attached.
4. The instance will be started.

The following explains the command processing for restoration in a cluster configuration. The database to be restored cannot be used temporarily since the cluster resource containing the database is placed offline.

1. The command places the cluster resource containing the database and the disk resource offline when the cluster resource containing the database to be restored is placed online.

   If operations to place the cluster resource containing databases and disk resource offline fail, the command displays an error message and the restoration processing fails.
2. The command performs disk resynchronization to restore the backup data from a secondary volume to the primary volume.
3. The command places the disk resource online and then the cluster resource online.

In restoration, data on the primary volume is overwritten by the disk image of the secondary volume at the time backup is performed. Therefore, data on the primary volume that was created or updated after the backup is invalid.

When you attempt to restore the system database for SQL server, the SQL server service to be restored needs to be stopped to recover the system database. The database to be restored cannot be accessed temporarily.

During command execution, from another computer such as an application server, you should not connect to the database that was restored. If another server connects to the database during command execution, the command might fail.

When you execute this command on the copy group in the paired status (**PAIR**), the status of the copy group is changed to **PSUS**.

When the pair status of the copy group is **COPY**, **SMPL**, or **PSUE**, the **drmsqlrestore** command might fail. Before executing this command, check the pair status of the copy group by using the CCI **pairdisplay** or **pairevtwait** command.

When you execute this command to perform restoration, if the name of the drive making up the SQL Server database has been changed since backup was performed, the command fails. Before performing restoration, with the **drmsqlcat** command or SQL Server Enterprise Manager, check the corresponding drive name of the restoration destination.

**Arguments:**

***backup-ID***

Specify the backup ID of the backup data to be restored. A backup ID, which is used to uniquely identify backup data, is registered in the backup catalog during backup. To check a backup ID, execute the **drmsqlcat** command.

**-resync**

Specifies that the primary and secondary volumes should be restored by disk resynchronization. Backup data on the secondary volume is synchronized to the primary volume.

When you execute the command with this option, stop the service of the program viewing the Windows performance registry.

**-force**

Specify this option to perform restoration by forced resynchronization of the primary and secondary volumes.

With this option, perform forced resynchronization if the copy group name of the primary volume obtained when the backup processing was performed on the database server corresponds with the information on the database server, even though the LDEV number and the SERIAL number do not correspond with the LDEV number and the SERIAL number when the backup processing was performed. Specify this option only if restoration by resynchronization could not be performed with the **-resync** option, such as when the LDEV number changes when the volume is replaced. If this option is specified under a normal restoration, data might be corrupted.

**-undo**

Specifies that the database should be restored in standby mode. When this option is specified, the database can be used as read-only once the restoration has finished. Temporary files will be created for each database in the undo file storage directory registered by the **drmsqlinit** command.

When this option is omitted, a regular restoration is performed. In this case, the database will be placed in loading status once the restoration has finished, and will not be usable.

**-nochk_host**

Specify this option to restore the data to a host that differs from the one specified for the **drmsqlbackup** command. This option is useful when the host name has been changed or the log-shipping functionality in Microsoft SQL Server 2000 Enterprise Edition is used.

***Note:*** When you specify the **-nochk_host** option, confirm that backup data is restored on the appropriate host, because the validity of the host name in the backup catalog is not checked when restoring backup data.

**-target** ***database-name(s)***

Restores an instance containing specific databases. The specified database needs to exist in the backup catalog specified by the backup ID. When databases that do not exist in the backup catalog are specified, those databases will not be restored. When specifying multiple databases to be restored at a time, use a comma to separate each database name. If you specify a database name containing a space character, enclose the database name in double quotations ".

When both this option and the **-f** option are omitted, the entire instance specified by the backup ID will be restored.

**-f** ***target-definition-file-name***

Like the **-target** option, this option restores an instance containing specific databases. Unlike the **-target** option, this option lets you specify a target definition file that collectively specifies all the databases to be restored. The target definition file containing the list of databases must be created before you attempt to use this option. Use an absolute path name to specify the target definition file. If you specify a target definition file name containing a space character, enclose the target definition file name in double quotations ".

When both this option and the **-target** option are omitted, all the objects included in the instance specified by the backup ID will be restored.

**-no_resync**

Specify this option if you want to apply only the metafiles for the data on the primary volume, without performing restoration processing or backing up data from the secondary volume to the primary volume. Use this option when the restore operation cannot be performed with the **drmsqlrestore** command (for example, when restoring backup data directly from the tape to the primary volume because of a disk failure).

**Notes:**

- When you specify this command on the SQL Server database whose name has been changed, make sure that the SQL Server database to be restored is detached. If the SQL Server database is restored without detach processing, the command fails and the SQL Server database might not be able to be used after restoration.
- The backup information in the backup catalog is managed based on the copy group used as a key. Depending on the backup method, you might not be able to perform restoration, even though the backup data exists on the secondary volume.

  The example is described below using the two databases, which are located on separate volumes:

  - Database A (copy group: **VG01,sql01**)
  - Database B (copy group: **VG01,sql01**)

  Use the following backup method to back up the databases:

  1. Back up database A and database B concurrently. Backup ID **0000000001** is created.
  2. Back up database A only. The backup ID **0000000002** is created.

When you use backup method 2, the backup ID **0000000002** is created, and the old backup information (backup ID: **0000000001**) about copy group **VG01,sql01** on database A is deleted from the backup catalog. In other words, since the backup information about database B, which is included in backup ID **0000000001**, is also deleted from the backup catalog, database B cannot be restored even though the backup data exists in the secondary volume. When you restore database B, restore the backup data obtained by using backup method 1 from tape to the secondary volume, and then restore the backup data from the secondary volume to the primary volume.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Example:**

- The following command restores, by disk resynchronization, the backup data identified by the backup ID **0000000001**:

```
PROMPT> drmsqlrestore 0000000001 -resync
```

## 6.6 Exchange Server Command Specifications

### 6.6.1 drmexgbackup (back up a storage group to a secondary volume)

**Format:**

To perform a cold backup:

```
drmexgbackup [-mode cold]
             [ -target storage-group-name | -f target-definition-file-name ]
             [ -transact_log_del ] [ -c { offline | online }]
```

To perform an online backup:

```
drmexgbackup -mode online
             [ -target storage-group-name | -f target-definition-file-name ]
```

**Description:**

The **drmexgbackup** command backs up the storage group of a primary volume to a secondary volume. If Exchange 2000 Server or Exchange 2003 Standard Edition is used, the command backs up the entire database. If Exchange 2000 Enterprise Server or Exchange 2003 Enterprise Edition is used, the command backs up the entire database, or in units of storage groups.

Before you execute the **drmexgbackup** command, make sure that the database files and log files are stored in separate copy groups.

Before this command is executed, the system cache of the secondary volume must be cleared. Mount or unmount the secondary volume on the backup server to clear the system cache.

**Arguments:**

**-mode cold**

Specify this option to perform a cold backup. Since the cold backup dismounts the Information Store to be backed up, this Information Store cannot be accessed until the backup finishes.

**-mode online**

Specify this option to perform an online backup. Unlike a cold backup, this option performs a backup without performing the following:

- Mount and unmount the Information Store.
- Switch the cluster resource (online and offline) in a cluster environment
- Mount and unmount the disk drive.

After performing a backup with this option, use the **drmexgverify** command to verify the integrity of the backup data. You must also specify the **-recovery** option to restore the data.

***Note:*** The online backup forcibly copies the target data from the primary volume to the secondary volume without dismounting the Information Store. Microsoft does not guarantee this backup method for Exchange Servers. It may be impossible to restore the backup data acquired by this function. To ensure restoration of the backup data, first use the **drmexgbackup** command to perform a cold backup. Then, make sure that the backup data is stored, and then perform an online backup.

**-target** ***storage-group-name(s)***

Specify this option to back up the database resource containing the specific storage group. However, the minimum unit for backup is a physical volume. If a single physical volume contains multiple storage groups, specify all the storage groups. If you specify only some of the storage groups, the command encounters an error.

When specifying multiple storage groups to be backed up, use a comma (,) to separate each storage group name. Use double quotation marks (") to enclose all storage group names that contain at least one space character.

If this option is omitted, all storage groups on the server will be backed up.

This option is only effective for Exchange 2000 Enterprise Server and Exchange 2003 Enterprise Edition. For any other Exchange Server, this option is invalid.

**-f** ***target-definition-file-name***

Like the **-target** option, this option performs a backup related to specific storage groups. Make sure that you specify this option or the **-target** option when multiple storage group information data files exist on one physical volume.

Unlike the **-target** option, however, the **-f** option lets you specify a target definition file that collectively specifies all the storage groups for which backup is to be performed. The target definition file containing the list of storage groups must be created before you use this option. Use an absolute path name to specify the target definition file.

This option is only effective for Exchange 2000 Enterprise Server and Exchange 2003 Enterprise Edition. For any other Exchange Server, this option is invalid.

**-transact_log_del**

Specify this option to delete the committed transaction log files.

When this command is executed, the transaction log file is deleted. This means that you will no longer be able to use the **-recovery** option to perform restoration from backups already performed.

This option is not valid when wrap-around logs are being used. For more information about wrap-around logs, see the Exchange 2000 Server manual.

**-c { offline | online }**

In a cluster environment, specify **-c offline** to perform offline backup of the cluster resources of a physical disk. To perform backup while online, specify **-c online**. The default for this option is **-c offline**.

Specify **-c online** together with the **-target** or **-f** option when you want to execute this command. A storage group that is not to be backed up might be dismounted when you specify **-c offline**.

This option is not valid for environments other than cluster environments.

**Notes:**

- Make sure that another volume is not mounted on the directory of the volume to be backed up when performing an online backup.
- The backup information in the backup catalog is managed based on the copy group used as a key. Depending on the backup method, you might not be able to perform restoration, even though the backup data exists on the secondary volume.

  The example described below uses two storage groups located on separate volumes:

  – Storage group A (copy group: **VG01,exg01**)

  – Storage group B (copy group: **VG01,exg02**)

  Use the following backup method to back up the storage groups:

  1. Back up storage group A and storage group B concurrently. The backup ID **0000000001** is created.
  2. Back up storage group A only. The backup ID **0000000002** is created.

  When you use backup method 2, backup ID **0000000002** is created, and the old backup information (backup ID: **0000000001**) about copy group **VG01,exg01** on storage group A is deleted from the backup catalog. In other words, since the backup information about storage group B, which is included in backup ID **0000000001**, is also deleted from the backup catalog, the file system B cannot be restored even though the backup data exists in the secondary volume. When you restore storage group B, restore the backup data obtained by using backup method 1 from tape to the secondary volume, and then restore the backup data from the secondary volume to the primary volume.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples:**

The following command performs an online backup for the entire database on the specific Exchange Server:

```
PROMPT> drmexgbackup
KAVX0001-I The drmexgbackup command will now start.
KAVX1600-I Backup processing will now start.
KAVX0040-I The backup ID has been assigned as follows.
backup-ID = 0000000001
KAVX1601-I Backup processing has finished.
KAVX0002-I The drmexgbackup command will now end.
```

The following command performs a cold backup for the storage group **STR1**:

```
PROMPT> drmexgbackup -target STR1 -mode cold
KAVX0001-I The drmexgbackup command will now start.
KAVX1805-I The information store will now be dismounted.
             Storage group name = STR1
KAVX1600-I Backup processing will now start.
KAVX0040-I The backup ID has been assigned as follows.
             Backup ID = 0000000001
KAVX1601-I Backup processing has finished.
KAVX1806-I The information store will now be mounted.
             Storage group name = STR1
KAVX0002-I The drmexgbackup command will now end.
```

The following command performs a cold backup for the storage groups specified in the target definition file **C:\temp\BACKUP_DB.txt**:

```
PROMPT> drmexgbackup -mode cold -f C:\temp\BACKUP_DB.txt
KAVX0001-I The drmexgbackup command will now start.
KAVX1805-I The information store will now be dismounted.
             Storage group name = STR1
KAVX1805-I The information store will now be dismounted.
             Storage group name = STR2
KAVX1805-I The information store will now be dismounted.
             Storage group name = STR3
KAVX1600-I Backup processing will now start.
KAVX0040-I The backup ID has been assigned as follows.
             Backup ID = 0000000001
KAVX1601-I Backup processing has finished.
KAVX1806-I The information store will now be mounted.
             Storage group name = STR1
KAVX1806-I The information store will now be mounted.
             Storage group name = STR2
KAVX1806-I The information store will now be mounted.
             Storage-group-name = STR3
KAVX0002-I The drmexgbackup command will now end.
```

### 6.6.2 drmexgcat (display backup information for a storage group)

**Format:**

```
drmexgcat [ -target storage-group-name | -f target-definition-file-name ]
          [ -transact_log ][ -datafile ][ -v ]
          [ -device device-file-name ][ -l ]
          [ -backup_id backup-ID ][ -hostname host-name ]
```

**Description:**

The **drmexgcat** command displays the backup information of the storage group on the server where the command is executed. Table 6.17 lists and describes the displayed items.

Each item is separated by a space. A hyphen (-) is displayed for any item that cannot be displayed. If none of the items can be displayed, an error message is displayed.

**Table 6.17 Items Displayed by the drmexgcat Command (continues on the next page)**

| Displayed Item | Description |
|---|---|
| STORAGEGROUP | Storage group name |
| BACKUP-ID | Backup ID |
| BACKUP-MODE | Backup mode |
| ORIGINAL-ID | Original backup ID obtained by the drmexgbackup command |
| START-TIME | Start time of backup |
| END-TIME | End time of backup |
| HOSTNAME | Name of the server where the snapshot backup was performed |

**Table 6.17 Items Displayed by the drmexgcat Command (continued)**

| Displayed Item | Description |
|---|---|
| T | Object type:<br>M: Mailbox store<br>P: Public folder store<br>T: Transaction log file<br>C: Checkpoint file |
| OBJECT | A type of Exchange Server object and its name:<br>MAILBOXSTORE: Mailbox store name<br>PUBLICSTORE: Public folder store name<br>TRANSACT: Transaction log file name<br>CHECKPOINT: Checkpoint file name |
| INFORMATIONSTORE | Information store name |
| FILE | File name |
| FS | Mount point directory name |
| FSTYPE | File system type (NTFS) |
| DG | A hyphen (-) is displayed. |
| LVM-DEVICE | A GUID is displayed. |
| DEVICE *1 | Harddiskn (where n is an integer) |
| COPY-GROUP | Copy group name, displayed as follows: CCI volume group name, paired volume name |
| PORT# | Port name on the host server |
| TID# | Target-ID on the host server |
| LUN# | Logical unit number on host server |
| MU# | Pair ID |
| LDEV# | Logical device number inside the RAID device |
| P/S | A letter identifying the primary or secondary volume:<br>P: Primary volume<br>S: Secondary volume |
| SERIAL# | Serial number inside the RAID device |
| VIRTUAL-SERVERNAME *2 | Virtual server name (value of the DRM_HOSTNAME environment variable) |
| DB-PATH *2 | Name of the directory storing the backup catalog |
| CATALOG-UPDATE-TIME *2 | Time when the backup catalog was created |

***Notes:***

1. When this command is executed with the **-device** option specified, this information will be displayed after **OBJECT**.
2. The command executed with the **-v** option displays this information.

**Arguments:**

**-target** ***storage-group-name(s)***

Specifies that information relating to certain storage groups is to be displayed. When specifying multiple storage groups to be displayed, use a comma to separate each group name. Use double quotation marks (") to enclose all storage group names that contain at least one space character.

If this option is omitted, information pertaining to all storage groups on the server on which the command was executed will be displayed or updated.

This option is only effective for Exchange 2000 Enterprise Server and Exchange 2003 Enterprise Edition. For any other Exchange Server, the command ignores this option and displays the backup information for the server on which the command was executed.

**-f** ***target-definition-file-name***

Specify this option to display information about specific storage groups. Unlike the **-target** option, this option lets you specify a target definition file that collectively specifies all the storage groups for which information is to be displayed. The target definition file containing the list of storage groups must be created before you attempt to use this option. Use an absolute path name to specify the target definition file.

This option is only effective for Exchange 2000 Enterprise Server and Exchange 2003 Enterprise Edition. For any other Exchange Server, the command ignores this option and displays the backup information for the server on which the command was executed.

**-transact_log**

Specifies that only information relating to the transaction log file is to be displayed. This option will display the following information:

- The name of the transaction log file
- File system information
- Logical volume structure information
- Physical disk information

When you specify this option with the **-target** option or **-f** option, only information pertaining to the transaction log of the specified storage group will be displayed when this option is specified. If either the **-target** or the **-f** option is omitted, information pertaining to all transaction logs of all storage groups will be displayed.

**-datafile**

Specifies that only information relating to the data file is to be displayed. This option will display the following information:

- The name of the data file
- File system information
- Logical volume structure information
- Physical disk information

When you specify this option with the **-target** option or **-f** option, only information pertaining to the data file of the specified storage group will be displayed when this option is specified. If either the **-target** or the **-f** option is omitted, information pertaining to all data files of all storage groups will be displayed.

**-v**

Specify this option to display management information for the backup catalog. The following information is displayed:

- Name of the directory storing the backup catalog: Displays the path that is set in **DRM_DB_PATH** in the environment setup file (**init.conf**). If **DRM_DB_PATH** has not been set, the product installation path appears.
- Virtual server name (value of the **DRM_HOSTNAME** environment variable): If the **DRM_HOSTNAME** environment variable has not been set, a hyphen (-) appears.
- Time when the backup catalog was created: For each backup ID, displays the time when the backup catalog was created.

**-device** ***device-file-name***

Specifies that only information relating to the device file is to be displayed. This option will display the following information:

- The name of the storage group
- File system information
- Physical disk information
- Logical volume information

**-l**

Specifies that storage group information is to be displayed in the long format.

**-backup_id** ***backup-ID***

Specify this argument when you want to display only the backup information of a specific backup ID. A backup ID uniquely identifies backup data and is registered in the backup catalog during the backup processing. To check a backup ID, execute the **drmexgcat** command.

**-hostname** ***host-name***

Specify this argument to display only information pertaining a specific host.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples:**

The following command outputs information about the Information Store specified in the storage group **STR1** that was backed up with the online backup mode:

```
PROMPT> drmexgcat -target STR1
STORAGEGROUP: STR1
BACKUP-ID:0000000001 BACKUP-MODE: ONLINE STORAGEGROUP: STR1 ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:01:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS          DG
DEVICE       COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.edb       D:          -
Harddisk1    VG01-dev01
- -             -                    -                       -           -       -
VG01-dev01
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.stm       D:          -
Harddisk1    VG01-dev01
- -             -                    -                       -           -       -
VG01-dev01
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.edb        D:          -
Harddisk1    VG01-dev01
- -             -                    -                       -           -       -
VG01-dev01
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.stm        D:          -
Harddisk1    VG01-dev01
- -             -                    -                       -           -       -
VG01-dev01
T TRANSACT     -                    E:\STR1\E00.log         E:          -
Harddisk2    VG01-dev02
- -             -                    -                       -           -       -
VG01-dev02
T TRANSACT     -                    E:\STR1\E000001.log     E:          -
Harddisk2    VG01-dev02
- -             -                    -                       -           -       -
VG01-dev02
T TRANSACT     -                    E:\STR1\E000002.log     E:          -
Harddisk2    VG01-dev02
- -             -                    -                       -           -       -
VG01-dev02
T TRANSACT     -                    E:\STR1\E000003.log     E:          -
Harddisk2    VG01-dev02
- -             -                    -                       -           -       -
VG01-dev02
C CHECKPOINT   -                    E:\STR1\E00.chk         E:          -
Harddisk2    VG01-dev02
- -             -                    -                       -           -       -
VG01-dev02
```

The following command outputs information, in the long format, about the Information Store specified in storage group **STR1**:

```
PROMPT> drmexgcat -target STR1 -l
STORAGEGROUP: STR1
BACKUP-ID:0000000001 BACKUP-MODE: COLD STORAGEGROUP: STR1 ORIGINAL-ID:0000000001
START-TIME:2002/06/01 10:00:00 END-TIME: 2002/06/01 10:01:00 HOSTNAME:EXG_SRV1
T OBJECT       INFORMATIONSTORE     FILE                    FS        FSTYPE    DG
LVM-DEVICE                                              DEVICE      COPY-GROUP   PORT#
TID# LUN# MU# LDEV# P/S SERIAL#
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.edb      D:        NTFS      -
\\?\Volume{2ef9993f-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev01   CLI-A
0    0    0   10000 P   15044
- -            -                     -                     -         -         -
-                                                        -          VG01-dev01   CLI-B
1    10   0   10010 S   15044
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.stm      D:        NTFS      -
\\?\Volume{2ef9993f-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev01   CLI-A
0    0    0   10000 P   15044
- -            -                     -                     -         -         -
-                                                        -          VG01-dev01   CLI-B
1    10   0   10010 S   15044
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.edb       D:        NTFS      -
\\?\Volume{2ef9993f-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev01   CLI-A
0    0    0   10000 P   15044
- -            -                     -                     -         -         -
-                                                        -          VG01-dev01   CLI-B
1    10   0   10010 S   15044
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.stm       D:        NTFS      -
\\?\Volume{2ef9993f-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev01   CLI-A
0    0    0   10000 P   15044
- -            -                     -                     -         -         -
-                                                        -          VG01-dev01   CLI-B
1    10   0   10010 S   15044
T TRANSACT     -                     E:\STR1\E00.log        E:        NTFS      -
\\?\Volume{2ef9993d-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev02   CLI-A
0    1    0   10001 P   15044
- -            -                     -                     -         -         -
-                                                        -          VG01-dev02   CLI-B
1    11   0   10011 S   15044
T TRANSACT     -                     E:\STR1\E000001.log    E:        NTFS      -
\\?\Volume{2ef9993d-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev02   CLI-A
0    1    0   10001 P   15044
- -            -                     -                     -         -         -
-                                                        -          VG01-dev02   CLI-B
1    11   0   10011 S   15044
T TRANSACT     -                     E:\STR1\E000002.log    E:        NTFS      -
\\?\Volume{2ef9993d-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev02   CLI-A
0    1    0   10001 P   15044
- -            -                     -                     -         -         -
-                                                        -          VG01-dev02   CLI-B
1    11   0   10011 S   15044
T TRANSACT     -                     E:\STR1\E000003.log    E:        NTFS      -
\\?\Volume{2ef9993d-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev02   CLI-A
0    1    0   10001 P   15044
- -            -                     -                     -         -         -
-                                                        -          VG01-dev02   CLI-B
1    11   0   10011 S   15044
C CHECKPOINT   -                     E:\STR1\E00.chk        E:        NTFS      -
\\?\Volume{2ef9993d-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev02   CLI-A
0    1    0   10001 P
```

### 6.6.3 drmexgdisplay (display or update information for storage groups)

**Format:**

To display the information for a storage group:

```
drmexgdisplay [ -target storage-group-name | -f target-definition-file-name ]
              [ -transact_log ][ -datafile ][ -v ]
              [ -device device-file-name ][ -l ]
```

To update the dictionary map file to the latest status:

```
drmexgdisplay [ storage-group-name ] -refresh
```

**Description:**

The **drmexgdisplay** command does the following:

1. Displays resource information for the storage groups on the server on which the command was executed.
2. Displays resource information for all of the optional storage groups on the server on which the command was executed.
3. Updates the storage group information in the dictionary map file. Execute this command before performing a backup.

The items displayed in (1) and (2) appear in the table below.

Each item is separated by a space. A hyphen (-) is displayed for any item that cannot be displayed. If none of the items can be displayed, an error message is displayed.

**Table 6.18 Items Displayed by the drmexgdisplay Command (continues on the next page)**

| Displayed Item | Description |
|---|---|
| STORAGEGROUP | Storage group name |
| T | Object type:<br>M: Mailbox store<br>P: Public folder store<br>T: Transaction log file<br>C: Checkpoint file |
| OBJECT | A type of Exchange Server object and its name:<br>MAILBOXSTORE: mailbox-store-name<br>PUBLICSTORE: public-folder-store-name<br>TRANSACT: transaction-log-file-name<br>CHECKPOINT: checkpoint-file-name |
| INFORMATIONSTORE | Information store name |
| FILE | File name |
| FS | Mount point directory name |
| FSTYPE | File system type (NTFS) |
| DG | A hyphen (-) is displayed. |
| LVM-DEVICE | A GUID is displayed. |

**Table 6.18 Items Displayed by the drmexgdisplay Command (continued)**

| Displayed Item | Description |
|---|---|
| DEVICE *1 | Harddiskn (where n is an integer) |
| COPY-GROUP | Copy group name, displayed as follows: CCI volume group name, paired volume name |
| PORT# | Port name on the host server |
| TID# | Target-ID on the host server |
| LUN# | Logical unit number on host server |
| MU# | Pair ID |
| LDEV# | Logical device number inside the RAID device |
| P/S | A letter identifying the primary or secondary volume<br>P: Primary volume<br>S: Secondary volume<br>-: A volume that is not part of a pair |
| SERIAL# | Serial number inside the RAID device |
| VIRTUAL-SERVERNAME *2 | Virtual server name (value of the DRM_HOSTNAME environment variable) |
| DB-PATH *2 | Name of the directory storing the dictionary map file |
| CORE-MAPFILE-UPDATE-TIME *2 | Update time for the core map file |
| APP.-MAPFILE-UPDATE-TIME *2 | Update time for the application map file |

***Notes:***

1. When this command is executed with the **-device** option specified, this information will be displayed after **OBJECT**.
2. The command executed with the **-v** option displays this information.

**Arguments:**

**-target** ***storage-group-name(s)***

Specifies that information relating to a certain storage group is to be displayed. When specifying multiple storage groups to be displayed, use a comma to separate each group name. Use double quotation marks (") to enclose all storage group names that contain at least one space character.

If this option is omitted, information pertaining to all storage groups on the server on which the command was executed will be displayed.

This option is only effective for Exchange 2000 Enterprise Server and Exchange 2003 Enterprise Edition. For any other Exchange Server, the command ignores this option and displays the backup information for the server on which the command was executed.

**-f** ***target-definition-file-name***

Specify this option to display information related to specific storage groups. Unlike the **-target** option, this option lets you specify a target definition file that collectively specifies all the storage groups for which information is to be displayed. The target definition file containing the list of storage groups must be created before you attempt to use this option. Use an absolute path to specify the target definition file.

This option is only effective for Exchange 2000 Enterprise Server and Exchange 2003 Enterprise Edition. For any other Exchange Server, the command ignores this option and displays the backup information for the server on which the command was executed.

**-transact_log**

Specifies that you want to display only information relating to the transaction logs. This option will display the following information:

- The name of the transaction log file
- File system information
- Logical volume structure information
- Physical disk information

When you specify this option with the **-target** option or **-f** option, only information pertaining to the transaction log of the specified storage group will be displayed when this option is specified. If either the **-target** or the **-f** option is omitted, information pertaining to all transaction logs of all storage groups will be displayed.

**-datafile**

Specifies that only information relating to the data file is be displayed. This option will display the following information:

- The name of the data file
- File system information
- Logical volume structure information
- Physical disk information

When you specify this option with the **-target** option or **-f** option, only information pertaining to the data file of the specified storage group will be displayed when this option is specified. If either the **-target** or the **-f** option is omitted, information pertaining to all data files of all storage groups will be displayed.

**-v**

Specify this option to display management information for the dictionary map file. The following information is displayed:

- Name of the directory storing the dictionary map file: Displays the path that is set in **DRM_DB_PATH** in the environment setup file (**init.conf**). If **DRM_DB_PATH** has not been set, the product installation path appears.
- Virtual server name (value of the **DRM_HOSTNAME** environment variable): If the **DRM_HOSTNAME** environment variable has not been set, a hyphen (-) appears.
- Update time for the dictionary map file: Displays the update time separately for the core map file and the application map file.

**-device** ***device-file-name***

Specifies that only information relating to the device file is to be displayed. This option will display the following information:

- The name of the storage group
- File system information
- Physical disk information
- Logical volume information

**-l**

Specifies that storage group information is to be displayed in the long format.

***storage-group-name***

If this argument is specified with the **-refresh** option, the information about the specified storage group is updated. If this option is omitted, the dictionary map file information about all storage groups is updated.

**-refresh**

Updates dictionary map file information.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples:**

The following command outputs information about the Information Store specified by the storage group **STR1** and management information for the dictionary map file:

```
PROMPT> drmexgdisplay -target STR1 -v
STORAGEGROUP: STR1
T OBJECT       INFORMATIONSTORE     FILE                  FS          DG      DEVICE
COPY-GROUP
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.edb     D:          -       Harddisk1
VG01-dev01
- -            -                    -                     -           -       -
VG01-dev01
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.stm     D:          -       Harddisk1
VG01-dev01
- -            -                    -                     -           -       -
VG01-dev01
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.edb      D:          -       Harddisk1
VG01-dev01
- -            -                    -                     -           -       -
VG01-dev01
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.stm      D:          -       Harddisk1
VG01-dev01
- -            -                    -                     -           -       -
VG01-dev01
T TRANSACT     -                    E:\STR1\E00.log       E:          -       Harddisk2
VG01-dev02
- -            -                    -                     -           -       -
VG01-dev02
T TRANSACT     -                    E:\STR1\E000001.log   E:          -       Harddisk2
VG01-dev02
- -            -                    -                     -           -       -
VG01-dev02
T TRANSACT     -                    E:\STR1\E000002.log   E:          -       Harddisk2
VG01-dev02
- -            -                    -                     -           -       -
VG01-dev02
T TRANSACT     -                    E:\STR1\E000003.log   E:          -       Harddisk2
VG01-dev02
- -            -                    -                     -           -       -
VG01-dev02
C CHECKPOINT   -                    E:\STR1\E00.chk       E:          -       Harddisk2
VG01-dev02
- -            -                    -                     -           -       -
VG01-dev02
```

The following command outputs information, in the long format, about the Information Store specified in the storage group **STR1**:

```
PROMPT> drmexgdisplay -target STR1 -l
STORAGEGROUP: STR1
T OBJECT       INFORMATIONSTORE     FILE                    FS        FSTYPE    DG
LVM-DEVICE                                              DEVICE      COPY-GROUP   PORT#  TID# LUN#
MU# LDEV# P/S SERIAL#
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.edb       D:        NTFS      -
\\?\Volume{2ef9993f-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev01   CLI-A  0    0    0
10000 P   15044
- -           -                     -                       -         -         -         -
-           VG01-dev01   CLI-B  1    10   0   10010 S   15044
M MAILBOXSTORE MAILBOX1(STR1)       D:\STR1\priv1.stm       D:        NTFS      -
\\?\Volume{2ef9993f-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev01   CLI-A  0    0    0
10000 P   15044
- -           -                     -                       -         -         -         -
-           VG01-dev01   CLI-B  1    10   0   10010 S   15044
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.edb        D:        NTFS      -
\\?\Volume{2ef9993f-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev01   CLI-A  0    0    0
10000 P   15044
- -           -                     -                       -         -         -         -
-           VG01-dev01   CLI-B  1    10   0   10010 S   15044
P PUBLICSTORE  PUBLIC1(STR1)        D:\STR1\pub1.stm        D:        NTFS      -
\\?\Volume{2ef9993f-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev01   CLI-A  0    0    0
10000 P   15044
- -           -                     -                       -         -         -         -
-           VG01-dev01   CLI-B  1    10   0   10010 S   15044
T TRANSACT     -                    E:\STR1\E00.log         E:        NTFS      -
\\?\Volume{2ef9993d-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev02   CLI-A  0    1    0
10001 P   15044
- -           -                     -                       -         -         -         -
-           VG01-dev02   CLI-B  1    11   0   10011 S   15044
T TRANSACT     -                    E:\STR1\E000001.log     E:        NTFS      -
\\?\Volume{2ef9993d-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev02   CLI-A  0    1    0
10001 P   15044
- -           -                     -                       -         -         -         -
-           VG01-dev02   CLI-B  1    11   0   10011 S   15044
T TRANSACT     -                    E:\STR1\E000002.log     E:        NTFS      -
\\?\Volume{2ef9993d-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev02   CLI-A  0    1    0
10001 P   15044
- -           -                     -                       -         -         -         -
-           VG01-dev02   CLI-B  1    11   0   10011 S   15044
T TRANSACT     -                    E:\STR1\E000003.log     E:        NTFS      -
\\?\Volume{2ef9993d-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev02   CLI-A  0    1    0
10001 P   15044
- -           -                     -                       -         -         -         -
-           VG01-dev02   CLI-B  1    11   0   10011 S   15044
C CHECKPOINT   -                    E:\STR1\E00.chk         E:        NTFS      -
\\?\Volume{2ef9993d-803e-11d7-96ae-0000e26ac10d}\   Harddisk1   VG01-dev02   CLI-A  0    1    0
10001 P   15044
- -           -                     -                       -         -         -         -
-           VG01-dev02   CLI-B  1    11   0   10011 S   15044
```

### 6.6.4 drmexgrestore (restore storage groups from secondary to primary vol)

**Format:**

```
drmexgrestore backup-ID -resync
              [ -target storage-group-name | -f target-definition-file-name ]
              [ -force ] [ -recovery ]
```

**Description:**

The **drmexgrestore** command performs disk resynchronization to restore data to the primary volume from the secondary volume. The backup data used for restoration is specified by a backup ID.

By restoring the backup data, a database can be returned to the status it was in when the backup was acquired. When the command is executed with the **-recovery** option specified, after restoration has finished, the database is recovered and updated to the latest status.

If a database is comprised of several volumes, all volumes will be restored in order.

The following explains the command processing for restoration in a non-cluster configuration.

1. If the restored database was mounted, the database will be unmounted automatically. If the unmount of the file system fails, an error message will be displayed, and restoration processing will terminate abnormally.
2. Once the database is stopped properly, and the file system confirms that unmount was successful, the backup data will be restored from the secondary volume to the primary volume by disk resynchronization.
3. If the file system was unmounted in step 1, the file system will be mounted. If the file system was already unmounted in step 1, the file system will not be mounted.
4. The database unmounted in step 1 will be mounted.

The following explains the command processing for restoration in a cluster configuration. For this type of restoration, the cluster group containing the storage groups to be restored must be online. If restoration is performed when the cluster group is not online, restoration will terminate abnormally. Because the cluster resources containing the storage groups are offline after restoration, the restored storage groups are temporarily unusable.

1. The disk resources for the storage groups to be restored are automatically set offline. If one or more cluster resources depend on a disk resource that is set offline here, these cluster resources are also set offline automatically. If the command is unable to set the disk resources offline, it outputs an error message and terminates restoration abnormally.
2. The command verifies that the disk resources have been normally set offline, and then restores backup data from the secondary volume to the primary volume by resynchronizing the disk.
3. The disk resources are set online. If one or more cluster resources have been set offline together with the disk resources, these cluster resources are also set online here.

In restoration, data on the primary volume is overwritten by the disk image of the secondary volume at the time backup is performed. Therefore, data on the primary volume that was created or updated after the backup is invalid.

**Arguments:**

***backup-ID***

Specify the backup ID of the backup data to be restored. The backup ID is used to uniquely identify backup data, and is registered in the backup catalog during backup. To check a backup ID, execute the **drmexgcat** command.

**-resync**

Specifies that the primary and secondary volumes should be restored by disk resynchronization. Backup data on the secondary volume is synchronized to the primary volume.

**-target *storage-group-name***

Specifies that databases related to a particular storage group or storage groups be restored. When multiple storage group names are specified, be sure to separate each one with a comma. Put any storage group names that contain space characters in double quotes (“). If this option is omitted, all storage groups on the server on which this command was executed will be restored.

This option is only effective for Exchange 2000 Enterprise Server and Exchange 2003 Enterprise Edition. For any other Exchange Server, this option is invalid.

**-f *target-definition-file-name***

Like the **-target** option, this option specifies that databases related to particular storage groups be restored. Unlike the **-target** option, however, option allows you to view information about multiple storage groups with one setting, so long as those storage groups are already contained in a definition file. Make sure that you specify the path of this definition file as an absolute path.

This option is only effective for Exchange 2000 Enterprise Server and Exchange 2003 Enterprise Edition. For any other Exchange Server, this option is invalid.

**-recovery**

Specifies that recovery is to be executed by roll-forward. You must specify this option when restoring data acquired by an online backup. When the command is executed, post-backup transactions are recovered, and the database is returned to the latest status. However, this is only true if from the time that the backup was acquired until the time that the command was executed, everything was stored properly in Exchange Server.

If this option is omitted, the database will return to the status it was in when the backup was acquired.

***Precaution for use:*** When a cold backup was restored without the **-recovery** option, if you want to restore a backup that is newer than the backup that was already restored it is not possible to use the **-recovery** option for that backup.

**-force**

Specify this option to perform restoration by forced resynchronization of the primary and secondary volumes.

With this option, perform forced resynchronization if the copy group name of the primary volume obtained when the backup processing was performed on the database server corresponds with the information on the database server, even though the LDEV number and the SERIAL number do not correspond with the LDEV number and the SERIAL number when the backup processing was performed. Specify this option only if restoration by resynchronization could not be performed with the **-resync** option, such as when the LDEV number changes when the volume is replaced. If this option is specified under a normal restoration, data might be corrupted.

**Note:**

The backup information in the backup catalog is managed based on the copy group used as a key. Depending on the backup method, you might not be able to perform restoration, even though the backup data exists on the secondary volume.

The example described below uses two storage groups located on separate volumes:

- Storage group A (copy group: **VG01,exg01**)
- Storage group B (copy group: **VG01,exg02**)

Use the following backup method to back up the storage groups:

1. Back up storage group A and storage group B concurrently. The backup ID **0000000001** is created.
2. Back up storage group A only. The backup ID **0000000002** is created.

When you use backup method 2, backup ID **0000000002** is created, and the old backup information (backup ID: **0000000001**) about copy group **VG01,exg01** on storage group A is deleted from the backup catalog. In other words, since the backup information about storage group B, which is included in backup ID **0000000001**, is also deleted from the backup catalog, the file system B cannot be restored even though the backup data exists in the secondary volume. When you restore storage group B, restore the backup data obtained by using backup method 1 from tape to the secondary volume, and then restore the backup data from the secondary volume to the primary volume.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Examples:**

The following command restores, by disk resynchronization, the backup data identified by the backup ID **0000000001**:

```
PROMPT> drmexgrestore 0000000001 -resync
KAVX0001-I The drmexgrestore command will now start.
KAVX1805-I The information store will now be dismounted.
             Storage group name = STR1
KAVX1700-I Restore processing will now start.
KAVX1701-I Restore processing has finished.
KAVX1806-I The information store will now be mounted.
             Storage group name = STR1
KAVX0002-I The drmexgrestore command will now end.
```

The following command restores, by disk resynchronization, the backup data identified by the backup ID **0000000003**, and then performs roll-forward recovery:

```
PROMPT> drmexgrestore 0000000003 -resync -recovery
KAVX0001-I The drmexgrestore command will now start.
KAVX1805-I The information store will now be dismounted.
             Storage group name = STR1
KAVX1700-I Restore processing will now start.
KAVX1701-I Restore processing has finished.
KAVX1806-I The information store will now be mounted.
             Storage group name = STR1
KAVX0002-I The drmexgrestore command will now end.
```

### 6.6.5 drmexgverify (verify the integrity of backup data)

**Format:**

```
drmexgverify backup-ID
```

**Description:**

The **drmexgverify** command verifies the integrity of the backup data on a secondary volume. This verification uses the checksum function of the **ESEUTIL** utility for the Exchange Server.

Execute this command on the backup server.

You must complete the following operations before executing this command:

- Install Microsoft® Exchange Administration Tool on the backup server. The Exchange Server version and service pack level must be the same on the database server and backup server.

  For information on installing the Microsoft(R) Exchange Administration Tool, see the manual for Microsoft® Exchange 2000 Server or Microsoft® Exchange Server 2003.

  Copy the following files to execute the **ESEUTIL** utility from ***Microsoft-exchange-administration-tool-installation-folder*\bin** on the backup server to ***Protection-Services-installation-folder*\bin\util** on the backup server:

  - **ESEUTIL.exe**
  - **ESE.dll**
  - **EXOSAL.dll**
  - **EXCHMEM.dll**
- Export and import the backup catalog to transfer it from the database server to the backup server.
- Use the **drmmount** command to mount the secondary volume containing the Exchange database (***.edb** file) to the backup server. After the **drmexgverify** command terminates, use the **drmumount** command to unmount the secondary volume.

The **ESEUTIL** utility version on the server where backup was performed (database server) and the **ESEUTIL** utility version on the server where the **drmexgverify** command is executed (backup server) are different, the verification result is not guaranteed. When you copy the **ESEUTIL** utility, make sure that you copy data in the server on which backup was performed.

**Argument:**

***backup-ID***

Specify the backup ID of the secondary volume for which you want to verity the integrity. A backup ID has been assigned when a backup catalog was created in the backup server by exporting and importing information.

**Note:**

This command only verifies the integrity for the Exchange database (***.edb** file), and not for the Exchange streaming database (***.stm** file). This means that even if this command successfully terminates the verification, the Exchange streaming database may have been corrupted. In this case, the backup data cannot be restored.

**Return values:**

**0**: Normal termination

**Other than 0**: Abnormal termination (A message indicating abnormal termination is sent to the standard output.)

**Example:**

The following command verifies the backup data whose backup ID is **0000000001**:

```
PROMPT> drmexgverify 0000000001
KAVX0001-I The drmexgverify command will now start.
KAVX1650-I The checksum of the Exchange database file was confirmed.
            Storage group name = STR1
KAVX0002-I The drmexgverify command will now end.
```

# Chapter 7 Troubleshooting

This chapter explains how to deal with problems that may occur during the operation of Protection Services.

7.1 General troubleshooting

7.2 Troubleshooting extended commands

7.3 Data to be collected when a problem occurs

7.4 Collecting the required data

7.5 Investigating the collected data

## 7.1 General Troubleshooting

To deal with problems that may occur during the operation of Protection Services follow these steps:

1. Check the operating conditions and output messages corresponding to when the problem occurred. For details on how to respond to a message, see Chapter 8.
2. Collect log information and other data that can be used to identify the primary cause. For details on the data to collect and how to collect it, see section 7.3.
3. Based on the data collected, investigate the cause and analyze the problem. Use the collected data to investigate the cause of the problem and determine where the problem occurred.
4. If you still cannot understand the cause of the problem after this step, contact your Hitachi Data Systems representative or the Hitachi Data Systems Support Center. For instructions on calling the Support Center, see section 7.6.

***ShadowImage:*** For information on troubleshooting ShadowImage operations, please refer to the ShadowImage manual for the applicable subsystem(s) (e.g., *Hitachi Lightning 9900™ V Series ShadowImage User's Guide*, MK-92RD110).

***CCI:*** For information on troubleshooting CCI operations, please refer to the CCI manual for the applicable subsystem(s) (e.g., *Hitachi Lightning 9900™ V Series and Lightning 9900™ Command Control Interface (CCI) User and Reference Guide*, MK-90RD011).

## 7.2 Troubleshooting Extended Commands

If a problem occurs during execution of an extended command, the extended command abnormal termination message is output to the standard output log file **drm_script.log** for extended commands. In such a case, you should perform the procedure described below.

To handle an extended command problem:

1. Check the problem status. Refer to the extended command log file **drm_script.log** or **drm_script.log.old** to check the operation status from the time the problem with the extended command occurred or the message content.

   For details on the message content and message troubleshooting, see Chapter 8.

2. Check the problem in the Protection Services log file. When an error occurs in the Protection Services internal command of the extended command, an error message is output to the Protection Services log file **drm_output.log**. See the content of the Protection Services log file regarding the time when the error message for the extended command was output, and check the message and the operation status from the time the problem with the Protection Services command occurred.

3. Check the OS log file. If the error message was not output to the **drm_output.log**, see the OS log file, and then check the operating status when the problem occurs.

## 7.3 Data to be Collected When a Problem Occurs

This section describes the data that needs to be gathered to determine the cause of a problem.

### 7.3.1 Data to be Collected (in UNIX)

#### *(1) OS log information*

Collect the OS log information shown in Table 7.1.

**Table 7.1 OS Log Information (UNIX)**

| Information Type | Summary | Default File |
|---|---|---|
| System log | syslog | In Solaris: **/var/adm/messages**<br>In HP-UX: **/var/adm/syslog/syslog.log** |
| System files | **hosts** file | **/etc/hosts** |
| | **services** file | **/etc/services** |
| | **passwd** file | **/etc/passwd** |
| Information about the operating system and installed product | ▪ Names of the operating system and installed product<br>▪ Version information<br>▪ Patch information | — |
| Process information | Process list * | — |
| Environment setting information | Environment variable | — |
| Disk configuration information | Configuration information for logical volumes | — |
| Dump information | **core** file | — |
| Cluster control software information | Definition file and log file | — |

Legend: — indicates that there is no corresponding file name.

* ***Note:*** Execute the **ps** command to check the status of the Protection Services processes. These processes have names that start with **drm**.

#### *(2) Protection Services information*

Collect information pertaining to Protection Services, as shown in

Table 7.2. Also, in cases where the problem occurred over a network connection, you will need to collect files from the connected machine.

**Table 7.2 Protection Services Information (UNIX)**

| Information Type | Summary | Default Files |
|---|---|---|
| Version information | Protection Services version information file | All of the following corresponding files: **/opt/drm/.version*** |
| Environment settings | Files for each type of Protection Services environment setting | All of the following corresponding files: **/opt/drm/conf/** |
| Standard output logs | Protection Services log files *1 | **/var/opt/drm/log/drm_output.log**<br>**/var/opt/drm/log/drm_output.log.old** |
| Extended command trace logs | Protection Services trace log files for extended commands *1 | **/var/opt/drm/script/log/drm_script.log**<br>**/var/opt/drm/script/log/drm_script.log.old** |
| Internal trace logs | Protection Services trace log files *2 | **/var/opt/drm/log/drm_pp_trace[1-16].log** |
| License trace logs | Protection Services license trace log files | **/var/opt/drm/log/drm_inst.log** |
| Trace logs of VERITAS NetBackup | Protection Services log files *3 | **/var/opt/drm/log/drm_nbu_backup.log**<br>**/var/opt/drm/log/drm_nbu_backup.log.old**<br>**/var/opt/drm/log/drm_nbu_restore.log**<br>**/var/opt/drm/log/drm_nbu_restore.log.old** |
| Internal operation information | Temporary files | All of the following corresponding files: **/var/opt/drm/tmp/** |
| Dictionary map *4 | Dictionary map files | All of the following corresponding files: **/var/opt/drm/db/** |

***Notes:***

1. If the size of these log files reaches 10 MB, a file with **.old** attached to the end of the file name is created. (For **drm_output.log**, the file to be created is **drm_output.log.old**.) If a file whose name ends with **.old** already exists, it is overwritten.
2. When the size of the log file reaches 10 MB, a file is created using a number from 1 to 16 for the file name.
3. When the **drmtapebackup** command is executed and the backup command of VERITAS NetBackup is executed, the result of the command operation is output to **drm_nbu_backup.log**. When the size of the **drm_nbu_backup.log** file reaches 10 MB, the contents of the file are moved to **drm_nbu_backup.log.old**. If **drm_nbu_backup.log.old** already exists, it is overwritten.

   When the **drmtaperestore** command is executed and the restoration command of VERITAS NetBackup is executed, the result of the command operation is output to **drm_nbu_restore.log**. When the size of the **drm_nbu_restore.log** file reaches 10 MB, the contents of the file are moved to **drm_nbu_restore.log.old**. If **drm_nbu_restore.log.old** already exists, it is overwritten.
4. When a different directory is specified for **DRM_DB_PATH** in the **init.conf** file, collect the data from the corresponding directory.

### *(3) CCI Information*

Collect the information about CCI shown in Table 7.3. Also, in cases where the problem occurred over a network connection, you will need to collect files from the connected machine.

***Note:*** For further information on CCI environment settings, log files, and RAID configuration information, please refer to the CCI manual for the applicable subsystem(s) (e.g., *Hitachi Lightning 9900™ V Series and Lightning 9900™ Command Control Interface (CCI) User and Reference Guide*, MK-90RD011).

**Table 7.3 CCI Information (UNIX)**

| Information Type | Summary | Default Files |
|---|---|---|
| Environment settings *1 | Files for each type of CCI environment setting | All of the following corresponding files: **/etc/horcm*** |
| Log information *2 | Each type of CCI log files | All of the files in the following directory: **/HORCM/log*** |
| RAID configuration information | Execution result of the CCI **inqraid**, **raidscan**, or **pairdisplay** command | — |

***Notes:***

1. When a different file is specified, collect the corresponding data.
2. When a different directory is specified for the log directory, collect data from the specified directory.

### *(4) Operation details*

The following information, pertaining to the operation that was being performed when the problem occurred, also needs to be collected.

- The details of the operation (parameters specified by commands, etc.)
- The date and time when the problem occurred
- The machine configuration (the version of each OS and the host name)
- Whether or not the error is reproducible

## 7.3.2 Data to be Collected (in Windows)

### *(1) OS log information*

Collect the OS log information shown in Table 7.4.

**Table 7.4 OS Log Information (Windows)**

| Information Type | Summary | Default File Name |
|---|---|---|
| System log | Windows event log *1 | --- |
| System files | **hosts** file | ***system-folder*\system32\drivers\etc\hosts** |
| | **services** file | ***system-folder*\system32\drivers\etc\services** |
| | Windows system information | --- |
| Information about the operating system and installed product | ▪ Names of the operating system and installed product<br>▪ Version information<br>▪ Patch information | --- |
| Environment setting information | Environment variable | --- |
| Disk configuration information | Configuration information for logical volumes | --- |
| Dump information | **Dr. Watson** log file *2 | ▪ Windows 2000 Server ***system-drive*\Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log**<br>▪ Windows Server 2003 ***system-drive*\Documents and Settings*user-name* *3 \Local Settings\ Application Data\Microsoft\Dr Watson\ drwtsn32.log** |
| | Memory dump *2,4 | ▪ Windows 2000 Server ***system-drive*\Documents and Settings\All Users\Documents\DrWatson\user.dmp**<br>▪ Windows Server 2003 ***system-drive*\Documents and Settings\ *user-name* *3 \Local Settings\Application Data\Microsoft\Dr Watson\user.dmp** |
| Cluster control software information | Definition file and log file | --- |
| | CHKDSK execution logs | ***system-folder*\cluster\ChkDsk_*.log** |

***Legend:*** --- indicates that there is no corresponding file name

***Notes:***

1. Collect CSV or text format using Windows Event viewer.
2. When a different file is specified, collect the corresponding data.
3. The name of the user that executed the Protection Services command is applied.
4. If these files are set to be output to another folder, collect them from the appropriate folder.

### *(2) Protection Services information*

Collect information pertaining to Protection Services as shown in Table 7.5. Also, in cases where the problem occurred over a network connection, you will need to collect files from the connected machine. For details on the extended command log files, see section 3.9.

**Table 7.5 Protection Services Information (Windows)**

| Information Type | Summary | Default Files |
|---|---|---|
| Version information | Protection Services version information file | All of the following corresponding files:<br>***Protection-Services-installation-directory*\.version*** |
| Environment settings | Files for each type of Protection Services environment setting | All of the files in the following directory:<br>***Protection-Services-installation-directory*\conf** |
| Standard output logs | Protection Services log files *1 | ***Protection-Services-installation-directory*\log\drm_output.log**<br>***Protection-Services-installation-directory*\log\drm_output.log.old** |
| Extended command trace logs | Protection Services trace log files for extended commands *1 | ***Protection-Services-installation-directory*\script\log\drm_script.log**<br>***Protection-Services-installation-directory*\script\log\drm_script.log.old** |
| Internal trace logs | Protection Services trace log files *2 | ***Protection-Services-installation-directory*\log\drm_pp_trace[1-16].log** |
| License trace logs | Protection Services license trace log files | ***Protection-Services-installation-directory*\log\drm_inst.log** |
| Trace logs of VERITAS NetBackup | Protection Services log files *3 | ***Protection-Services-installation-directory*\log\drm_nbu_backup.log**<br>***Protection-Services-installation-directory*\log\drm_nbu_backup.log.old**<br>***Protection-Services-installation-directory*\log\drm_nbu_restore.log**<br>***Protection-Services-installation-directory*\log\drm_nbu_restore.log.old** |
| Internal operation information | Temporary files | All of the following corresponding files:<br>***Protection-Services-installation-directory*\tmp** |
| Dictionary map *4 | Dictionary map files | All of the following corresponding files:<br>***Protection-Services-installation-directory*\db** |

***Notes:***

1. If the size of these log files reaches 10 MB, a file with **.old** attached to the end of the file name is created. (For **drm_output.log**, the file to be created is **drm_output.log.old**.) If a file whose name ends with **.old** already exists, it is overwritten.
2. If the size of these log files reaches 10 MB, files given a number from 1 to 16 for its file name are created.

3. When the **drmtapebackup** command is executed and the backup command of VERITAS NetBackup is executed, the result of command operation is output to **drm_nbu_backup.log**. When the size of the **drm_nbu_backup.log** file reaches 10 MB in size, it will be moved to **drm_nbu_backup.log.old**. If **drm_nbu_backup.log.old** already exists, it is overwritten.

   When the **drmtaperestore** command is executed and the restoration command of VERITAS NetBackup is executed, the result of command operation is output to **drm_nbu_restore.log**. When the size of the **drm_nbu_restore.log** file reaches 10 MB in size, it will be moved to **drm_nbu_restore.log.old**. If **drm_nbu_restore.log.old** already exists, it is overwritten.

4. When a different directory is specified in **DRM_DB_PATH** of the **init.conf** file, collect data from the specified directory.

### *(3) CCI information*

Collect information pertaining to CCI, as shown in Table 7.6. Also, in cases where the problem occurred over a network connection, you will need to collect files from the connected machine.

**Table 7.6 CCI Information (Windows)**

| Information Type | Summary | Default Files |
|---|---|---|
| Environment settings *1 | Files for each type of CCI environment setting | All of the following corresponding files: ***system-folder*\horcm*** |
| Log information *2 | Each type of CCI log files | All of the files in the following directory: ***system-drive*\HORCM\log*** |
| RAID configuration information | Execution result of the CCI **inqraid**, **raidscan**, or **pairdisplay** command | — |

***Notes:***

1. When a different file is specified, collect the corresponding data.
2. When a different directory is specified for the log directory, collect data from the specified directory.

### *(4) Database information*

Collect the database information listed in Table 7.7. In cases where the problem occurred over a network connection, you will need to collect files from the connected machine.

**Table 7.7 Database Information**

| Information Type | Summary | Default file |
|---|---|---|
| Definition information | Definition file | Not applicable |
| Log information | Log file | Not applicable |

### *(5) Operation details*

The following information, pertaining to the operation that was being performed when the problem occurred, also needs to be collected.

- The details of the operation (parameters specified by commands, etc.)
- The date and time when the problem occurred
- The machine configuration (the version of each OS and the host name)
- Whether or not the error is reproducible

## 7.4 Collecting the Required Data

This section describes how to collect the required data when a problem occurs.

### 7.4.1 Collecting Data (in UNIX)

1. Execute the data collection tool to collect the data to analyze problems. This tool creates a compressed file in tar format and is executed as follows:
   **PROMPT> /opt/drm/bin/util/drm_log.vbs**

   By default, the compressed file (**DRM.log.tar.Z**) is created in the **/tmp/drm/** directory. You can change the file location when you execute the tool by specifying **-f <filename>** as a parameter. If you specify **-f <filename>** as a parameter, this tool will create the **<filename>.tar.Z** file.

   When you execute the data collection tool, confirm that the necessary data was collected.
2. Collect definition information and log information for the cluster control software.
3. Collect definition information and log information for the backup management product.
4. Find out details about the operation that was being performed when the problem occurred, and record the details for later use. The following information needs to be confirmed.
   - The details of the operation (parameters specified by commands, etc.)
   - Error information, such as messages output to the console
   - The date and time when the problem occurred
   - The machine configuration (the version of each OS and the host name)
   - Whether or not the error is reproducible

### 7.4.2 Collecting Data (in Windows)

1. Execute the data collection tool to collect the data to analyze problems. This tool is executed as follows:
   **PROMPT>** ***Protection-Services-installation-directory*****\bin\util\drm_log.bat**

   By default, the data is stored in **%TEMP%\drmlog**. The file location can be changed when you execute the tool, by specifying the desired directory in the parameter.

   When you execute the data collection tool, confirm that the necessary data was collected.

2. Collect the Windows system information.

   ***In Windows 2000:*** Open the **Control Panel**, select **Administrative Tools**, and select **Computer Management**. Collect the **System Information** in **Computer Management**.

   ***In Windows 2003:*** From the **Start** menu, click **Execute with filename**. In the **Execute with filename** dialog box, enter **msinfo32** in the **Name** field. Collect text format data using **Export** under the **File** menu in the **System information** window.

3. Collect the information about the OS and the installed product.

   ***In Windows 2000:*** Open the **Control Panel**, and select **Add/Remove Applications**. With the **Add/Remove Applications** button selected, take a hard copy of the Add/Remove Applications window.

   ***In Windows 2003:*** Open the **Control Panel**, and select **Add/Remove Applications**. With the **Add/Remove Applications** button selected, take a hard copy of the Add/Remove Applications window.

4. Collect the disk configuration information. Open the **Control Panel**, select **Administrative Tools**, and then select **Computer Management**. Select **Disk Management** in **Computer Management**, and then obtain a hard copy of the window displaying volume information.

5. Collect definition information and log information for the cluster control software.

6. Collect definition information and log information for the database.

7. Collect definition information and log information for the backup management product.

8. Record the status when the problem occurred. Find out details about the operation that was being performed when the problem occurred, and record the details for later use. The following information needs to be confirmed.
   - The details of the operation (parameters specified by commands, etc.)
   - Error information, such as messages output to the console
   - The date and time when the problem occurred
   - The machine configuration (the version of each OS and the host name)
   - Whether or not the error is reproducible

### 7.4.3 Adjusting the Output Level for Processed Trace Log Information

The level of information output to trace log files of Protection Services can be changed whenever necessary. Edit the initial settings file for the log output level when you want to adjust the amount of log information to be collected, or to select a certain type of log information necessary to be collected.

- The location for the initial settings file:

  In UNIX, use: **/opt/drm/conf/init.conf**

  In Windows, use: ***Protection-Services- installation-directory*\conf\init.conf**

- Method for editing the file:

  Specify a numerical value in **LOGLEVEL=*n***. The numerical value that can be specified and the correspondence with the target log information to be output are shown below (default = **3**).

  **0**: Error
  **1**: Warning, Error
  **2**: Notification, Warning, Error
  **3**: Information, Notification, Warning, Error
  **9**: All (Information, Notification, Warning, Error, Debug)

### 7.4.4 Adjusting the Number of Log Files for Internal Trace Log Information

The number of trace log files output to the trace log directory of Protection Services can be changed whenever necessary. Edit the initial settings file when you want to adjust the amount of log information to be collected.

- The location of the initial settings file:

  In UNIX, use: **/opt/drm/conf/init.conf**

  In Windows, use: ***Protection-Services- installation-directory*\conf\init.conf**

- Method for editing the file:

  Specify a numerical value in **PP_LOGFILE_NUM=*n***.
  The range is from 1 to 16 (default = 2).

## 7.5 Investigating the Collected Data

This section explains the procedure for investigating the data collected for solving problems when a Protection Services command is executed and a problem occurs.

Investigate the data in the following order.

1. Standard output logs
2. Trace logs for Protection Services-cooperative software
3. Internal trace logs

### 7.5.1 Investigating standard output logs

When execution of a Protection Services results in some problem, investigate the information in the standard output logs. When a problem occurs, the messages that were displayed in the standard output, and the time when the problem occurred, are recorded in the standard output logs.

Refer to the contents of the standard output log, and check what messages were output when the problem occurred. For details on how to respond to messages, see Chapter 8.

### 7.5.2 Investigating the Trace Logs for Protection Services-Cooperative Software

When the cause of a problem cannot be solved even if you have investigated the message in the standard output log, or when a problem is not eliminated even if you have carried out the recommended action, then investigate the information in the trace log of the software that cooperates with Protection Services (referred to as Protection Services-cooperative software).

Protection Services functions by cooperating with various products: such as a logic volume manager, a backup manager product, and CCI. The execution results of such Protection Services-cooperative software are recorded in trace logs. The trace log files that record the execution results of Protection Services-cooperative software are as follows:

- Trace logs related to disk operations
- Trace logs of VERITAS NetBackup

The execution results when controlling CCI and a logic volume manager are output to trace logs related to disk operations. When you investigate trace logs related to disk operations and a problem with the CCI is found, examine the detailed trace log provided by the CCI software, and handle the problem according to the contents of the log.

The execution results when controlling VERITAS NetBackup are output to a VERITAS NetBackup trace log. When you investigate a VERITAS NetBackup trace log and a problem with VERITAS NetBackup is found, handle the problem by using the VERITAS NetBackup GUI or by referring to the detailed trace log provided by VERITAS NetBackup.

### 7.5.3 Investigating Internal Trace Logs

When a problem is not solved, even after you have investigated the standard output log and the trace log files of the Protection Services-cooperative software, then investigate the Protection Services internal trace log.

The following information is output to the internal trace log:

- Internal functions that were used from the execution of a command to the end, as shown in the internal processing sequence information
- The time and the command execution process ID for the processing that was performed at the system call level
- Keywords indicating normal and abnormal processing
- Messages indicating error causes

The keyword **ER**, which indicates an abnormality, is output to the log record that the problem generated. In the case of OS system-call abnormalities, the system also outputs the returned value in addition to the keyword. The error causes are output in a message.

Table 7.8 shows the output items for the internal trace logs.

**Table 7.8 Output Items for Internal Trace Logs**

| Output Item | Description |
|---|---|
| Number | Log sequence number |
| Date | Date when the log was output, using the ***yyyy*/*mm*/*dd*** format |
| Time | Time when the log was output, using the ***hh*:*mm*:*ss.sss*** format |
| Application name | Name of the Protection Services command (**drm*xxx***) that triggered the output of the log. |
| Process ID | Process ID |
| Thread ID | Thread ID |
| Message ID | ID of the message |
| Type | Type of the message. The types of message are as follows:<br>**ER** (Error)<br>**WR** (Warning)<br>**NT** (Notification)<br>**IF** (Information)<br>**DB** (Debug) |
| Text | Maintenance information on the product and the message text.<br>The output format is ***maintenance-information*:*message-text***. |

Table 7.9 shows the message IDs that may be output to internal trace logs. In the internal trace log showing the error, use the message ID to find the product that caused the error. Then, take action according to the manual for the product.

To investigate the internal trace log, use the following steps:

1. Use a text editor to search for the keyword **ER** near the time when the error occurred.
2. Check what sort of processing (system call) was being performed when the error occurred.
3. Respond to the error according to the message showing the error causes.
4. If you cannot eliminate the cause of the problem even after you have investigated the internal trace log or if you cannot eliminate the problem, please gather the recommended data (described earlier) and contact the Hitachi Data Systems Support Center. For instructions on calling the Support Center, see section 7.6.

**Table 7.9 Causes of Messages Output to Internal Trace Logs**

| Output Type | Message Output is Triggered By: | Message ID |
|---|---|---|
| Volume Manager | Volume Manager operations (general) | KAVX9000-I, KAVX9001-W, KAVX9002-E |
| | Volume Manager operations (cluster) | KAVX9003-I, KAVX9004-W, KAVX9005-E |
| System | Operations that change the system | KAVX9100-I, KAVX9101-W, KAVX9102-E |
| | System operations using the Windows API | KAVX9103-I, KAVX9104-W, KAVX9105-E |
| | Service operations using the Windows API | KAVX9106-I, KAVX9107-W, KAVX9108-E |
| | Device operations using the Windows API | KAVX9109-I, KAVX9110-W, KAVX9111-E |
| Cluster | Cluster operations using the UNIX cluster product functions | KAVX9200-I, KAVX9201-W, KAVX9202-E |
| | Cluster operations using the Windows API | KAVX9203-I, KAVX9204-W, KAVX9205-E |
| Database | Operations and instructions using commands | KAVX9300-I, KAVX9301-W, KAVX9302-E |
| | Operations and instructions using OCI | KAVX9303-I, KAVX9304-W, KAVX9305-E |
| | Operations and instructions using ODBC | KAVX9306-I, KAVX9307-W, KAVX9308-E |
| COM component | Use of the COM (MSSQL) interface | KAVX9400-I, KAVX9401-W, KAVX9402-E |
| | Use of the COM (ADO) interface | KAVX9403-I, KAVX9404-W, KAVX9405-E |
| | Use of the COM (CDOEXM) interface | KAVX9406-I, KAVX9407-W, KAVX9408-E |
| | Use of the COM (ADSI) interface | KAVX9409-I, KAVX9410-W, KAVX9411-E |
| Other products | Internal trace | KAVX9800-I, KAVX9801-W, KAVX9802-E |
| | General operations | KAVX9803-I, KAVX9804-W, KAVX9805-E |
| | General file operations | KAVX9806-I, KAVX9807-W, KAVX9808-E |
| External product | Cluster products | KAVX9900-I |
| | CCI | KAVX9901-I |
| | Backup management product | KAVX9902-I |

## 7.6 Calling the Support Center

If you need to call the Hitachi Data Systems Support Center, make sure to provide as much information about the problem as possible, including the circumstances surrounding the error or failure, the exact content of any error messages displayed, and the troubleshooting data collected as described in section 7.4.

The worldwide Hitachi Data Systems Support Centers are:

- Hitachi Data Systems North America/Latin America
  San Diego, California, USA
  1-800-348-4357
- Hitachi Data Systems Europe
  Contact Hitachi Data Systems Local Support
- Hitachi Data Systems Asia Pacific
  North Ryde, Australia
  011-61-2-9325-3300

# Chapter 8 Messages

list the Protection Services messages by message ID and provide recommended actions for the messages, if appropriate.

8.1 Message overview

8.2 KAVX0001-I - KAVX0486-W

8.3 KAVX1000-I - KAVX1400-I

8.4 KAVX1500-E - KAVX1901-E

8.5 KAVX2500-E - KAVX2525-E

8.6 Detailed messages

## 8.1 Message Overview

Each Protection Services message consists of a message ID and message text. The following shows the message format:

**KAVX*nnnn-Z message-text***

The message ID consists of the following components:

- **KAVX**: This indicates that the message is a Protection Services message.
- ***nnnn***: The message sequence number.
- ***Z***: The type of the message (see Table 8.1).

**Table 8.1 Message Types**

| Message Type | Description |
|---|---|
| I (information) | An informational message output during normal operation. |
| W (warning) | A message that reports that the operation will continue with some restriction. |
| E (error) | A message that reports that a fatal error occurred and processing cannot continue. |

Some message texts display the error cause depending on the conditions when the error occurred. The *detailed message* is displayed in *Cause*, and is also composed of a message ID and message text. The message format of a detailed message is as follows:

**DRM-*nnnnn message-text***

The message ID consists of the following components:

- **DRM**: This indicates that the message is a Protection Services detailed message.
- ***nnnnn***: The message sequence number.

## 8.2 KAVX0001-I - KAVX0485-W

Table 8.2 lists and describes Protection Services messages KAVX0001-I to KAVX0485-W and provides corrective actions that you can take in response to the messages, if appropriate.

**Table 8.2 KAVX0001-I - KAVX0485-W**

| Message ID | Message Text | Description and Recommended Action |
|---|---|---|
| KAVX0001-I | The command-name command will now start. | The command has started. |
| KAVX0002-I | The command-name command will now end. | The command has ended. |
| KAVX0003-E | The command-name command ended abnormally. | The command ended abnormally. Take action according to the message displayed together with this message. |
| KAVX0004-E | Memory is insufficient. | Memory is insufficient. Increase memory, or check the settings for virtual memory. |
| KAVX0005-E | An error that stops processing occurred. Cause=*detailed-message*, Code=*OS-error-cause-code* | A fatal error that stopped processing in the operating system occurred. Examine the system log and check whether there is any problem in the OS. View the internal trace log information to confirm the details about the error cause. For details on the error cause, see *OS-error-cause-code*. |
| KAVX0006-E | An error that stopped processing occurred. Cause=*detailed-message* | A fatal error occurred, preventing further processing. For details on the error cause, see section 8.6. |
| KAVX0007-E | An error that stopped processing occurred. Code=*OS-error-cause-code* | A fatal error that stopped processing in the operating system occurred. Examine the system log and check whether there is any problem in the OS. View the internal trace log information to confirm the details about the error cause. For details on the error cause, see *OS-error-cause-code*. |
| KAVX0008-E | An error that stopped processing occurred. Cause=*detailed-message* Cause=*Cause* | A fatal error occurred, preventing further processing. For details on the error cause, see section 8.6. |
| KAVX0009-E | The file name specified with the -f option is invalid. | Possible causes are as follows:<br>▪ The specified file does not exist.<br>▪ You do not have read permission for the specified file.<br>▪ The file was not specified by its absolute path.<br>Check the name of the batch definition file, and then re-execute the command. |
| KAVX0010-E | License information is invalid. | Protection Services was not installed by using the installer. Use the installer to re-install Protection Services. |
| KAVX0011-E | Backup ID information could not be obtained. | Possible causes are as follows:<br>▪ The contents of the backup catalog are invalid.<br>▪ The backup catalog is damaged.<br>▪ The backup catalog does not exist. |
| KAVX0012-E | An invalid option was specified. | Possible causes are as follows:<br>▪ A non-existent option was specified.<br>▪ A required option is missing.<br>Check the command usage, and then re-execute the command. |

| | | |
|---|---|---|
| KAVX0013-E | The specified device file cannot be found. | The specified device file name does not exist in the dictionary map file or backup catalog. Make sure that the name of the device file is correct, and then re-execute the command. |
| KAVX0014-E | The specified mount point directory does not exist. | Possible causes are as follows:<br>▪ The specified mount point was not found.<br>▪ The specified mount point is a floppy disk or other removable disk, which is not a storage subsystem.<br>▪ The specified mount point is a network volume.<br>Check the mount point for which you want to perform backup, and then re-execute the command. |
| KAVX0015-E | The specified backup ID does not have corresponding backup data. | The specified backup ID does not have the corresponding backup data in the backup catalog. Check the backup ID. Specify the correct backup ID if necessary and then re-execute the command. If this message appears, even though you specified the correct backup ID with the drmumount command, unmount the secondary volume with the umount command provided by either the OS (in UNIX) or CCI (in Windows). |
| KAVX0016-E | The specified file or directory does not exist.<br>File or directory name =<br>*file-name-or-directory-name* | Possible causes are as follows:<br>▪ The specified file or directory does not exist.<br>▪ The specified file or directory does not exist in the specified object (mount point, instance, or backup ID).<br>▪ The file or directory was not specified by its absolute path.<br>Take the following action depending on the executed command:<br>▪ When the drmdbimport, or the drmdbexport command is executed: Check whether the specified file name is correct, and then re-execute the command.<br>▪ When a command other than the above is executed: Check whether the file or the directory specified (for example, the file or the directory specified with the -target option) is correct. If the specified file or directory is correct, make sure that the file system has sufficient space to store the Protection Services installation directory, and then re-execute the command. |
| KAVX0017-E | The specified file or directory does not exist in the target definition file.<br>File or directory name =<br>*file-name-or-directory-name* | Possible causes are as follows:<br>▪ The file or directory specified in the target definition file does not exist.<br>▪ The file or directory associated with the object specified in the target definition file (mount point, instance, or backup ID) does not exist.<br>▪ The file or directory was not specified by its absolute path.<br>Check and correct the file names or directory names specified in the target definition file, and then re-execute the command. |
| KAVX0018-E | The specified copy group does not exist. | The specified copy group does not exist. Use one of the following commands to check the name of the copy group, and then re-execute the command.<br>▪ drmfsdisplay or drmfscat command for Copy Controller<br>▪ drmsqldisplay or drmsqlcat command for SQL Server<br>▪ drmexgdisplay or drmexgcat command for Exchange Server |

| | | |
|---|---|---|
| KAVX0019-I | Copying file(s) now... | Files are now being copied. |
| KAVX0020-I | Restoring file(s) now... | Files are now being restored. |
| KAVX0021-E | You do not have permission to execute the command. | The user who attempted to execute the command is not a member of the Administrators group (in Windows) or does not have root privileges (in UNIX). Add the user who wants to execute the command to the Administrators group (in Windows) or grant the user root privileges (in UNIX). |
| KAVX0022-E | The specified file or directory does not exist in the mount point directory.<br>File or directory name =<br>*file-name-or-directory-name* | Possible causes are as follows:<br>▪ The specified file or directory does not exist in the mount point directory.<br>▪ The file or directory was not specified by its absolute path.<br>Check and correct the file name or directory name, and then re-execute the command. |
| KAVX0023-I | Dictionary map file was updated. | The drmfsdisplay, drmsqldisplay, or drmexgdisplay command, executed with the -refresh option specified, terminated normally. |
| KAVX0024-E | The specified backup data does not exist. | Possible causes are as follows:<br>▪ There is no information to be displayed because a backup has not been made yet.<br>▪ No backup has been performed, and therefore there is no backup data to display.<br>▪ No data satisfies the conditions specified with the drmfscat, drmsqlcat, drmexgcat, or drmtapecat command option.<br>Check whether backup has been performed. If backup has been performed, check the specified command options. If there is an error, correct the command options, and then re-execute the command. |
| KAVX0025-E | There is no backup data that satisfies the specified conditions. | There is no backup data that satisfies the specified conditions. Check the command options you specified. If they are incorrect, re-execute the command with correct command options specified. |
| KAVX0026-W | Other commands are already running.<br>This command waits for all the other commands to terminate. | You attempted to execute the command while other commands were running. You do not need to do anything because the system will automatically retry executing the command. |
| KAVX0027-E | The command was not executed because other commands were running. | You attempted to execute the command while other commands were running. The system retried executing the command the specified number of times, but the command was not executed because a timeout occurred. Wait until all the other commands terminate, and then re-execute the command. |
| KAVX0028-E | The parameter information set by the initialization command is incorrect. | Re-execute the initialization command to renew the environment settings. |
| KAVX0029-E | Installation-path information could not be obtained. | The system could not obtain the installation path information that is automatically set when Protection Services is installed. Re-install Protection Services. |
| KAVX0030-E | An invalid value was specified. | You specified incorrect parameter values in the initialization command. Specify correct values as initialization parameters. |
| KAVX0031-E | The specified mount point is already in use. | Another volume has already been mounted at the mount point where you attempted to mount a volume. Unmount the file system from the desired mount point, and then re-execute the command. |
| KAVX0032-E | An invalid mount point directory was specified. | A non-existent mount point directory was specified. Specify a mount point directory that actually exists, and then re-execute the command. |

| | | |
|---|---|---|
| KAVX0033-E | The type of backup data with the specified backup ID is different. | The format of the backup data specified with a backup ID is different from the format of the data subject to the executed command. Possible causes are as follows:<br>▪ The data could not be recovered because the format of the backup data subject to the command used for restoring it is different from the format of the backup data specified with a backup ID.<br>▪ The copy group could not be resynchronized because the backup ID created with the drmtapebackup command was specified with the drmresync command.<br>To re-synchronize the copy group, do not specify the ID of a backup created by the drmtapebackup command. Execute the drmfscat, drmsqlcat, or drmexgcat command to check the permitted backup ID, then re-execute the drmresync command. |
| KAVX0034-E | The specified instance has not been initialized. | The initialization command was executed with the -v option specified, but the initialization information of the specified instance was not found. Execute the initialization command for the specified instance. |
| KAVX0035-E | An attempt to update the *application-name* information failed. | The executed command failed to register the initialization information for the application indicated in *application-name*. Expand the disk capacity in the installation directory, and then re-execute the command. |
| KAVX0036-E | The specified backup ID is invalid.<br>Backup ID = *backup-ID* | The backup record corresponding to the specified backup ID does not exist. Check the backup ID, and then re-execute the command. |
| KAVX0037-E | The specified character string exceeds the maximum number of characters.<br>String = *character-string* | The length of the file name, directory name, mountpoint directory name, or storage group name specified when the command was executed exceeds the maximum length for a character string. Check the number of characters in the file name, directory name, mountpoint directory name, or storage group name. |
| KAVX0038-E | The content of the specified target definition file is invalid. | One or more of the following items are not specified in the batch definition file.<br>▪ File name<br>▪ Directory name<br>▪ Storage group name<br>Enter valid information in the batch definition file. |
| KAVX0039-E | The core map file(s) cannot be found. | The appropriate data does not exist in the dictionary map file. Possible causes are as follows:<br>▪ The core map file has not been created.<br>▪ Creating a dictionary map file is being performed.<br>▪ The core map file has been deleted because creating a dictionary map file fails.<br>▪ The specified mount point directory does not exist in the RAID device.<br>Take the following action depending on the cause of the error:<br>▪ Use the drmfsdisplay, drmsqldisplay, or drmexgdisplay command, and then re-create the dictionary map file. Execution examples:<br>drmfsdisplay –refresh<br>drmsqldisplay –refresh<br>drmexgdisplay –refresh<br>▪ Wait until creating a dictionary map file finishes, and re-execute the command.<br>▪ See the message displayed when creating a dictionary map file fails, and then take actions to re-create a dictionary map file. After creating a dictionary map file ends successfully, re-execute the command.<br>▪ If the specified mount point directory does not exist on the RAID device, specify a mount point directory that exists on the RAID device, and then re-execute the command. |

| | | |
|---|---|---|
| KAVX0040-I | The backup ID has been assigned as follows.<br>Backup ID = *backup-ID* | This message is displayed when a backup ID was assigned to data that was backed up successfully. |
| KAVX0041-W | The invalid area is increasing in the dictionary map file or the backup catalog. | During backup or restore processing, the ratio of invalid records to all the records in the dictionary map file or the backup catalog exceeded 90%. Using the control tool for dictionary map files, delete the dictionary map files or invalid records in the backup catalog.<br>In UNIX:<br>PROMPT> /opt/drm/bin/util/drmdbcond –c<br>In Windows:<br>PROMPT> *Protection-Services-**installation-directory***\bin\util\drmdbcond –c |
| KAVX0042-E | An error occurred during cluster processing.<br>Cause = *detailed-message* | An error has occurred during cluster operation. For details on the error cause, see section 8.6. |
| KAVX0043-E | A cold backup was not performed for the mount point directory because the specified mount point was being managed by the cluster. | A cold backup could not be performed for the mount point directory, because the cluster system is managing the mount point. Perform an online backup. |
| KAVX0044-E | A resynchronize restoration could not be performed for the mount point directory because the specified mount point was being managed by the cluster. | A resynchronize restoration could not be performed for the mount point directory, because the cluster system is managing the mount point. Perform a restoration by file copy. |
| KAVX0047-E | You cannot execute this command under this configuration. | Backups can fail for any of the following reasons:<br>▪ All the file systems in the volume to be backed up were not specified.<br>▪ Only some of the databases in the volume to be backed up were specified for backup.<br>▪ There is an error in the definition contents of the CCI copy group.<br>Depending on the cause, take the following actions:<br>▪ Specify all the objects in the volume to be backed up.<br>▪ Make sure that the copy group contained in the file system to be backed up is configured correctly, and then check the options of the backup command. |
| KAVX0048-E | Characters that cannot be handled with this program have been found. | Protection Services is not compliant with the Unicode character set. If any Unicode characters exist in command parameters or configuration files, commands will not execute successfully. Make sure that no Unicode characters are being used in command parameters of configuration files, and then re-execute the command. |
| KAVX0049-E | You cannot specify the -raw option for the specified backup ID. | You cannot specify the -raw option for the specified backup ID. Perform backup again, without the -raw option specified. |
| KAVX0050-E | An attempt to read the target definition file failed. | Use a text editor to check whether the specified target definition file can be opened. |
| KAVX0051-E | An attempt to execute restoration by disk resynchronization failed. | You cannot perform restoration because, in the current configuration, restoration by disk resynchronization may damage file systems or storage groups other than those you want to restore. Use the drmfscat, drmsqlcat, or drmexgcat command to check whether the target copy group contains only the file systems and storage groups you want to restore. |
| KAVX0052-E | You cannot specify the -mode cold option because the cluster resource is not online. | Set the cluster resource you want to back up online or re-execute the command with the -mode online option specified. |
| KAVX0053-E | The system could not restore the target data because the cluster resource is not online or offline. | The cluster resource has an invalid status. Check the status of the cluster resource, and then re-execute the command. |
| KAVX0054-E | An attempt to mount the directory failed.<br>Mount point = *mount-point-directory-name* | Make sure the specified mount point directory exists. If it exists, examine the system log and check whether there is any problem with the OS. |

| | | |
|---|---|---|
| KAVX0055-E | An attempt to unmount the directory failed.<br>Mount point = *mount-point-directory-name* | Check whether another process is using the disk you want to unmount. Note that you cannot unmount the disk that contains the current directory at which you execute the command. If the specified mount point directory is correct, examine the system log and check whether there is any problem with the OS. |
| KAVX0056-E | An attempt to create the directory failed.<br>Directory name = *directory-name* | Check the indicated directory pathname to see whether the directory can be created. If the directory can be created, examine the system log and check whether there is any problem with the OS. |
| KAVX0057-E | An attempt to remove the directory failed.<br>Directory name = *directory-name* | Check the indicated directory pathname to see whether the directory exists. If the directory exists, examine the system log and check whether there is any problem with the OS. |
| KAVX0069-W | An error occurred during operation of the trace log file. | This message is output when an error is detected during processing executed for the trace log files, which are provided by Protection Services. Check the system log, and make sure that the OS is running properly. If no problems are found, contact the Support Center. |
| KAVX0070-W | The system had changed the configuration of effective path(s) of the logical volume(s) .<br>Effective Path = *effective-path* | In HP-UX, this message appears when a disconnected path is found in a multi-path environment for logical volumes. If the file server is not in the cluster configuration, recover the disconnected physical path, and then re-execute the command. If the file server is in the cluster configuration, follow the recovery procedure shown in section 8.7. |
| KAVX0071-W | Unable to stop the Command Control Interface instance.<br>Cause = *detailed-message* | This message appears if the CCI instance cannot stop for some reason. Check what is indicated in Cause. Then, stop the CCI instance as required. For details on the error cause, see section 8.6. |
| KAVX0072-E | The application map file(s) cannot be found. | Use the drmfsdisplay, drmsqldisplay, or drmexgdisplay command to re-create the dictionary map file. To do this, execute one of the following commands:<br>drmfsdisplay -refresh<br>drmsqldisplay -refresh<br>drmexgdisplay -refresh |
| KAVX0073-E | The data associated with the specified conditions does not exist. | There is no data that satisfies the conditions specified with the option of the drmfsdisplay, drmsqldisplay, or drmexgdisplay command. Check the options of the specified command. If there is a problem, specify the correct command option, and then re-execute the command. |
| KAVX0074-E | An attempt to obtain a mount point failed. | Information about the mount point that was mounted by the drmmount command is invalid. Re-execute the drmmount command. |
| KAVX0100-E | The root directory cannot be specified as the mount point directory. | The root directory was specified as the mount point directory. Specify a directory other than the root directory as the mount point directory for the backup. |
| KAVX0101-E | A drive containing a system directory cannot be specified as the mount point directory. | A drive containing a system directory was specified as the mount point directory. As the mount point for backup, specify a drive that does not contain a system directory. |
| KAVX0102-E | The mount point directory does not contain any files to be backed up. | No files exist in the specified mount point directory. Since the specified mount point contains no files, backup was not performed. |
| KAVX0103-E | Disk space is insufficient at the restoration destination. | The restoration-destination volume does not have sufficient free space. Check the amount of free space at the restoration-destination volume, and then re-execute the command. |

| | | |
|---|---|---|
| KAVX0104-E | The specified mount point definition file does not exist. | The specified mount point definition file name contains an error. Check that the specified mount point definition file exists, and re-execute the command. |
| KAVX0105-E | The specified mount point directory does not exist on the RAID device.<br>Mount point directory = *mount-point* | Possible causes are:<br>▪ The specified mount point directory was not found.<br>▪ The specified mount point directory is mounted on a device other than a RAID device.<br>▪ The mount point directory was not specified by its absolute path.<br>▪ The specified file system cannot be recognized as a file system.<br>Check the specified mount point directory, and then re-execute the command. |
| KAVX0106-E | The specified mount point directory is wrong.<br>Mount point directory = *mount-point* | This message appears when the mount point directory is not a directory. Check the specified mount point directory, and then re-execute the command. |
| KAVX0150-I | The license was updated. | The license key was updated properly. |
| KAVX0151-E | The license has expired. | The current license has been expired. Extend the expiration date, or update the license to the one with no limited date. |
| KAVX0152-E | The system environments is incorrect. | The license environment is invalid. Check the license environment, including the location and format of the license file. |
| KAVX0153-E | The entered license key is invalid. | The new license key is invalid. Check the license key, and change it to the correct license key. |
| KAVX0154-E | The product id is invalid. | The product ID is invalid. Check the product ID, and then re-execute the command. |
| KAVX0155-E | The entered options are not enough. | The command options are not sufficient. Re-execute the command by specifying the options in the correct format. |
| KAVX0156-I | The temporary (emergency) key will expire in n days on *yyyy*/*mm*/*dd*. | The expiration date and the remaining days until the temporary (emergency) key expires are reported. |
| KAVX0300-I | The specified copy group was locked. | The specified copy group was locked. |
| KAVX0301-I | The specified copy group was unlocked. | The specified copy group was unlocked. |
| KAVX0302-I | The copy group(s) associated with the specified backup ID were locked. | The copy group(s) associated with the specified backup ID were locked. |
| KAVX0303-I | The copy group(s) associated with the specified backup ID were unlocked. | The copy group(s) associated with the specified backup ID were unlocked. |
| KAVX0304-W | The specified copy group has already been locked or unlocked. | Possible causes are as follows:<br>▪ You attempted to lock a copy group that has already been locked.<br>▪ You attempted to unlock a copy group that has already been unlocked. |
| KAVX0305-W | The copy group(s) associated with the specified backup ID have already been locked or unlocked. | Possible causes are as follows:<br>▪ You attempted to lock copy groups associated with the backup ID that have already been locked.<br>▪ You attempted to unlock copy group(s) associated with the backup ID that have already been unlocked. |

| | | |
|---|---|---|
| KAVX0309-E | An attempt to execute the command-name command failed.<br>Cause = *detailed-message* | An error was detected when the command command-name was executed. Check the Protection Services trace log and the OS system log for any message that indicates a file system error. If the OS is Solaris and one of the causes listed below is displayed, unmount the secondary volume and then execute the drmfsbackup command.<br>▪ Cause = vxvm:vxdg: ERROR: Disk group *disk-group-name*: cannot create:<br>▪ Cause = vxvm:vxdg: ERROR: Device *device-name* is in use<br>When the unmount operation to the secondary volume fails, and the message "Device busy" appears, use the fuser command provided by the OS to check whether the file system is being used by another process. |
| KAVX0310-I | Enter the resource group name: | This message is output when you execute the drmclusinit command. The message prompts you to input the name of the cluster resource group. |
| KAVX0311-I | Enter the resource name: | This message is output when you execute the drmclusinit command. The message prompts you to input the name of the cluster resource. |
| KAVX0312-I | Cluster information was updated. | This message is output when you execute the drmclusinit command, and cluster information is updated successfully. |
| KAVX0313-I | Enter the virtual host name: | This message appears when you execute the drmclusinit command. The message prompts you to enter the cluster's virtual server name. |
| KAVX0314-I | Enter the resource type (S for service. D for disk): | This message appears when you execute the drmclusinit command. The message prompts you to enter the cluster's resource type. |
| KAVX0315-I | Enter the service name: | This message appears when you execute the drmclusinit command. The message prompts you to enter the cluster's service resource name. |
| KAVX0316-I | Enter the disk name: | This message appears when you execute the drmclusinit command. The message prompts you to enter the cluster's disk resource name. |
| KAVX0317-I | Enter the instance name: | This message appears when you execute the drmclusinit command. The message prompts you to enter the name of the instance or storage group to be backed up or restored in a cluster environment. |
| KAVX0318-E | An attempt to update the cluster information failed. | This message appears when you execute the drmclusinit command but register cluster management information incorrectly. Check the settings and the startup status of the cluster management product. If they are correct, examine the system log and check whether there is any problem with the OS. |
| KAVX0319-E | An attempt to check the cluster resource failed. | This message appears if an error occurs during the checking of the entered cluster resource. Check the settings and the startup status of the cluster management product. If they are correct, examine the system log and check whether there is any problem with the OS. |
| KAVX0320-E | An attempt to check the cluster resource failed because the specified cluster process was stopped. | This message appears when the status of the cluster could not be checked because the cluster was inactive when you attempted to check the entered cluster resource. Check the settings and the startup status of the cluster management product. Start the cluster, and then re-execute the drmclusinit command. |
| KAVX0321-W | The specified cluster resource does not exist. | This message appears if the entered cluster resource does not exist. Check whether the settings of the cluster management product and the entered parameters are correct. When they are correct, examine the system log and check whether there is any problem with the OS. |

| | | |
|---|---|---|
| KAVX0322-E | The specified cluster information is not registered. | This message appears when the required parameters are not set for the specified cluster product. Check the settings and the startup status of the cluster management product. Start the cluster, and then re-execute the drmclusinit command. |
| KAVX0400-I | Mounting will now start.<br>Mount point = *name-of-mount-point-directory-on-backup-server* | This message is displayed when executing a backup to tape or a restoration from tape, at the start of the operation to mount the secondary volume on the backup server. |
| KAVX0401-I | Mounting has finished.<br>Mount point = *name-of-mount-point-directory-on-backup-server* | This message is displayed when executing a backup to tape or a restoration from tape, at the successful end of the operation to mount the secondary volume on the backup server. |
| KAVX0402-I | Backup processing will now start.<br>To see more details on backup progress, use the monitoring method of the backup management product.<br>Source = *backup-source-directory-name* | This message is displayed when the backup command of the backup management product starts when backing up to tape. |
| KAVX0403-I | Backup processing has finished.<br>Source = *backup-source-directory-name* | This message is displayed when the backup command of the backup management product ends successfullywhen backing up to tape. |
| KAVX0404-I | Restoration will now start.<br>To see more details on restoration progress, use the monitoring method of the backup management product.<br>Source = *restoration-source-directory-name*<br>Target = *name-of-mount-point-directory-at-restoration-destination* | This message is displayed when the restore command of the backup management product starts when restoring from tape. |
| KAVX0405-I | Restoration has finished.<br>Source = *restoration-source-directory-name*<br>Target = *name-of-mount-point-directory-at-restoration-destination* | This message is displayed when the restore command of the backup management product ends successfully after restoring from tape. |
| KAVX0406-I | Unmounting will now start.<br>Mount point = *name-of-mount-point-directory-on-backup-server* | This message is displayed when executing a backup to tape or a restoration from tape, at the start of the operation to unmount the secondary volume on the database server. |
| KAVX0407-I | Unmounting has finished.<br>Mount point = *name-of-mount-point-directory-on-backup-server* | This message is displayed when executing a backup to tape or a restoration from tape, at the successful end of the operation to unmount the secondary volume on the database server. |
| KAVX0408-E | An attempt to execute the backup command failed.<br>Command = *name-of-command-executed-by-VERITAS-NetBackup-or-VERITAS-Backup-Exec*<br>Error code = *error-number-returned-by-the-command-of-VERITAS-NetBackup-or-VERITAS-Backup-Exec* | The VERITAS NetBackup command or VERITAS Backup Exec command resulted in an error. Refer to the documentation for VERITAS NetBackup or VERITAS NetBackup Exec to obtain error information associated with the error code, and take action based on this information. Then re-execute the command. |

| | | |
|---|---|---|
| KAVX0409-E | An attempt to execute the restore command failed.<br>Command = *name-of-command-executed-by-VERITAS-NetBackup-or-VERITAS-Backup-Exec*<br>Error code = *error-number-returned-by-the-command-of-VERITAS-NetBackup-or-VERITAS-Backup-Exec* | The VERITAS NetBackup command or VERITAS Backup Exec command resulted in an error. Refer to the documentation for VERITAS NetBackup or VERITAS NetBackup Exec to obtain error information associated with the error code, and take action based on this information. Then re-execute the command. |
| KAVX0410-E | An attempt to obtain the installation path failed.<br>Backup management product = *name-of-backup-management-product-to-be-used* | The backup management product (VERITAS NetBackup or VERITAS Backup Exec) you want to use is not installed. Install VERITAS NetBackup or VERITAS Backup Exec, and then re-execute the command. |
| KAVX0411-I | Enter the backup management product name. | After the drmtapeinit command was executed, this message prompts you to specify the type of the backup management product you want to work with Protection Services.<br>When the OS is UNIX, specify NBU and then press Enter.<br>When the OS is Windows, specify NBU, BENT, or BEWS and then press Enter. |
| KAVX0412-I | Enter the backup class name. | After the drmtapeinit command was executed and NBU was selected as the product type, this message prompts you to specify the name of the backup class definition for VERITAS NetBackup. |
| KAVX0413-I | Enter the backup schedule name: | After the drmtapeinit command was executed and NBU or BEWS was selected as the product type, this message prompts you to specify the name of the backup class definition for VERITAS NetBackup and the name of the related backup schedule. |
| KAVX0414-I | Backup parameters were updated. | The drmtapeinit command terminated normally and the parameters for working with the backup management product were correctly updated. |
| KAVX0415-I | Enter the file name of the backup job script: | After the drmtapeinit command was executed and BENT was selected as the product type, this message prompts you to enter the file name of the VERITAS Backup Exec backup job script. Enter the file name of the VERITAS Backup Exec backup job schedule script used with the backup management product command, the drmtapebackup command, and the drmtaperestore command. Then press Enter. |
| KAVX0416-E | The backup management product has not been set up yet. | You executed the drmtapebackup or drmtaperestore command before using the drmtapeinit command to set the parameters for working with the backup management product. Execute the drmtapeinit command and then execute this command. |
| KAVX0417-I | Enter the number of days to store the backup catalog. | This message is displayed during execution of the drmtapeinit command and prompts you to specify the number of days to store the backup catalog used for tape backup. |
| KAVX0418-I | Backup information from the specified file was imported into the backup catalog.<br>Imported backup ID = *backup-ID* | This message is displayed when the drmdbimport command successfully imported backup catalog information for the backup ID. |
| KAVX0419-E | Backup information associated with the specified backup ID cannot be exported. | You attempted to export backup catalog information before backing up data to tape. Back up data to tape, and then export the backup catalog information. |
| KAVX0420-E | An invalid backup ID was specified.<br>Specify the backup ID of the backup record that was imported by the drmdbimport command. | Data cannot be backed up to tape because the specified backup ID is incorrect. When you back up data to tape, specify the backup ID associated with the backup record that was imported by the drmdbimport command. |

| | | |
|---|---|---|
| KAVX0421-E | An invalid backup ID was specified.<br>Please specify the backup ID acquired using the drmtapebackup command. | The backup ID specified with the drmtapebackup command could not be acquired. Using the drmtapebackup command, specify the backup ID acquired when you backed up to tape. |
| KAVX0422-W | The specified name of the backup management product is invalid. | The specified name of the backup management product is invalid. Enter a correct name for the backup product. |
| KAVX0423-W | The specified value is not in the range from 0 to 365. | During execution of the drmtapeinit command, an incorrect number of days specified for the retention period for the backup record was detected. Specify a value in the range from 0 to 365 days. |
| KAVX0424-I | The backup record corresponding to the specified backup ID has been deleted.<br>Backup ID = *backup-ID-to-be-deleted* | This message is displayed when the drmtapecat command successfully deleted the backup record corresponding to the specified backup ID. |
| KAVX0425-E | The specified backup ID is unavailable for mounting the volumes. | The backup data of the specified backup ID is structured as raw volumes. Since no file systems are created on the volumes, the volumes cannot be mounted. |
| KAVX0426-E | You cannot execute this command because the number of available drive letters is insufficient. | This message appears if the number of secondary volumes used for the backup identified by the specified backup ID is larger than the number of drive letters currently available for mounting the volumes. Unmount unnecessary volumes to make sure that the number of available drive letters is sufficient for mounting the secondary volumes. Then re-execute the command. |
| KAVX0427-E | An attempt to perform backup has failed.<br>Mount point = *mount-point-directory-name* or *drive-letter*<br>Cause = *detailed-message* or *error-code* | This message is output when an attempt to perform backup to tape media fails. See the cause of the error as displayed in the message, and the trace log provided by the backup management product, and make sure that no messages are output that would indicate that the backup was not performed properly. If no problems are found, contact your Support Center. |
| KAVX0428-E | The type of backup object that was specified is invalid. | This message appears when you specify the drmtapecat command with the -o option and the specified backup object type is incorrect. Check the backup object type output by the drmtapecat command, and then re-execute the drmtapecat command. |
| KAVX0429-E | An attempt to perform restore has failed.<br>Restore source = *mount-point-directory-name or drive-letter*<br>Restore point = *mount-point-directory-name or drive-letter*<br>Cause = *cause-code-being-output-to-backup-management-product* | This message appears if an attempt to perform a restoration to tape media fails. View the message displayed in the cause-code-being-output-to-backup-management-product and the trace log provided by the backup management product, and check whether there are any messages indicating that the backup failed. If no problems are found, contact the Support Center. |
| KAVX0430-E | An invalid backup ID was specified.<br>Please specify the backup ID acquired using the drmtapebackup command or the drmmediabackup command. | The backup ID specified with the drmtapebackup command or the drmmediabackup command could not be acquired. Using the drmtapebackup command or the drmmediabackup command, specify the backup ID obtained when you backed up to other media. |
| KAVX0431-E | An attempt to create the backup execution interface file failed.<br>Cause = *cause* | Possible cases are as follows:<br>- Access to the file is not permitted to the user executing the command.<br>- There is not sufficient disk space.<br>Make sure that the disk space is sufficient, and then re-execute the command with the system administrator privileges. |

| | | |
|---|---|---|
| KAVX0432-E | An attempt to create the restore execution interface file failed.<br>Cause = *cause* | Possible cases are as follows:<br>▪ Access to the file is not permitted to the user executing the command.<br>▪ There is not sufficient disk space.<br>Check that the disk space is sufficient, and then re-execute the command with the system administrator privileges. |
| KAVX0450-I | The *extended-command-name* command will now start. | The extended command has started. |
| KAVX0451-I | The *extended-command-name* command will now end. | The extended command has ended. |
| KAVX0452-E | The *extended-command-name* command ended abnormally. | The extended command has ended abnormally. Read the message output to the trace log file for extended commands (drm_script.log or drm_script.log.old), and take appropriate measures. |
| KAVX0453-E | An error that stopped processing occurred.<br>Cause = *cause* | A fatal error has occurred which prevents processing from continuing. For the cause of the error, see section 8.6. |
| KAVX0454-E | An attempt to obtain the information for the specified operation ID failed.<br>Cause = *cause*<br>Definition File = *definition-file-name* | The definition file for the specified operation ID could not be obtained. Check that the displayed definition file exists in the definition file storage directory. When the file exists, execute the check tools and check that the contents are valid. |
| KAVX0455-E | An invalid option was specified. | Possible causes are as follows.<br>▪ The specified option does not exist.<br>▪ A required option is not specified.<br>Check the extended command usage and re-execute the extended command. |
| KAVX0456-E | An attempt to obtain a backup ID failed.<br>Cause = *cause*<br>Backup ID recording file = *backup-ID-recording-file-name* | A backup ID that is required to execute an extended command could not be obtained from the backup ID file. Check that the extended commands are executed in the correct sequence and that the backup ID file is created. For information on where the backup ID recording file is stored, see section 3.3.2. |
| KAVX0457-E | An attempt to obtain the information described in the specified file failed.<br>Cause = *cause*<br>Target File = *file-name* | Required information could not be obtained from the specified file. Check that the specified file exits. When the file exists, check the contents. |
| KAVX0458-W | An error occurred in the trace log file.<br>Cause = *cause* | An error was detected when the trace log file (drm_script.log or drm_script.log.old) was manipulated. Examine the system log and check if there is any problem with the operating system. If no problem is found, contact the Support Center. |
| KAVX0459-E | An attempt to execute the *command-name* command or failed.<br>Cause = *cause*<br>Code = *return-value-of-the-command* | An attempt to execute a command started from the extended command failed. Perform either of the following:<br>▪ See Chapter 3 (Extended Commands) and eliminate the cause of the failure. Then re-execute the command.<br>▪ When the failed command is a Protection Services command (drmxxx), examine the trace log of Protection Services, and eliminate the cause of the failure. Then re-execute the command. |

| | | |
|---|---|---|
| KAVX0460-E | An attempt to execute the *command-name* command failed.<br>Code = *return-value-of-the-command* or *code* | An attempt to execute a command started from the extended command failed. Perform either of the following:<br>▪ See Chapter 3 (Extended Commands) and eliminate the cause of the failure. Then re-execute the command.<br>▪ When the failed command is a Protection Services command (drmxxx), examine the trace log of Protection Services and the SQL Server manual, and eliminate the cause of the failure. Then re-execute the command. |
| KAVX0461-E | An attempt to transmit files failed.<br>Cause = *cause-of-file-transmission-error*<br>From = *source-host-name*<br>To = *destination-host-name* | An FTP file transmission operation failed. On the FTP server, check that you have write permission for the destination directory. Check also that the destination directory has sufficient space and that the network status is normal. |
| KAVX0462-I | The verification of the specified file will now start.<br>File = *definition-file-name* | The verification of the definition file specified in the option has started. |
| KAVX0463-I | The verification of the specified file will now end. | The verification of the specified file has succeeded. The verification of the definition file specified in the option has ended. |
| KAVX0464-E | The verification of the specified file ended abnormally. | The verification of the definition file ended abnormally. Check the message that was displayed and take appropriate measures. |
| KAVX0465-E | An attempt to obtain the information described in the specified definition file failed.<br>Cause = *cause*<br>Target File = *definition-file-name* | Required information could not be obtained from the specified definition file. Check that the specified file exists. If the file exists, check the contents. |
| KAVX0466-E | An essential item is not found in the specified file.<br>Item = *item-name* | The required items are not defined in the definition file specified by the option. Check the contents of the definition file, define the required items, and re-execute the check tool. |
| KAVX0467-E | An item with an empty value exists in the specified file.<br>Item = *item-name* | The value of a required item is not set in the definition file specified by the option. Check the contents of the definition file, set the values of the required items, and re-execute the check tool. |
| KAVX0468-E | The specified file assigns conflicting values for the same item.<br>Item = *item-name* | The same item is specified more than once in the definition file specified by the option. Check the contents of the definition file and make sure that each item is not overlapped. Then re-execute the check tool. |
| KAVX0469-E | The assigned character string for the item exceeds the maximum number of characters.<br>Item = *item-name*<br>Character = *item-value*<br>Maximum number = *maximum-number-of-characters* | The number of characters of an item set in the definition file specified by the option exceeds the maximum limit. Check the contents of the definition file and enter the value within the allowed number of characters. Then re-execute the check tool. |

| | | |
|---|---|---|
| KAVX0470-E | An attempt to connect the database with assigned resources failed.<br>DB_SERVER_NAME = *database-server-name*<br>INSTANCE_NAME = *instance-name*<br>Cause = *cause* | The database could not be connected using the current settings. Possible reasons are as follows.<br>1. In the definition file specified by the option, the database server name or the instance name set in the file is incorrect.<br>2. SQL Server is inactive.<br>3. The user does not have permissions to connect the database.<br>Perform the applicable step shown below. Then re-execute the check tool.<br>1. Check the contents of the definition file. If the specified name is not the name of an existing database server or instance, set a name of an existing server or instance.<br>2. Check the operating status of SQL Server. If SQL Server is inactive, start it.<br>3. Check the access permission of the user who executes the check tool. The user must belong to the Administrators group for SQL Server (sysadmin) to execute the check tool. |
| KAVX0471-E | The instance does not contain the specified database.<br>INSTANCE_NAME = *instance-name*<br>TARGET_NAME = *database-name* | A database name set in the definition file specified by the option is invalid. Check that the database name set in the definition file exists, and then re-execute the check tool. |
| KAVX0472-E | The specified database is invalid.<br>INSTANCE_NAME = *instance-name*<br>TARGET_NAME = *database-name* | A database name set in the definition file specified with the extended command option cannot be backed up to disk. Check the database name set in the definition file, and then re-execute the check tool. |
| KAVX0473-E | An attempt to get the information of the instance assigned by parameter-registration-command-name failed.<br>Cause = *cause*<br>INSTANCE_NAME = *instance-name*<br>Initialization command = *parameter-registration-command-name* | The information set for the target instance by a parameter registration command (drmsqlinit command for SQL Server) could not be read.<br>Execute parameter-registration-command -v target-instance-name to check if the target instance information can be obtained. If the information cannot be obtained, execute parameter-registration-command target-instance-name to set the information again and re-execute the command. |
| KAVX0474-E | The directory specified in the file does not exist.<br>Cause = *cause*<br>Item = *item-name*<br>Directory = *directory-name* | The directory specified in the file is invalid. This message is displayed when the directory name specified in the option-specified definition file is in appropriate.<br>Check the contents of the definition file, make sure that the directory name is correct and that a directory exists, then correct the specified contents and re-execute the check tool. |
| KAVX0475-E | The assigned value for the item is out of the available range.<br>Item = *item-name*<br>Value = *item-value*<br>Available range = *value-range* | The value specified for an item in the definition file specified by the option is outside the specifiable range. Check the contents of the definition file and specify a value within the range. Then re-execute the check tool. |
| KAVX0476-E | The assigned value conflicts with the value assigned by parameter-registration-command-name.<br>AP_FILE_DIR = *metafile-directory-name-set-in-the-definition-file-for-extended-commands*<br>VDI_METAFILE_DIR = *metafile-directory-name-set-by-the-parameter-registration-command*<br>Initialization command = *parameter-registration-command-name* | Possible causes are as follows:<br>▪ Metafile directory information in the file specified in the definition file conflicts with the information set with the parameter registration command (drmsqlinit).<br>▪ The case of the actual directory name does not match that of a directory name set in the definition file.<br>Check for conflicts and case differences between the actual directory name and the metafile directory name set in the definition file for extended commands. Then, correct the metafile directory information set in the definition file for extended commands and re-execute the check tool. |

| | | |
|---|---|---|
| KAVX0477-I | The *command-name* command will now start. | This message appears when a command executed by an extended command starts. When a standard command in the operating system (such as ftp.exe and fc.exe) or an internal command of Protection Services (such as the drmidextract command) starts, this message is output. |
| KAVX0478-I | The *command-name* command will now end.<br>Code = *return-value-of-the-command* | This message appears when the command executed by the extended command ended successfully. When a standard command in the operating system (such as ftp.exe and fc.exe) or an internal command of Protection Services (such as the drmidextract command) starts, this message is output. |
| KAVX0479-E | The backup object is invalid.<br>BACKUP_OBJECT = *backup-object-name* (specified in the definition file)<br>Required Value = *backup-object-name* | The value of the BACKUP_OBJECT in the specified definition file is invalid. Check the BACKUP_OBJECT in the definition file, modify the value if necessary, and then re-execute the check tool. |
| KAVX0480-E | The specified file assigns duplicate target names.<br>TARGET_NAME = *file name-or-directory-name* | The same file name or directory name was specified multiple times with the file name or directory name specification (TARGET_NAME) in the definition file specified with the option.<br>Check the specifications in the definition file, uniquely specify the file name or directory name, and then re-execute the check tool. |
| KAVX0481-E | The HOST_ROLE specified in the definition file and in the command line parameter do not match.<br>Command option = *host-role* (specified in the parameter)<br>HOST_ROLE = *host-role* (specified in the definition file) | The host role specified in the definition file and the host role specified in the parameter of the extended command are different. Check the host roles both in the definition file and in the parameter of the extended command. Match both host roles and then re-execute the check tool. |
| KAVX0482-E | An error that stopped processing occurred.<br>Cause = *cause*<br>File or directory name = *subject-file-name-or-directory-name* | A fatal error occurred, preventing further processing. For details on the error cause, see section 8.6. |
| KAVX0483-E | The command file is not placed in the regular folder.<br>File = *absolute-path-of-the-executed-extended-command* | Possible reasons are as follows.<br>▪ The extended command file was not in the installation directory of Protection Services.<br>▪ A file required for executing the extended command could not be found.<br>Make sure that the extended command is in the installation directory of Protection Services. If the extended command is in the installation directory of Protection Services, reinstall Protection Services. If the extended command is not in the installation directory of Protection Services, move the extended command in the installation directory of Protection Services and then re-execute the extended command. |
| KAVX0484-W | An attempt to obtain the information coded in the message catalog file has failed.<br>Cause = *cause*<br>Message Catalog File = *message-catalog-file-name* | Message information could not be acquired from the message catalog file. The message catalog file may be damaged. Re-install Protection Services. |
| KAVX0485-W | An attempt to obtain the information coded in the definition file has failed.<br>A default value was assigned<br>Definition File = *definition-file-name*<br>Item = *item-name*<br>Default Value = *value* | As the value of MAX_LOG_LINES specified in the host environment setup file was not appropriate, the processing was executed with the MAX_LOG_LINES value specified to 100,000. Correct the value of MAX_LOG_LINES specified in the host environment setup file and re-execute the check tool. |

| | | |
|---|---|---|
| KAVX0486-E | An error occurred in the meta file.<br>Cause = *cause*<br>File = *meta-file-name* | The metafile on the SQL Server that was to be operated on by the extended command could not be copied.<br>Check if a metafile output with the asterisk specification exists, and then take the following corrective action.<br>▪ If you executed the EX_DRM_SQLFILE_PACK command: Execute either the EX_DRM_SQL_BACKUP command or the EX_DRM_TAPE_RESTORE command to create the metafile.<br>▪ If you executed the EX_DRM_SQLFILE_EXTRACT command: Specify the EX_DRM_FTP_PUT command, EX_DRM_FTP_GET command, or the EX_DRM_SQLFILE_PACK command to transfer the metafile. |

## 8.3 KAVX1000-I - KAVX1400-I (SQL Server)

Table 8.3 lists and describes Protection Services messages KAVX1000-I to KAVX1400-I and provides corrective actions that you can take in response to the messages, if appropriate.

**Table 8.3 KAVX1000-I - KAVX1400-I**

| Message ID | Message Text | Description and Recommended Action |
|---|---|---|
| KAVX1000-I | Logged on to the SQL Server system. | An attempt to log on to the SQL Server finished successfully. |
| KAVX1001-I | Logged off from the SQL Server system. | An attempt to log off from the SQL Server finished successfully. |
| KAVX1002-E | The specified database does not exist in this instance of SQL Server.<br>Database name = database-name | The specified database does not exist in this instance of SQL Server. Specify the database in the SQL Server. |
| KAVX1003-E | An attempt to connect to SQL Server has failed. | Possible causes are as follows:<br>▪ The specified instance of SQL Server does not exist.<br>▪ The specified instance of SQL Server is not running.<br>Specify a correct instance of SQL Server. If the specified instance is correct, confirm that the instance is running in Enterprise Manager. If the instance is not running, start an instance and then re-execute this command. |
| KAVX1004-E | You must use the drmsqlinit command before using other commands. | The instance environment has not been configured. Use the drmsqlinit command to configure the environment, and then re-execute the command. |
| KAVX1008-E | An error occurred during SQL Server processing.<br>Processing = *processing*<br>Code = *error-code-for-SQL-server*<br>Cause = *error-message-for-SQL-server* | An error occurred during SQL Server processing. Check the SQL Server documentation, remove the cause of the error, and then re-execute the command. |
| KAVX1010-E | The user lacks appropriate permission to use SQL Server.<br>Processing = processing<br>Cause = *error-message-for-SQL-server* | A user who does not have permission to use SQL Server executed a command. Check the SQL Server documentation, confirm that the user has the appropriate permissions, and then re-execute the command. |
| KAVX1013-E | This version of SQL Server is not supported.<br>SQL Server version = SQL-Server-version | A command was executed on a version of SQL Server not supported by Protection Services. Check the version of SQL Server being used. |
| KAVX1014-E | The database to be processed does not exist. | The specified database to be processed does not exist. Confirm that the specified database name is correct, and then re-execute the command. |
| KAVX1015-E | The temporary database tempdb cannot be specified. | This message is displayed if the user tries to specify the temporary database tempdb using the -target, -f, or -transact_log_list options. Do not specify tempdb as a database name. |
| KAVX1017-I | SQL Server information is being collected now. | SQL Server information is being collected now. |
| KAVX1018-E | An attempt to stop SQL Server failed. | This message is displayed when an attempt to stop SQL Server fails. Collect the SQL Server error log and the Windows event log, and make sure that no problems exist with either SQL Server or the OS. If no problems are found, contact your support center. |
| KAVX1100-I | Enter the name of the storage directory for VDI metafiles: | The system is waiting for the user to enter the name of the storage directory for VDI metafiles. |

| | | |
|---|---|---|
| KAVX1101-I | Enter the timeout interval for VDI generation (in seconds, between 0 and 3600): | The system is waiting for the user to enter the timeout interval for VDI generation. This value should be between 0 and 3600. |
| KAVX1102-I | Enter the name of the storage directory for undo files: | The system is waiting for the user to enter the name of the storage directory for undo files. |
| KAVX1103-I | SQL Server information has been updated. | One or more parameters linked with SQL Server have been registered. |
| KAVX1104-W | The specified storage directory for VDI metafiles cannot be found.<br>Directory name = *directory-name* | Possible causes are as follows:<br>▪ The name of the storage directory for VDI metafiles registered by the drmsqlinit command contains an error.<br>▪ The directory storing the VDI metafiles was not specified with an absolute path.<br>Specify a correct name for the storage directory for VDI metafiles, and then re-execute the command. |
| KAVX1105-W | The value specified for the timeout interval for VDI generation is outside of the acceptable range (between 0 and 3600).<br>Timeout interval for VDI generation = VDI-timeout-second | The value of the timeout interval for VDI generation registered with the drmsqlinit command contains an error. Specify a correct value for the timeout interval for VDI generation, and then re-execute the command. |
| KAVX1106-W | The specified undo file directory cannot be found.<br>Directory name = *directory-name* | Possible causes are as follows:<br>▪ The name of the storage directory for the undo files registered with the drmsqlinit command contains an error.<br>▪ The storage directory for the undo files is not specified with an absolute path.<br>Specify a correct name for the storage directory for undo files, and then re-execute the command. |
| KAVX1107-E | Enter the name of the storage directory for backup-log files: | The system is waiting for the user to enter the name of the storage directory for backup-log files. |
| KAVX1108-W | The specified directory cannot be found.<br>Directory name = *directory-name* | Possible causes are as follows:<br>▪ The specified directory does not exist.<br>▪ The directory was not specified with an absolute path.<br>Re-execute the command with a correct directory name specified. |
| KAVX1202-E | A data file, transaction log file, or storage directory for VDI metafiles belong to the same copy group. | A data file, transaction log file, or storage directory for VDI metafiles belong to the same copy group. These items need to be stored in their own separate copy groups. |
| KAVX1203-E | The specified database cannot perform a backup.<br>Database name = *database-name*<br>Cause = *cause* | The specified database cannot perform backup processing. Confirm that the database is able to perform backup processing, and then re-execute the command. |
| KAVX1204-E | An attempt to back up the specified database has failed because it is stored on a volume from which a directory is mounted.<br>Database name = *database-name* | The specified database is stored in a volume mounted to a directory. Backup processing cannot be performed if the database is stored in a volume mounted to a directory. All files should be stored in a volume assigned to a drive letter. Mount point directories are not supported. |
| KAVX1205-E | An attempt to back up the specified database has failed because no backup target file exists on the RAID storage device.<br>Database name = *database-name* | Not all files that make up the database are stored in the storage subsystem. Backup processing cannot be performed for databases that include files not stored in a storage subsystem. All files need to be stored in a storage subsystem. |

| | | |
|---|---|---|
| KAVX1207-I | Backing up the database... | The database is being backed up. |
| KAVX1209-I | The number of specified databases exceeds the maximum number of databases. | The maximum number of databases that can be specified for one command execution is 64. Specify fewer than 64 databases, and then re-execute the command. |
| KAVX1300-I | Restore processing will now start. | Restore processing has started. |
| KAVX1301-I | Restore processing has finished. | Restore processing finished successfully. |
| KAVX1302-I | Recovery processing will now start. | Recovery processing has started. |
| KAVX1303-I | Recovery processing has finished. | Recovery processing finished successfully. |
| KAVX1304-E | The name of the target definition file for transaction logs specified by the -transact_log_list option is invalid. | Possible causes are as follows:<br>▪ The file does not exist.<br>▪ You do not have read permission for the file.<br>▪ The contents of the file are invalid.<br>▪ The file was not specified with an absolute path.<br>Confirm that the target definition file for transaction logs is specified correctly, and then re-execute the command. |
| KAVX1305-E | The database specified by the target definition file for transaction logs does not exist.<br>Database name = *database-name* | The database specified by the target definition file for transaction logs does not exist. Confirm that the database is specified correctly, and then re-execute the command. |
| KAVX1306-E | A transaction log file specified by the target definition file for transaction logs does not exist.<br>File name = *transaction-log-file-name* | Possible causes are as follows:<br>▪ The transaction log file specified by the target definition file for transaction logs does not exist.<br>▪ The transaction log file was not specified with an absolute path.<br>Confirm that the transaction log file is specified correctly, and then re-execute the command. |
| KAVX1307-E | The specified database information could not be acquired.<br>Database = *database-name* | The backup information about the database associated with the specified backup ID or instance does not exist. Specify a correct database name. |
| KAVX1308-E | The name of the metafile is invalid.<br>Metafile name = *metafile-name* | Possible causes are as follows:<br>▪ No such metafile exists.<br>▪ You do not have read permission for the metafile.<br>Check that the metafile exists, and that you have the appropriate read permission. |
| KAVX1309-E | The database specified by the -transact_log_list option is not a recovery target.<br>Database name = *database-name* | The database specified by the -transact_log_list option exists in the target instance, but it has not yet been specified as a target.<br>Either specify the database as a target, or remove it from the -transact_log_list option. |
| KAVX1310-W | The database has already been recovered. Processing will be skipped.<br>Database name = *database-name* | The user tried to perform recovery processing with the -undo option for a database that has already been recovered. Re-execute restore and recovery processing. |

| | | |
|---|---|---|
| KAVX1311-E | An attempt to recover the SQL Server database failed.<br>Database name = *database-name*<br>Code = *error-code*<br>Cause = *error-cause* | An attempt to recover the SQL Server database failed. Remove the cause of the error, and then re-execute the command. |
| KAVX1312-E | An attempt to recover the transaction log failed.<br>Database name = *database-name*<br>Backup file name = *backup-file-name*<br>Code = *error-code*<br>Cause = *error-cause* | An attempt to recover the transaction log failed. Remove the cause of the error, and then re-execute the command. |
| KAVX1313-I | The cluster resource will now be taken offline. | A cluster resource in the cluster environment will now be taken offline. |
| KAVX1314-I | The cluster resource will now be put online. | A cluster resource in the cluster environment will now be put online. |
| KAVX1315-E | A directory cannot be specified for the mount point. | A string other than a drive letter was specified for the mount point. Specify a drive letter for the mount point. |
| KAVX1316-I | Performing restore pre-processing... | Pre-processing for the restoration is being performed. |
| KAVX1318-I | Performing restore post-processing... | Post-processing for the restoration is being performed. |
| KAVX1322-I | The SQL Server will now start. | The SQL Server will now start because the database restoration finished successfully. |
| KAVX1323-I | The SQL Server was successfully started. | The SQL Server that was stopped due to database restoration has started successfully. |
| KAVX1324-I | The SQL Server will now start in minimal configuration. | The SQL Server will now start in a minimal configuration to restore the master database. |
| KAVX1326-I | SQL Server-dependant services will now start. | The SQL Server-dependant services that have been stopped will start after the SQL Server startup. |
| KAVX1327-I | SQL Server-dependant services were successfully started. | SQL Server-dependant services, which were stopped, started successfully after the SQL Server startup. |
| KAVX1328-I | The SQL Server will now stop. | The SQL Server will stop restoration of a database. |
| KAVX1329-I | The SQL Server has stopped. | The SQL Server has stopped restoration of a database. |
| KAVX1330-I | SQL Server-dependant services will now stop. | The SQL Server-dependant services will stop after the SQL Server terminates. |
| KAVX1331-I | SQL Server-dependant services have stopped. | The SQL Server-dependant services stopped after the SQL Server terminated. |
| KAVX1332-E | You cannot specify the -resync option for the specified backup ID. | Possible causes are as follows:<br>▪ You attempted to restore data by specifying the -resync option even though the data was backed up by specifying the -target option.<br>▪ When the system database and user database exist on the same disk volume, you attempted to restore data by specifying the -resync option even though the data was backed up without specifying the -system option.<br>When the system database and user database exist on the same disk volume, the -system option must be specified to back up data. Data backed up without specifying the -system option cannot be restored. |

| | | |
|---|---|---|
| KAVX1333-E | The list(s) of the transaction logs are not continuous. | Possible causes are as follows:<br>1. The transaction log continuity for the transaction logs to be backed up was lost while the transaction logs were being backed up.<br>2. The log continuity was lost when an attempt was made to display a list of transaction log backup files.<br>Take appropriate action depending on the cause.<br>1. You cannot back up transaction logs when log continuity is lost. Re-execute the drmsqlbackup command, and then execute the drmsqllogbackup command to back up the transaction logs.<br>2. You cannot use the drmsqlrecover command to perform roll-forward processing with transaction-log backup files that are not continuous. In the list of transaction-log backup files, use only continuous ones for roll-forward processing. |
| KAVX1334-E | The backup ID of the specified transaction log is invalid.<br>Backup ID = *log-backup-id* | This message appears if an invalid log backup ID was specified in the drmsqllogbackup command. Re-execute the command with a valid log backup ID specified. |
| KAVX1335-E | The backup record of transaction log could not be obtained. | This message appears if the backup record for transaction-log backup files could not be obtained. Check the transaction-log backup files for the specified backup ID. If they do not have any problems, examine the system log and check whether there is any problem with the OS. |
| KAVX1336-E | The backup ID of the transaction log has reached the maximum limit of the program. | This message appears if the drmsqllogbackup command attempted to generate a new log backup ID when the last log backup ID has already reached the maximum, 9,999. The command cannot back up any more transaction logs by using the specified backup ID as the basis for starting start backup. Execute the drmsqlbackup command to create a new base backup ID. |
| KAVX1337-E | An attempt to update the backup record for the transaction log failed. | This message appears if the backup record of transaction-log backup files could not be written. Examine the transaction-log backup files for the specified backup ID. If they do not have any problems, examine the system log and check whether there is any problem with the OS. |
| KAVX1338-I | The backup file(s) of the transaction log have been deleted. | This message appears when the command successfully deleted transaction-log backup files. |
| KAVX1339-E | The backup file(s) of the transaction log to be processed does not exist. | This message appears when none of the transaction-log backup files matches the conditions specified in the option of the drmlsqllogbackup command. |
| KAVX1340-E | The transaction log cannot be backed up because the backup catalog has only the information of the system database associated with the specified backup ID. | This message appears when only the system database was backed up by the drmsqlbackup command. If only the system database was backed up, you cannot back up the transaction log. |
| KAVX1341-E | The transaction log of the target database cannot be backed up.<br>Database name = *database-name*<br>Cause = *detailed-message* | This message appears when the specified database cannot be backed up. Examine the detailed message and the status of the database. |
| KAVX1342-W | The target database does not exist in SQL Server.<br>Processing will be skipped.<br>Database name = *database-name* | This message appears if the specified database existed when the drmsqlbackup command was executed but did not exist when the transaction log was backed up by using the drmsqllogbackup command. Check whether the specified database exists. |

| | | |
|---|---|---|
| KAVX1343-E | An attempt to delete the backup file of transaction log has failed.<br>Backup file name = *transaction-log-backup-file-name* | This message appears if the drmsqllogbackup command could not delete the transaction-log backup file. Examine the transaction-log backup files for the specified backup ID. If they do not have any problems, examine the system log and check whether there is any problem with the OS. |
| KAVX1344-E | An attempt to back up the transaction log failed.<br>Database name = *database-name*<br>Code = *error-code-for-SQL-server*<br>Cause = *error-message-for-SQL-server* | This message appears if the drmsqllogbackup command could not back up the transaction log. Examine the error code and error message, and take appropriate action. |
| KAVX1345-E | You cannot specify the -resync option for the specified database.<br>Database name = *database-name* | This message appears when the volume that contains the database specified in the drmsqlrestore command also contains databases that have not been backed up. Do not use the -resync option. If this option is specified, the command may damage databases other than the one you want to restore. |
| KAVX1346-E | The transaction log cannot be used for backup because the file name of the database to be backed up contains an invalid character. Processing will be skipped.<br>Database name = *database-name* | This message is output when the transaction log of the database to be backup up contains one of the following characters:<br>– "\", "/", ":", ";", "*", "?", "<", ">", "\|", or ",".<br>Do not use these characters in the names of databases required for backup by the transaction log. |
| KAVX1347-E | A timeout error occurred when starting SQL Server. | This message is output when SQL Server does not start successfully, even after the period specified by the SVC_RETRY_TIME time-out value in the configuration file has elapsed. Check the system log to make sure that no problems exist with either SQL Server or the OS. If no problems are found, change the SVC_RETRY_TIME and SVC_RETRY_WAIT value in the init.conf file, and re-execute the command. |
| KAVX1348-E | A timeout error occurred when stopping SQL Server. | This message is output when SQL Server does not stop successfully, even after the period specified by the SVC_RETRY_TIME time-out value in the configuration file has elapsed. Check the system log to make sure that no problems exist with either SQL Server or the OS. If no problems are found, contact your support center. |
| KAVX1349-E | The metafile already exists.<br>File name = *file-name* | This message is output when backup is performed using the drmsqlbackup command, and an attempt to create a metafile fails because a metafile with the same name already exists. Use the drmsqlinit command to change the storage directory for the metafile, and execute this command again. |
| KAVX1350-E | The transaction log of the system database cannot be backed up. | This message is output when the drmsqllogbackup command is executed and a system database is specified as the database whose transaction log is to be backed up. Transaction logs of system databases cannot be backed up. |
| KAVX1351-W | The database has not been backed up. Processing will be skipped.<br>Database name = *database-name* | This message appears when the drmsqllogbackup command has not been used to back up the transaction log. |
| KAVX1352-E | The transaction log has not been backed up. | This message appears when the rmsqllogbackup command has not been used to back up the transaction log. Back up the transaction log and then re-execute the command. |
| KAVX1353-E | You cannot specify the nochk_host option for the system database. | This message appears when the system database is specified with the -nochk_host option of the drmsqlrestore command. Do not restore the system database. |

| | | |
|---|---|---|
| KAVX1354-I | The drmsqlrecover command is running. | This message indicates that the drmsqlrecovertool command is currently executing the drmsqlrecover command. |
| KAVX1355-I | There is a database with which recovery is not completed.Does it end? | This is a confirmation message when you click the Exit button while the database recovery is being operated with the online specification of the drmsqlrecovertool command. |
| KAVX1356-W | This file already exists in a list. | A file that the user attempted to add to a list with the drmsqlrecovertool command was already in the list. Do not attempt to add the same log file twice, since it cannot be recovered twice. |
| KAVX1357-W | A network file cannot be added. | A file that the user attempted to add to a list with the drmsqlrecovertool command was on a network. Transfer the file to a local disk. |
| KAVX1358-E | The drmsqlrecover command failed. | An error occurred in the drmsqlrecover command that was started by the drmsqlrecovertool command.<br>Check output.log to resolve the cause of the drmsqlrecover command failure. Then, re-do the procedure from the restore step. |
| KAVX1359-E | The drmsqlrecover command was not able to be started. | Possible causes are as follows:<br>▪ A failure occurred when the drmsqlrecovertool command attempted to start the drmsqlrecover command.<br>▪ The drmsqlrecovertool command failed to create a temp file when executing the drmsqlrecover command.<br>Take appropriate action, depending on the cause.<br>▪ Confirm that the drmsqlrecover command exists.<br>▪ Allocate resources sufficient to start the OS.<br>▪ Configure access settings appropriately if you do not have the proper access or write permissions. |
| KAVX1360-E | The item was not able to be added to Transaction log backup list. | The drmsqlrecovertool command failed when an item was being added to a list. Either the limit for the number of items in the list was exceeded, or there were insufficient OS resources. Reduce the number of items or allocate resources, and then re-execute. |
| KAVX1361-E | The drmsqlrecovertool command has already started. | The drmsqlrecovertool command is running. Stop the operating drmsqlrecovertool command, and then re-execute it. |
| KAVX1400-I | Updating database information now... | The database information is being updated. |

## 8.4 KAVX1500-E - KAVX1901-E (Exchange Server)

Table 8.4 lists and describes Protection Services messages KAVX1500-E to KAVX1900-E and provides corrective actions that you can take in response to the messages, if appropriate.

**Table 8.4 KAVX1500-E - KAVX1901-E**

| Message ID | Message Text | Description and Recommended Action |
|---|---|---|
| KAVX1500-E | The specified storage group does not exist in Exchange Server.<br>Storage group name = *storage-group-name* | The specified storage group does not exist in Exchange Server. Check that the specified storage group name is correct, and then re-execute the command. |
| KAVX1501-E | An error occurred during Exchange Server processing.<br>Processing = *processing*<br>Cause = *error-cause* | An error occurred during Exchange Server processing. Refer to the Exchange Server documentation, remove the cause of the error, and then re-execute the command. |
| KAVX1502-E | An error occurred during Exchange Server processing.<br>Processing = *processing*<br>Code = *error-code* | An error occurred during Exchange Server processing. Refer to the Exchange Server documentation, remove the cause of the error, and then re-execute the command. |
| KAVX1503-E | An error occurred during Exchange Server processing.<br>Processing = *processing*<br>Code = *error-code*<br>Cause = *error-cause* | An error occurred during Exchange Server processing. Refer to the Exchange Server documentation, remove the cause of the error, and then re-execute the command. |
| KAVX1504-E | An error occurred during Exchange Server processing.<br>Processing = *processing*<br>Cause = *error-cause* | An error occurred during Exchange Server processing. Refer to the Exchange Server documentation, remove the cause of the error, and then re-execute the command. |
| KAVX1505-E | The user lacks appropriate permission to use Exchange Server.<br>Processing = *processing*<br>Cause = *error-cause* | A user who does not have permission to use Exchange Server executed a command. Refer to the Exchange Server documentation, make sure that the user has the appropriate permissions, and then re-execute the command. |
| KAVX1506-E | The user lacks appropriate permission to use Exchange Server.<br>Processing = *processing*<br>Code = *error-code* | A user who does not have permission to use Exchange Server executed a command. Refer to the Exchange Server documentation, make sure that the user has the appropriate permissions, and then re-execute the command. |
| KAVX1507-E | The user lacks appropriate permission to use Exchange Server.<br>Processing = *processing*<br>Code = *error-code*<br>Cause = *error-cause* | A user who does not have permission to use Exchange Server executed a command. Refer to the Exchange Server documentation, make sure that the user has the appropriate permissions, and then re-execute the command. |
| KAVX1508-E | Multiple storage groups exist. | Multiple storage groups exist in Exchange 2000 Server. Delete storage groups that will not be used. |
| KAVX1509-E | Exchange Server has not yet been installed on this system. | Exchange Server has not been installed on this system. Install Exchange Server on this system. |

| | | |
|---|---|---|
| KAVX1510-E | An attempt to mount the database failed.<br>Storage group name = *storage-group-name*<br>Information store name = *information-store-name* | An attempt to mount the database failed, after either backup or restore processing. Make sure that the following services have stopped:<br>▪ IIS Admin Service<br>▪ System Attendant Service<br>▪ Information Store Service |
| KAVX1511-E | An attempt to dismount the database failed.<br>Storage group name = *storage-group-name*<br>Information store name = *information-store-name* | An attempt to dismount the database failed. Neither backup nor restore processing could be performed. Make sure that the following services have stopped:<br>▪ IIS Admin Service<br>▪ System Attendant Service<br>▪ Information Store Service |
| KAVX1512-E | The same storage group name is being used on two or more Exchange virtual servers which have the same cluster configuration node set as a priority node.<br>Node name = node-name<br>Storage group name = *storage-group-name* | If two or more Exchange virtual servers in the cluster configuration set the same node as a priority node, these servers will use the same storage group name. In this case, you will need to specify a separate storage group name for each Exchange virtual server. |
| KAVX1513-E | The status of the cluster group on the Exchange virtual server is invalid.<br>Cluster group name = cluster-group-name | The command could not be executed because the cluster group on Exchange Virtual Server is not in the online status. Correct this problem on Exchange Virtual Server, and then re-execute the command. |
| KAVX1514-E | An attempt to obtain the Exchange Server information failed. | This message appears if an error occurs during acquisition of the Exchange Server configuration information. Check whether the DNS server and domain controller for the domain where Exchange Server is installed are normally operating. If they do not have any problems, refer to the documentation for Exchange Server to check whether Exchange Server is normally operating. |
| KAVX1515-E | The information of the cluster resource associated with the storage group does not exist.<br>Storage group name = *storage-group-name* | This message appears when a cluster system is created but the cluster resource information for the indicated storage group has not been registered. Re-execute the command after you use the drmclusinit command to register the cluster resource information. |
| KAVX1516-E | No virtual host name has been specified. | This message is output when, in a cluster environment, no virtual host name is specified in the environment variable DRM_HOSTNAME. Set the name of the virtual host in the environment variable DRM_HOSTNAME, and execute the command again. |
| KAVX1517-E | The virtual host name is not a valid Exchange virtual server name.<br>Virtual host name = *virtual-host-name* | This message is output when, in a cluster environment, the virtual host name specified in the environment variable DRM_HOSTNAME is not a valid Exchange virtual server name. Enter the name of a virtual host that exists on the Exchange Server in the environment variable DRM_HOSTNAME, and execute the command again. |
| KAVX1518-I | The Information Store Service will now start. | This message is output to notify you that the Information Store Service is starting. |
| KAVX1519-I | The Information Store Service was started successfully. | This message is output when the Information Store Service has started successfully. |

| | | |
|---|---|---|
| KAVX1520-E | The specified storage group is the recovery storage group.<br>Storage group name = *storage-group-name* | A recovery storage group was specified for the storage group. Make sure the storage group name, and then re-execute the command. |
| KAVX1550-E | An attempt to obtain the information for verification of the specified file failed.<br>Item = *item-name*<br>Processing = *processing* | An attempt to obtain information needed to execute the check tool and to verify the definition file has failed. For details about the cause of the error, see 7.5 Detailed messages. |
| KAVX1551-E | An attempt to obtain the information for verification of the specified file failed.<br>Item = *item-name*<br>Processing = *processing*<br>Cause = *cause* | An attempt to obtain information needed to verify the items of the definition file has failed. For details about the cause of the error, see 7.5 Detailed messages. |
| KAVX1552-E | The specified Exchange Server has not been found.<br>Exchange Server name = *Exchange-server-name* | If the system displays this message when executing the check tool EX_DRM_EXG_DEF_CHECK, verify the Exchange server name that is specified in an item (DB_SERVER_NAME) of the definition file. Additionally, ensure that the Exchange server specified in the definition file actually exists. If the system displays this message when executing the extended command EX_DRM_EXG_BACKUP, verity that the Exchange server that is specified by -hostname option actually exists. |
| KAVX1553-E | The storage group specified in the definition file has not been found.<br>Exchange Server name = *Exchange-server-name*<br>TARGET_NAME = *storage-group-name* | Verify the storage group name that is specified in an item (TARGET_NAME) of the definition file. Additionally, ensure that the storage group specified in the definition file actually exists. |
| KAVX1554-E | The characters specified in definition file are invalid for a storage group name.<br>TARGET_NAME = *character-string* | Verify the storage group name that is specified in an item (TARGET_NAME) of the definition file. Additionally, ensure that the storage group specified in the definition file actually exists. |
| KAVX1555-E | Exchange Server has not yet been installed on this system. | Exchange Server has not yet been installed on the appropriate machine. Install Exchange Server on the appropriate machine. |
| KAVX1556-E | A value specified in definition file is invalid.<br>Item = *item-name*<br>Current value = *current-value*<br>Required value = *value-to-be-specified* | The value of an item specified in the definition file is invalid. Verify the definition file according to the displayed message to modify the value of the item, and then re-execute the check tool. |
| KAVX1600-I | Backup processing will now start. | Backup processing has started. |
| KAVX1601-I | Backup processing has finished. | Backup processing finished successfully. |
| KAVX1602-E | A transaction log file is being stored in the same copy group in which an information store is stored.<br>Storage group name = *storage-group-name* | ▪ At the execution time of the backup command On a server from which the secondary volume cannot be accessed, a transaction log file is being stored in the same copy group as an Exchange configuration data file (*.edb or *.stm). Separate the following: the copy group in which the information store is stored, and the copy group in which the log files are stored.<br>▪ At the execution time of the restore command<br>A transaction log file is being stored in the same copy group as a data file (*.edb or *.stm). Retry the command without specifying the -recovery option. |

| | | |
|---|---|---|
| KAVX1603-E | An attempt to delete a transaction log file has failed.<br>Storage group name = *storage-group-name*<br>Transaction log file name = *storage-group-name* | An error occurred when an attempt was made to delete a transaction log file. Either delete the transaction log file manually, or specify the -transact_log_del option and perform backup again. |
| KAVX1604-E | A transaction log file could not be deleted.<br>Storage group name = *storage-group-name* | An error occurred during deletion processing of a transaction log file, and the transaction log file of the corresponding storage group could not be deleted. Specify the -transact_log_del option and perform backup processing again. |
| KAVX1605-E | The cluster resource of Exchange depends on the physical disks to be backed up.<br>Exchange virtual server name = *virtual-server-name* | This message appears when you executed the drmexgbackup command with the -transact_log_del option, and the command found that Microsoft Exchange System Attendant or Microsoft information store, which was a cluster resource, depended on the backup-target disk resource for storing the information store objects. Re-execute the drmexgbackup command with the -c online option specified. Next, change the configuration so that Microsoft Exchange System Attendant or Microsoft information store cluster resource does not depend on a disk to be backed up. Then, re-execute the command. |
| KAVX1607-E | The Storage group was not online backuped because the specified circulation log was set up.<br>Storage group name = *storage-group-name* | This message appears when either the -mode option was omitted or when the -mode online option was used in an attempt to back up a storage group set in the circulation log. If you are performing online backup, clear the circulation log setting and re-execute the command. If you are performing offline backup, re-execute the command, specifying the -mode cold option. |
| KAVX1650-I | The checksum of the Exchange database file was confirmed.<br>Storage group name = *storage-group-name* | This message appears when the checksum of the Exchange database file is correct. |
| KAVX1651-E | A file needed to execute the ESEUTIL utility has not been copied. | This message appears when a file needed to execute the ESEUTIL utility has not been copied to the server on which the command is executing. Check the Exchange Server documentation, copy the required files, and then re-execute the command. |
| KAVX1652-E | The checksum of the Exchange database file is invalid.<br>Storage group name = *storage-group-name*<br>Information store name = *information-store-name*<br>File name = *file-name* | This message appears when a fault is detected in the checksum for an Exchange database file. Check the Exchange Server documentation, and take the appropriate recovery measures. |
| KAVX1700-I | Restore processing will now start. | Restore processing will now start. |
| KAVX1701-I | Restore processing has finished. | Restore processing finished successfully. |
| KAVX1702-E | When the circulation log is to be used, set the -recovery option when restoring.<br>Storage group name = *storage-group-name* | When using the circulation log, do not specify the -recovery option if restore processing is to be performed. You cannot restore by roll-forward if the circulation log is being used. Re-execute the command without specifying the -recovery option. |
| KAVX1703-E | Inconsistencies exist in the sequence of the transaction log files.<br>Storage group name = *storage-group-name* | Possible causes are as follows:<br>▪ In the .edb file and .stm files, the LogSignature of the file with the smallest generation number in the final integrated log is not consistent with the signature of the transaction log file corresponding to the generation number.<br>▪ There is a discontinuity or inconsistency in the signatures in the generated transaction log file.<br>In this case, contact your support center. |

| | | |
|---|---|---|
| KAVX1704-I | An attempt to execute the restore command failed.<br>Storage group name = *storage-group-name*<br>Storage group status = *storage-group-status* | When restore processing fails, the status of the information store is displayed. |
| KAVX1705-I | Creating temporary files... | A temporary file is being created for one of the following types of files in the storage group to be restored:<br>▪ Data files (*.edb or *.stm)<br>▪ Transaction log files (*.log) |
| KAVX1706-E | An attempt to create a temporary restore file has failed. | An attempt is being made to create a temporary file for one of the following types of files in the storage group to be restored:<br>▪ Data files (*.edb or *.stm)<br>▪ Transaction log files (*.log)<br>Re-execute the command without specifying the -recovery option. |
| KAVX1707-W | An attempt to delete a temporary file has failed.<br>Temporary file = *temporary-file* | An attempt to delete a temporary file has failed. Delete the temporary file manually. |
| KAVX1708-E | The configuration of storage group has changed since it was backed up.<br>Storage group name = *storage-group-name* | Restore processing cannot be performed because the configuration of the storage group is different from the version stored during backup processing. |
| KAVX1709-E | The copy group contains objects that have not been backed up.<br>Storage group name = *storage-group-name* | A backup could not be performed because both files related to and files unrelated to the storage group to be backed up exist in the same copy group. Specify all of the storage groups within the same copy group, and then re-execute the command. |
| KAVX1710-E | The cluster resource of Exchange is dependent on the physical disk to be restored.<br>Exchange virtual server name = *virtual-server-name* | The system cannot perform restore specifying the -recovery option because the system attendant service or information store service, which is the cluster resource, requires the use of the disk storing the information store object to be restored. Execute restore using one of the following methods:<br>▪ Execute restore without specifying the -recovery option.<br>▪ Modify so that the system attendant service or information store service, which is the cluster resource, does not require use of the disk to be restored, and then re-execute restore. |
| KAVX1711-E | The backup record for the specified storage group cannot be obtained.<br>Storage group name = *storage-group-name* | This is a message output if the specified storage group does not exist in the backup data with the specified backup ID when the drmexgrestore command is executed with the backup ID and storage group.<br>Re-execute the command with a correct backup ID and storage group name specified. |
| KAVX1712-E | The -recovery option has not been specified with the specified backup ID. | The backup data that needs the roll-forward recovery has been performed without using the -recovery option. Execute the drmexgrestore command together with the -recovery option. |
| KAVX1713-E | The Storage group was not recovery because the specified transaction log does not exist.<br>Storage group name = *storage-group-name* | This message appears when the transaction log file for the storage group to be recovered does not exist. Check the Exchange configuration and restart from backup, or restore without specifying the -recovery option. |
| KAVX1800-W | The information store has already been dismounted.<br>Storage group name = *storage-group-name*<br>Information store name = *information-store-name* | The database was already dismounted during backup or restore processing. |

| | | |
|---|---|---|
| KAVX1801-W | The information store has already been mounted.<br>Storage group name = *storage-group-name*<br>Information store name = *information-store-name* | The database was already mounted during backup or restore processing. |
| KAVX1802-E | Inconsistencies exist in the information store.<br>Storage group name = *storage-group-name*<br>Information store name = *information-store-name* | Either the statuses of the .edb and .stm files are inconsistent, or are not the same as LastConsistent. Refer to the Exchange Server documentation, confirm that the information store can be mounted or dismounted successfully, and then re-execute the command. |
| KAVX1803-E | Inconsistencies exist between the transaction log files and the checkpoint files.<br>Storage group name = *storage-group-name* | The generation number of the transaction file indicated in the checkpoint file (the .chk file in the system path) is not the latest transaction log file. Refer to the Exchange Server documentation, confirm that the information store can be mounted or dismounted successfully, and then re-execute the command. |
| KAVX1804-E | The signature of the information store is invalid.<br>Storage group name = *storage-group-name*<br>Information store name = *information-store-name* | The signature of the information store does not match DBSignature of either the .edb file or the .stm file. A data file in the information store may have been destroyed. Contact your support center for more information. |
| KAVX1805-I | The information store will now be dismounted.<br>Storage group name = *storage-group-name* | The information store will now be dismounted so that backup or restore processing can be performed. |
| KAVX1806-I | The information store will now be mounted.<br>Storage group name = *storage-group-name* | The information store will now be mounted, since either backup or restore processing has been performed. |
| KAVX1807-E | The target database file does not exist. | Possible causes are as follows:<br>1. You specified the -target option, and the specified storage group did not include an information store.<br>2. No storage groups exist on Exchange Server if you have not specified the -target option, or storage groups that contain information stores do not exist.<br>Perform one of the following actions depending on the cause of the error:<br>1. If you specify the -target option, specify a storage group that includes an information store, and then re-execute the command.<br>2. If you do not specify the -target option, make sure that at least one storage group that contains an information store, and then re-execute the command. |
| KAVX1900-I | The dictionary map file was updated. | This message is displayed to notify you when processing ends normally after a command is executed with the -refresh option. |
| KAVX1901-E | The specified backup record does not exist. | No information can be displayed because a backup has not yet been performed. Perform backup processing, and then re-execute the command. |

## 8.5 KAVX2500-E - KAVX2525-E

Table 8.5 lists and describes Protection Services messages KAVX2500-E to KAVX2525-E and provides corrective actions that you can take in response to the messages, if appropriate.

**Table 8.5 KAVX2500-E - KAVX2525-E**

| Message ID | Message Text | Description and Recommended Action |
|---|---|---|
| KAVX2500-E | You can not assign the same directory name for AP_FILE_DIR and DB_DATA_FILE_DIR.<br>Directory =*directory-name* | In the definition file, the same directory name is specified for both AP_FILE_DIR and DB_DATA_FILE_DIR. Check the contents of the definition file, specify different directory names for AP_FILE_DIR and DB_DATA_FILE_DIR, and then re-execute the check tool. |
| KAVX2501-E | You can not assign the same directory name for AP_FILE_DIR and BK_DATA_FILE_DIR.<br>Directory = *directory-name* | In the definition file, the same directory name is specified for both AP_FILE_DIR and BK_DATA_FILE_DIR. Check the contents of the definition file, specify different directory names for AP_FILE_DIR and BK_DATA_FILE_DIR, and then re-execute the check tool. |
| KAVX2502-E | You do not have permission to execute this command. | The user does not have permission to execute the specified command. Have the command re-executed by a user who has permission. |
| KAVX2503-E | An attempt to execute the *command-name* command failed.<br>Cause = *cause* | Command execution failed within an extended command. Check to see if the command indicated in the message is executable and then re-execute the extended command. |
| KAVX2504-E | Duplicate copy groups present in the specified file.<br>Copy group = *Copy group* | The system ignores the duplicate copy group in the copy group batch definition file. Correct the copy group batch definition file so that no copy group file name is duplicated, then re-execute the check tool. |
| KAVX2505-E | An attempt to transmit files failed.<br>Cause = *cause*<br>FTP server = *FTP-server-name*<br>File or directory name = *target-file-name-or-directory-name* | A file transfer failed at the FTP server. Possible causes are as follows:<br>When this message is displayed during file transmission:<br>▪ The specified directory does not exist on the FTP server.<br>▪ The user who executed the command did not have write permission for the specified directory on the FTP server.<br>▪ There is not enough space in the specified directory on the FTP server.<br>When this message is displayed during file reception:<br>▪ The specified directory does not exist on the FTP server.<br>▪ The user who executed the command did not have read permission for the specified directory on the FTP server.<br>Check the above causes. If there is no problem, make sure that the network status is normal. |
| KAVX2506-E | An attempt to transmit files failed.<br>Cause = *cause*<br>File or directory name = *target-file-name-or-directory-name* | A file transfer failed at an FTP client. Possible causes are as follows:<br>When this message is displayed during file reception:<br>The specified directory does not exist on the local server.<br>▪ The user who executed the command did not have the write permission for the specified directory on the local server.<br>▪ There is not enough space in the specified directory on the local server.<br>When this message is displayed during file transmission:<br>▪ The specified directory does not exist on the local server.<br>▪ The user who executed the command did not have read permission for the specified directory on the local server.<br>Check the above causes. If there is no problem, make sure that the network status is normal. |

| | | |
|---|---|---|
| KAVX2507-E | The specified file path is invalid.<br>Target file = *file-name* | The path to the definition file is not specified correctly. Make sure that the definition file is specified by its absolute path and then re-execute the command. |
| KAVX2508-E | The specified file does not exist.<br>Target file = *file-name* | The specified definition file does not exist. Make sure that the specified definition file exists. |
| KAVX2509-E | The copy group specified in the file does not exist.<br>Copy group = *copy-group-name* | The copy group name specified in the copy group batch definition file does not exist in the Protection Services dictionary map. Use the drmcgctl command to output a list of copy groups registered in the Protection Services dictionary map, and then check that the specified copy group exists in the list. |
| KAVX2510-E | The copy group specified in the file is invalid.<br>Copy group = *copy-group-name* | The specification format of the copy group name is invalid in the copy group batch definition file. Specify copy group name left-justified and then re-execute the command. |
| KAVX2511-E | The mount point directory or target definition file of mount point directory specified in the file does not exist.<br>INSTANCE_NAME = *mount-point-directory-name-or-mount-point-batch-definition-file-name* | The mount point directory name or mount point batch definition file name specified in the operation definition file does not exist. Make sure that the specified mount point name or mount point batch definition file exists and can be referenced. |
| KAVX2512-E | The backup target files or directories specified in the file does not exist.<br>INSTANCE_NAME = *file-name-or-directory-name* | The file name or directory name specified as being subject to backup in the operation definition file does not exist. Make sure that the specified file or directory name subject to backup exists and can be referenced. |
| KAVX2513-E | The backup target files or directories specified in the file does not exist in the mount point directory specified in the same file.<br>INSTANCE_NAME = *mount-point-directory-name-or-mount-point-batch-definition-file-name*<br>TARGET_NAME = *file-name-or-directory-name* | The file name or directory name specified as being subject to backup in the operation definition file does not exist in the mount point directory specified in the operation definition file. Set the mount point directory that contains the file name or directory name subject to backup, make sure that the file or directory to be backed up can be referenced, and then re-execute the command. |
| KAVX2514-I | The procedure of command-name command will now continue on another window.<br>Confirm the message displayed on the window. Enter required value when the window prompts input. | This message is displayed when a command requiring message monitoring or an interactive operation on the screen is started in a separate window within an extended command. Check the message displayed in the window and enter information, if necessary. If the command does not need to wait for an entry, the window closes automatically upon completion of the processing. |
| KAVX2515-I | The procedure of command-name command on another window will now end.<br>This procedure will resume on this window. | This message indicates that the command that was started within an extended command and that was executing in a separate window has terminated. |
| KAVX2516-E | The directory name of Item specified in the file is invalid.<br>Item = *item-name*<br>Directory = *directory-name*<br>Operation ID = *operation ID* | The subdirectory corresponding to the value specified in the operation ID does not exist in the directory written in the operation definition file. Make sure that the item displayed in this message conforms to the rules described in section 3.3.2, check the contents of the operation definition file, and then re-execute the checking tool. |
| KAVX2517-E | The server name specified in the file is conflict with the value or not exist in the configuration file.<br>DB_SERVER_NAME = *value-of-DB_SERVER_NAME-in-definition-file*<br>*Configuration file = configuration-file-name* | The value of DB_SERVER_NAME in the definition file does not match the server name (the value of DRM_HOST_NAME) defined for DRM_DB_PATH in the init.conf file, the configuration file provided by Protection Services. Check the contents of the definition file for the extended command and the init.conf file, change the value of DB_SERVER_NAME, and then re-execute the check tool. When changing a value in the init.conf file, follow the environment setup procedure for Protection Services. |

| | | |
|---|---|---|
| KAVX2518-E | The content of the specified copy group target definition file is invalid.<br>Filename = *file-name* | The copy group has not been set in the copy group batch definition file. Register the copy group name in the copy group batch definition file and then re-execute the check tool. |
| KAVX2519-E | The mount point in the mount point batch definition file specified in the definition file does not exist.<br>Name of mount point batch definition file = *file-name*<br>Mount point name = *mount-point-name* | The mount point registered in the mount point batch definition file does not exist. Check the mount point batch definition file and then re-execute the command. |
| KAVX2520-E | A mount point is missing in the mount point batch definition file specified in the definition file.<br>Name of mount point batch definition file = *file-name* | No mount point has been registered in the mount point batch definition file. Register a mount point in the mount point batch definition file and then re-execute the command. |
| KAVX2521-E | An attempt to obtain the information described in the configuration file failed.<br>Cause = *cause*<br>Configuration file = *configuration-file-name* | Required information could not be obtained from the Protection Services configuration file. Check that the configuration file displayed in the message exists. If the file exists, check the contents of the file. |
| KAVX2522-W | The path specified in the file contains extra '/'. These characters are ignored.<br>Item = *item-name*<br>Directory = *directory-name* | The specified directory contains an extra slash (/). Eliminate the extra slash (/) from the directory name displayed in the message, and then re-execute the check tool. |
| KAVX2523-E | The value specified in the file contains non-numeric characters.<br>Item = *item-name*<br>Value = *item-value* | In the definition file, the value of the item displayed in the message contains a non-numeric character. Specify the value using the numeric characters only, and then re-execute the check tool. |
| KAVX2524-E | The backup ID cannot be found in input. | Information about the backup ID created by Protection Services could not be obtained. See the system log to check whether an error has occurred in the OS. |
| KAVX2525-E | Syntax of the contents in the specified file is wrong.<br>Target file = *file-name* | A syntax error exists in the entries coded in the definition file. Check the entries in the definition file, correct the syntax error, and then re-execute the check tool. |
| KAVX2800-E | The storage group specified in the definition file is the recovery storage group.<br>Exchange server name = *Exchange-server-name*<br>TARGET_NAME = *storage-group-name* | A recovery storage group was specified in TARGET_NAME of the definition file.<br>Remove the recovery storage group name from the storage group names specified in TARGET_NAME of the definition file. |

## 8.6 Detailed Messages

Table 8.6 lists and describes the detailed messages displayed as causes of the Protection Services messages and provides corrective actions that you can take in response to the messages, if appropriate.

**Table 8.6 Detailed Messages**

| Message ID | Message Text | Description/Recommended Action |
|---|---|---|
| DRM-10000 | An error occurred during exclusive processing. | An error occurred because another command was executing at the time of command execution even though exclusive processing (locking) was specified. Wait a while and then re-execute the command. |
| DRM-10001 | The specified file is being used. | Since a file to be restored is being used, restore processing cannot continue. Wait a while, and then re-execute the command. |
| DRM-10002 | An internal error occurred. | An unknown internal error occurred because the information in a dictionary map file or backup catalog has lost conformity or was damaged. Or, an unknown internal error occurred duing execution of an OS system call. Check the operating environment of Protection Services in the following order:<br>▪ Make sure that the CCI instance to be communicated with the CCI instance specified in the HORCMINST parameter of the Protection Services configuration definition file (DEFAULT.dat) has already started.<br>▪ Make sure that the instance number specified in the HORCMINST parameter of the Protection Services configuration definition file (DEFAULT.dat) is correct.<br>▪ Make sure that the CCI configuration definition file (horcmn.conf) is correct.<br>When there is no problem in the operating environment of Protection Services, refer to Chapter 7 (Troubleshooting), collect data, and then contact the Support Center. To recover, you must uninstall and re-install Protection Services. |
| DRM-10003 | An attempt to obtain a backup ID failed. | The system could not obtain a backup ID because the information in a dictionary map file or a backup catalog became mismatched or corrupted. Refer to Chapter 7 (Troubleshooting), collect data, and then contact the Support Center. To recover, you must uninstall and then re-install Protection Services. |
| DRM-10004 | The backup record associated with the specified backup ID does not exist. | During an operation such as restoration or displaying backup record, the backup record associated with the backup ID that was specified by the command did not exist. Specify the correct backup ID and then re-execute the command. |
| DRM-10008 | The pair status of the copy group is invalid. | The command cannot be executed because the pair status of the copy group is invalid. Possible causes are as follows:<br>▪ The pair status of the copy group became invalid because a program other than Protection Services changed the status of the paired volume.<br>▪ The pair status of the copy group is PAIR.<br>Re-create the dictionary map file (drmfsdisplay, drmsqldisplay, or drmexgdisplay command), and then re-execute the command. Or, use the pairsplit command provided by CCI to change the pair status of the copy group to PSUS, and then execute the command. |
| DRM-10009 | An attempt to resynchronize the copy group(s) failed. | During backup or restore processing, the system failed to resynchronize the copy group(s). Check whether the setup of CCI is correct. If the setup is correct, examine the log information of CCI and check whether there is any problem. |
| DRM-10010 | RAID configuration information could not be obtained. | A command of CCI could not obtain the RAID configuration information. Check whether the setup of CCI is correct. If the setup is correct, examine the log information of CCI and check whether there is any problem. |

| | | |
|---|---|---|
| DRM-10011 | A timeout error occurred. | During backup or restore processing, a timeout error occurred because resynchronization of a copy group took an excessive amount of time. Wait a while, and then re-execute the command. |
| DRM-10012 | The target file system cannot be locked. | During online backup processing, an error occurred in the lock processing for a file system in VxFS of UNIX, Examine the Protection Services trace log files and the system log, and check whether any output messages show errors in the file system. |
| DRM-10013 | An attempt to obtain the installation path failed. | The system could not obtain the installation path of Protection Services because Protection Services was not installed correctly in the Windows system. First uninstall Protection Services, and then re-install it. |
| DRM-10014 | The specified copy group does not exist. | The copy group specified in the dictionary map file did not exist at the time when the drmcgctl command or the drmresync command was executed. Re-create the dictionary map file (drmfsdisplay, drmsqldisplay, or drmexgdisplay command), and then re-execute the command. |
| DRM-10015 | An attempt to obtain RAID information failed. | The system could not obtain the RAID configuration information when updating the dictionary map file. Check whether the setup of CCI is correct. If the setup is correct, examine the log information of CCI and check whether there is any problem. |
| DRM-10016 | An attempt at mounting failed. | During backup or restore processing, an attempt at mounting failed because the mount point directory did not exist. Check the operating environment of Protection Services with the following procedure:<br>▪ During the backup/restore processing on the primary volume, neither the mount operation nor the tape backup/restore operation was executed on the secondary volume.<br>▪ Check whether the specification of the mount point directory is correct.<br>If the setup of the mount point directory is correct, examine the system log and check whether there is any problem with the OS. |
| DRM-10017 | The specified path has already been mounted. | Processing could not continue because the specified disk to be mounted was already mounted at the time of backup or restore processing. Unmount the disk that has been mounted, and then re-execute the command. If the same error still occurs, examine the system log and check whether there is any problem with the OS. |
| DRM-10018 | The specified path is invalid. | The path name specified for backup with the -target option or -f option is invalid. Specify the correct path name and then re-execute the command. |
| DRM-10019 | An attempt at unmounting failed. | Check the operating environment of Protection Services in the following order:<br>▪ Make sure that the CCI instance to be communicated with the CCI instance specified in the HORCMINST parameter of the Protection Services configuration definition file (DEFAULT.dat) has already been started.<br>▪ Make sure that the instance number specified in the HORCMINST parameter of the Protection Services configuration definition file (DEFAULT.dat) is correct.<br>▪ Make sure that the CCI configuration definition file (horcmn.conf) is correct.<br>If there is no problem in the Protection Services operating environment, check the following items.<br>▪ Determine if a mount operation or tape backup/tape restore operation for the secondary volume was performed during the backup or restore processing for the primary volume.<br>▪ Determine if a disk subject to unmounting was being used.<br>▪ Determine if a work directory for executing commands was placed on a disk subject to unmounting.<br>The unmounting operation cannot be performed if the work directory is placed on a disk subject to unmounting. If the unmounting operation is specified appropriately, examine the system log and check whether there is any problem with the OS. |

| | | |
|---|---|---|
| DRM-10020 | An attempt to generate a pair of the copy group failed. | During backup or restore processing, the system failed to generate a pair of the copy group. Check whether the setup of CCI is correct. If the setup is correct, examine the log information of CCI and check whether there is any problem. |
| DRM-10021 | An attempt to resynchronize the pair of the copy group failed. | During backup or restore processing, the system failed to resynchronize the pair of the copy group. Check whether the setup of CCI is correct. If the setup is correct, examine the log information of CCI and check whether there is any problem. |
| DRM-10022 | An attempt to split the pair of the copy group failed. | During backup or restore processing, the system failed to split the pair of the copy group. Check whether the setup of CCI is correct. If the setup is correct, examine the log information of CCI and check whether there is any problem. |
| DRM-10023 | An attempt to reconfigure the disk information failed. | During backup or restore processing, the system failed to reconfigure the logical volume manager's disk information. If the message was displayed during mounting/unmounting of the secondary volume or during tape backup/restore processing, make sure that no process is using the secondary volume to be used or the disk group containing the secondary volume.<br>If the message was displayed during backup/restore processing between volumes, make sure that the physical disk volume used for backup or restore processing belongs to the rootdg disk group.<br>If the physical disk belongs to the rootdg disk group, delete the physical disk for backup or restore processing from the rootdg disk group. If the physical disk does not belong to the rootdg disk group, examine the logical volume manager's trace log and check whether the error was output to the logical volume manager. |
| DRM-10024 | An attempt to lock the file system failed. | During backup or restore processing, the system failed to lock the file system (VxFS of UNIX). Examine the Protection Services trace log file and the UNIX system log, and check whether messages were output that show errors in the file system. |
| DRM-10025 | An attempt to unlock the file system failed. | During backup or restore processing, the system failed to unlock the file system (VxFS of UNIX). Examine the Protection Services trace log file and the UNIX system log, and check whether messages were output that show errors in the file system. |
| DRM-10026 | The status of the copy group could not be obtained. | During backup or restore processing, the system could not obtain the status of the copy group. The status of the copy group cannot be obtained when:<br>▪ The instance to be backed up has stopped.<br>▪ The copy group containing the object to be backed up is managed by multiple CCI instances.<br>Check the operating environment of Protection Services in the following order:<br>▪ Make sure that the CCI instance to be communicated with the CCI instance specified in the HORCMINST parameter of the Protection Services configuration definition file (DEFAULT.dat) has already been started.<br>▪ Make sure that the instance number specified in the HORCMINST parameter of the Protection Services configuration definition file (DEFAULT.dat) is correct.<br>▪ Make sure that the CCI configuration definition file (horcmn.conf) is correct.<br>When there is no problem in the operating environment of Protection Services, check whether the setup of CCI or definition file is correct. If the setup is correct, examine the log information of CCI and check whether there is any problem.<br>Depending on the cause where the pair status of the copy group cannot be obtained, take the following actions:<br>▪ Start the instance if the instance to be backed up has stopped.<br>▪ When the copy group containing the object to be backed up is managed by multiple CCI instances, modify the contents of the definition file. |

| | | |
|---|---|---|
| DRM-10027 | Two or more logical disks exist on one physical disk. | Backup cannot be performed because there are two or more logical disks on the physical disk that has the logical disk corresponding to the mount point directory to be backed up. Use a logical volume manager to change the volume configuration. |
| DRM-10028 | The specified file or directory does not exist on the RAID device. | The path name of a file or a directory that was specified with the -target option or -f option does not exist on the RAID device. Specify the path name on the RAID device and then re-execute the command. |
| DRM-10031 | Two or more mount points exist in the same copy group. | Backup cannot be performed because there are two or more logical disks on the physical disk that has the logical disk corresponding to the mount point directory to be backed up. Use a logical volume manager to change the volume configuration to a configuration allowing backup. |
| DRM-10032 | The specified file or directory is not backed up. | A file or directory path name specified with the -target option or -f option at the time of execution of a restore command is invalid. Check the backup file or directory, specify a correct path name, and then re-execute the restore command. |
| DRM-10033 | The path of the specified file or directory is invalid. | The path name of the file or directory specified with the -target option or -f option at the time of execution of a restore command was invalid. Check the specified file or directory for which backup was executed, and then re-execute the command. |
| DRM-10034 | The file system associated with the specified instance is not mounted. | The file system associated with the instance specified at the time of backup or restore processing was not mounted. Mount the file system to be backed up or restored, and then re-execute the command. |
| DRM-10035 | Primary volume(s) and secondary volume(s) are mixed in the same logical disk group. | The primary volume(s) and the secondary volume(s) of the copy group are in one logical disk group. With this volume configuration, Protection Services cannot perform backup or restore processing. Separate the primary volumes and the secondary volumes into other disk groups, and then re-execute the command. |
| DRM-10036 | The specified backup object cannot identify the backup-target secondary volume(s). | A backup or restore command was executed for a volume for which a copy group is not defined. Use CCI to define a copy group, and then re-execute the command. |
| DRM-10037 | The name of mount point directory is too long. | The length of the specified mount-point-directory name exceeded 255 characters. This program can only handle mount-point-directory names of 255 or fewer characters. |
| DRM-10038 | The name of disk group is too long. | The length of the disk-group name exceeded 31 characters. This program can only handle disk-group names of 31 or fewer characters. |
| DRM-10039 | The secondary volumes to be processed are already mounted. | An attempt was made to perform backup or restoration, but the secondary volumes to be backed up or restored are already mounted. Unmount all secondary volumes to be backed up or restored. |
| DRM-10040 | The cluster resource could not be placed offline. | In a cluster environment, an attempt to place the cluster resource offline has failed. Confirm that the cluster product is functioning normally. If no problem exists, see Chapter 7 (Troubleshooting) for more information, collect the appropriate information, and then contact the Support Center. |
| DRM-10041 | The cluster resource could not be placed online. | In a cluster environment, an attempt to place the cluster resource online has failed. Confirm that the cluster product is functioning normally. If no problem exists, see Chapter 7 (Troubleshooting) for more information, collect the appropriate information, and then contact the Support Center. |
| DRM-10042 | An attempt to execute the chkdsk command on the primary volume(s) failed. | In a cluster environment, an attempt to execute the chkdsk command on the primary volume(s) failed. Check the system logs to confirm whether a problem exists. If no problem exists, see Chapter 7 (Troubleshooting) for more information, collect the appropriate information, and then contact the Support Center. |

| | | |
|---|---|---|
| DRM-10043 | An attempt to obtain the cluster information failed. | An attempt to check whether the specified mount point exists on the cluster server failed. Confirm that the cluster product is functioning normally. If no problem exists, see Chapter 7 (Troubleshooting) for more information, collect the appropriate information, and then contact the Support Center. |
| DRM-10044 | The specified mount point is being managed by the cluster. | The requested operation could not be executed for the file system of the specified cluster manager. Operations cannot be performed on a mount point managed by a cluster. |
| DRM-10045 | A cluster volume and a non-cluster volume exist in the same logical disk group. | Within one logical disk group, volumes being managed by the cluster server are mixed with those that are not. Resynchronized restoration cannot be performed under this configuration. Decide whether all volumes existing in the logical disk group are to be managed by the cluster server of not, and execute the command. |
| DRM-10047 | An attempt to perform the resynchronize restoration failed. | When the files to be restored were specified, some of the files to be backed up were not specified. When you specify the files to be restored, specify all the files that were backed up. Then re-execute the command. |
| DRM-10049 | An attempt to synchronize the file system failed. | Examine the system log and check whether error messages have been output for the file system. |
| DRM-10050 | The specified mount point is already mounted. | A file system has already been mounted to the mount point managed as a cluster resource by the cluster management product. Therefore, you cannot perform restoration by disk resynchronization for the mount point. To perform restoration by disk resynchronization in a cluster environment, unmount the file system you want to restore, and then re-execute the command. |
| DRM-10052 | An attempt to start Command Control Interface failed. | An instance of CCI could not be started. Check the operating environment of Protection Services in the following order:<br>▪ Make sure that the CCI instance to be communicated with the CCI instance specified in the HORCMINST parameter of the Protection Services configuration definition file (DEFAULT.dat) has already been started.<br>▪ Make sure that the instance number specified in the HORCMINST parameter of the Protection Services configuration definition file (DEFAULT.dat) is correct.<br>▪ Make sure that the CCI configuration definition file (horcmn.conf) is correct.<br>When there is no problem in the operating environment of Protection Services, examine the CCI trace log and configuration definition files, and check whether the configuration definitions are correct. |
| DRM-10053 | An attempt to stop Command Control Interface failed. | An instance of CCI could not be stopped. Examine the CCI trace log and check whether there is any problem. |
| DRM-10054 | The path configuration for the primary volume(s) and secondary volume(s) is invalid. | This message is output when, in a multi-path configuration of the logical volume manager, the number of physical paths specified for the secondary volume(s) is greater than that of the primary volume(s). Reduce the number of physical paths for the secondary volume(s) until it is equal to or less than that of the primary volume(s). |
| DRM-10055 | An attempt to restore the volume group information failed. | This message appears when the volume group information in the logical volume manager cannot be restored. The volume group cannot be recognized from the backup server because the management information about the volume group in the logical volume manager is rewritten. Use the logical volume manager on the backup server to register the management information about the volume group. |
| DRM-10058 | The system detected the same copy group(s). | This message appears when the same copy group is detected. Check whether the same copy group is configured in CCI. If the same copy group exists, change the CCI settings so as not to configure the same copy group, and then restart the CCI instance. |

| | | |
|---|---|---|
| DRM-10059 | An attempt to access the DEFAULT.dat file failed. | This message appears when a DEFAULT.dat file was not found or the contents written in the file are incorrect. Check whether the DEFAULT.dat file exists. If the DEFAULT.dat file does not exist, uninstall Protection Services and then re-install Protection Services. If the DEFAULT.dat exists, check the contents written in the file and try to access the file again. If the same error occurs, contact the Support Center. |
| DRM-10061 | The target copy group is managed by different Command Control Interface instance. | The copy group to be backed up or restored needs to be managed in one CCI instance. Check whether the setup of CCI is correct, set up the correct instance, and then re-execute the command. |
| DRM-10062 | Two or more logical disks exist under the target mount point. | The mount point directory contains a mount point that corresponds to another logical disk. Check the volume configuration. |
| DRM-10063 | A secondary volume is being managed by the primary volume's host. | The primary and secondary volumes of the copy group are managed by the same command executing host. Assign separate command executing hosts to the primary and secondary volumes, and then execute the command. |
| DRM-10064 | Two or more mount points exist on one physical disk. | The mount point disk is mounted at another mount point. Check the volume configuration. |
| DRM-10065 | The target volume's ldev or serial is inconsistent between the backup record and the present. | The current configuration does not indicate the logical device or serial number of the volume subject to backup record processing. Make sure that there is no change to the volume configuration during backup processing with the following procedure:<br>▪ Use the drmfscat command with the -l option specified to check the backup volume configuration.<br>▪ Check the current volume configuration by using a method such as a CCI command.<br>If you are executing the restore operation forcibly, such as when the logical device number is changed by replacing a volume, execute the command with the -force option specified. |
| DRM-10100 | The maximum number of files that the OS can open at one time was exceeded. | An attempt was made to open files that exceeded the maximum number that can be opened in the system. Redefine the OS kernel parameter to increase the maximum number of files that can be opened in the system. |
| DRM-10101 | The dictionary map file is corrupted. | The dictionary map file is corrupted. Use the drmdbsetup utility to re-create the dictionary map file. |
| DRM-10102 | The target record is locked. | A record to be updated was locked when the attempt was made to update the dictionary map file, so it has not updated. Wait a while, and then re-execute the command. |
| DRM-10103 | The target file is locked. | The file to be updated was locked when the attempt was made to update the dictionary map file, so it has not updated. Wait a while, and then re-execute the command. |
| DRM-10104 | No target record exists. | A record to be referenced did not exist when the attempt was made to reference the dictionary map file, so it was not referenced.<br>With the -refresh option, use the drmfsdisplay, drmsqldisplay, or drmexgdisplay command to update the contents of the dictionary map file. |
| DRM-10105 | Memory is insufficient. | Memory became insufficient when the command was executed. Increase available memory, and then re-execute the command. |
| DRM-10106 | An internal error occurred. | During internal processing, an unknown internal error occurred when a system call was used. Refer to Chapter 7 (Troubleshooting), collect data, and then contact the Support Center. |

| | | |
|---|---|---|
| DRM-10107 | The dictionary map file already exists. | This message is output for either of the following reasons:<br>▪ Protection Services was re-installed in a situation in which the dictionary map file existed because Protection Services was previously uninstalled incorrectly.<br>▪ The dictionary map file already existed when the dictionary map file was created in the specified directory by using the drmdbsetup utility.<br>Depending on the cause, take the following actions:<br>▪ Uninstall Protection Services correctly and then re-install Protection Services.<br>▪ Delete the dictionary map file in the specified directory and re-create the dictionary map file by using the drmdbsetup utility. |
| DRM-10108 | The dictionary map file cannot be found. | The dictionary map file was deleted for some reason. Use the drmdbsetup utility to create the dictionary map file. |
| DRM-10109 | Disk space is insufficient. | Disk space was insufficient when the command was executed. Increase available disk space, and then re-execute the command. |
| DRM-10110 | You do not have access permission. | The user is not authorized to execute the command. Re-execute the command with system administrator permissions. |
| DRM-10111 | The specified copy group is already locked. | The system tried to lock the specified copy group, but it was already locked. |
| DRM-10112 | The specified copy group is not locked. | The system tried to unlock the copy group, but it was not locked. |
| DRM-10113 | No usable copy group exists. | Since all the copy groups were locked at the time of executing backup, a usable copy group did not exist. Unlock a copy group and then re-execute the backup command. |
| DRM-10114 | A system error occurred during operation on a temporary file. | A system error occurred during operation on a temporary file. Check that memory and free disk space are sufficient. If they are, check the system log and confirm that no problems exist with the OS. |
| DRM-10115 | The backup data is already locked. | The user attempted to execute a backup command on a locked copy group. Before the backup, unlock the copy group for the backup. |
| DRM-10116 | The dictionary map file is incorrect, but you lack permission to restore it. | The user tried to execute a command to restore a corrupted dictionary map file, but the user had general user permissions only. Obtain system administrator permissions, and then re-execute the command to update the dictionary map file. |
| DRM-10117 | The backup ID for the backup to the tape could not be resynchronized. | The user tried to execute the drmresync command to perform disk resynchronization on a backup ID displayed by the drmtapecat command. |
| DRM-10118 | The version of the dictionary map file is incorrect. | When Protection Services was upgraded, either the dictionary map file was not stored in the default storage directory or the directory specified by init.conf, so the dictionary map file was not updated.<br>To update the dictionary map file, you will need to re-install Protection Services. Save them dictionary map file in either the default storage directory or the directory specified by init.conf, and re-install Protection Services.<br>The default storage directory for the dictionary map file is as follows:<br>In UNIX: /var/opt/drm/db<br>In Windows: Protection-Services-installation-directory\db |
| DRM-10119 | The specified virtual server name is invalid in the configuration file (init.conf). | The virtual server name specified in the DRM_DB_PATH parameter in the configuration definition file (init.conf) does not match that defined in the DRM_HOSTNAME environment variable.<br>Check the virtual server name specified in the DRM_DB_PATH parameter in the configuration definition file (init.conf) and the virtual server name defined in the DRM_HOSTNAME environment variable. |

| | | |
|---|---|---|
| DRM-10120 | The virtual server name of the DRM_HOSTNAME environment variable or the configuration file (init.conf) is too long. | The virtual server name specified in the DRM_DB_PATH parameter in the configuration definition file (init.conf) or the virtual server name defined in the DRM_HOSTNAME environment variable is too long.<br>Check the virtual server name specified in the DRM_DB_PATH parameter in the configuration definition file (init.conf) and the virtual server name defined in the DRM_HOSTNAME environment variable. |
| DRM-10121 | The specified directory name of the dictionary map file directory is invalid. | Possible causes are as follows:<br>▪ The directory name of the dictionary map file defined in the DRM_DB_PATH parameter in the configuration definition file (init.conf) is too long.<br>▪ The directory name of the dictionary map file defined in the DRM_DB_PATH parameter in the configuration definition file (init.conf) is not an absolute path name.<br>Check the directory name of the dictionary map file defined in the DRM_DB_PATH parameter in the configuration definition file (init.conf). |
| DRM-10405 | The file name is too long. | The file path name specified with the -target option or -f option for backup exceeds 1,024 bytes. A file path name exceeding 1,024 bytes cannot be specified. Specify a correct file name by using less than 1,024 bytes. |
| DRM-10406 | The process has reached the maximum number of files that can be opened. | The process has reached the maximum number of files that can be opened. Redefine the kernel parameter and increase the number of files that a process can open. |
| DRM-10407 | The number of open files in the entire system has reached the maximum allowed limit. | The number of open files in the entire system has reached the maximum allowed limit. Redefine the kernel parameter to increase the number of files that the system can open. |
| DRM-10408 | An attempt to access a file failed. | The system cannot access the file path because an invalid file name or invalid directory name was specified for backup or restore processing. Check whether the path name used in backup or restore processing is specified correctly. If the path name is correct, examine the Protection Services trace log file and the system log, and check whether there is any problem. |
| DRM-10409 | An attempt to generate a process failed. | When a command was executed, an attempt to generate an internal process failed. Make sure there is sufficient memory and disk space. If there are no problems with memory or disk capacity, examine the system log and check whether there are any problems in the OS. |
| DRM-10410 | The host name could not be obtained. | During execution of a command to back up to tape, the host name that executes the command could not be obtained. Set up the system so that the name of the host that executes the command can be obtained correctly. Then, re-execute the command. |
| DRM-10411 | The expiration period could not be set. | When executing the drmtapebackup command, the system could not set the expiration period, based on the number of days that the backup data is to be stored (previously specified in the drmtapeinit command). Re-execute the drmtapeinit command and reset the number of days that the backup data is to be stored, and then re-execute the drmtapebackup command. |
| DRM-10450 | An attempt to transfer files to the FTP client has failed. | An attempt to transfer files to the FTP client has failed. Check the following items.<br>▪ Ensure the FTP service in the FTP server is running normally.<br>▪ Determine if connection to the FTP server can be made properly with the specified user ID and password.<br>▪ When connection to the FTP server can be made, determine if a temporary directory for extended command on the FTP server and a backup catalog file subject to transfer exist. |

| | | |
|---|---|---|
| DRM-10451 | An attempt to transfer files to the FTP server has failed. | An attempt to transfer files to the FTP server has failed. Check the following items.<br>▪ Ensure the FTP service in the FTP server is running normally.<br>▪ Determine if connection to the FTP server can be made properly with the specified user ID and password.<br>▪ When connection to the FTP server can be made, determine if a temporary directory for extended command on the FTP server exists and if a file can be created. |
| DRM-10452 | The character string specified as the operation ID exceeds the maximum number of characters. | The operation ID, which was specified when the command was executed, exceeds the maximum number of characters allowed. Specify an operation ID within the limit. |
| DRM-10453 | The specified file does not exist. | The file required by the executed extended command does not exist. Check that the specified file exists. |
| DRM-10454 | An attempt to access the specified file failed. | An attempt to access the required file failed during the processing of the extended command. Check that the user has the proper permission for the target file and that there is sufficient memory and free disk space. If there is sufficient memory and free disk space, examine the system log and check if there is any problem with the operating system. |
| DRM-10455 | An attempt to read the specified file failed. | An attempt to read the required file failed during the processing of the extended command. Use a text editor to check that the specified definition file can be opened. |
| DRM-10456 | An attempt to copy the specified file failed. | An error occurred when the file is copied. Check if the file system capacity is full. If the file system capacity is not full, examine the system log and check if there is any error message about the target file system. If the file system is normal, contact the Support Center. |
| DRM-10457 | The content of the specified file is invalid. | The contents of the specified file are incorrect. Check that the contents of the file are correct. |
| DRM-10458 | An attempt to generate a process failed. | Generation of an internal process failed during command execution. Check that there is sufficient memory and free disk space. If there is sufficient memory and free disk space, examine the system log and check if there is any problem with the operating system. |
| DRM-10459 | An attempt to obtain the installation path failed. | Since Protection Services is not installed correctly in the Windows system, the installation path of Protection Services could not be obtained. Uninstall Protection Services and then re-install it. |
| DRM-10460 | An attempt to connect to the FTP server failed. | Connection to the FTP server was not possible. On the FTP server, check that the FTP service is running normally. Also make sure that you can use the specified ID and password to connect to the specified FTP server. |
| DRM-10461 | An attempt to connect to database server failed. | Connection to the database server was impossible.<br>On the database server, check that the service is running normally. Also make sure that you can use the name of the user who is logged in and password to connect to the database server. |
| DRM-10462 | An internal error occurred. | An unknown internal error occurred. See Chapter 7 (Troubleshooting), and collect necessary data. Then contact the Support Center. |
| DRM-10463 | The target backup catalog file does not exist. | This message appears when the backup catalog file to be operated by executing the extended command cannot be found. Create or copy a backup catalog file to execute the extended command. |

| | | |
|---|---|---|
| DRM-10464 | An error occurred during database server processing. | This message appears if an error occurs during the database server processing.<br>Check that the service is running on the database server. Check also that the database server can be connected by using the name of the user who is logging in and the password. |
| DRM-10465 | The Assigned directory does not exist in the specified file. | This message appears when the specified directory does not exist on the host. Confirm that the specified directory exists. |
| DRM-10466 | The Assigned directory name is not an absolute path. | This message appears when the specified directory is not an absolute path. Use the absolute path to specify the directory name. |
| DRM-10467 | The target file does not exist. | The file subject to the extended command operation could not be found. Use the following extended commands and create a file to operate.<br>EX_DRM_BACKUPID_SET<br>EX_DRM_TAPE_RESTORE<br>EX_DRM_DB_IMPORT |
| DRM-10469 | An attempt to write an internal file failed. | An attempt to write a file while processing an extended command failed. Determine the file name displayed with this message and see whether the file could be written. |
| DRM-10470 | The target SQL Server metafile does not exist. | The target SQL Server metafile executed by the extended command cannot be found. Create or copy the SQL Server metafile and then re-execute the extended command. |
| DRM-10471 | The required initialization command is not executed. | Either a parameter registration command needed to execute the extended command was not executed, or information generated when the parameter registration command was executed was corrupt.<br>Execute the parameter registration command that is output with this message, and then re-execute the extended command. |
| DRM-11010 | An internal error occurred. | An unexpected internal error occurred during command execution. Check the error code and the details indicated in the message, refer to the SQL Server documentation, and then remove the cause of the error. Collect the SQL Server error log and the Windows event log as required, and then check the status of the OS or the SQL Server. If you cannot detect any abnormal status, contact your support center. |
| DRM-11011 | SQL Server terminated abnormally while executing a statement. | An unexpected internal error occurred during command execution. Check the error code and the details indicated in the message, refer to the SQL Server documentation, and then remove the cause of the error. Collect the SQL Server error log and the Windows event log as required, and then check the status of the OS or the SQL Server. If you cannot detect any abnormal status, contact your support center. |
| DRM-11012 | SQL Server terminated abnormally while performing logon processing. | An unexpected internal error occurred during command execution. Check the error code and the details indicated in the message, refer to the SQL Server documentation, and then remove the cause of the error. Collect the SQL Server error log and the Windows event log as required, and then check the status of the OS or the SQL Server. If you cannot detect any abnormal status, contact your support center. |
| DRM-11013 | Logging on to SQL Server... | The above message was returned while logging on to SQL Server. Check the error code and the details indicated in the message, refer to the SQL Server documentation, and then remove the cause of the error. Collect the SQL Server error log and the Windows event log as required, and then check the status of the OS or the SQL Server. If you cannot detect any abnormal status, contact your support center. |
| DRM-11014 | SQL Server terminated abnormally while logging off. | An unexpected error occurred and SQL Server terminated abnormally while logging off from SQL Server. Check the error code and the details indicated in the message, refer to the SQL Server documentation, and then remove the cause of the error. Collect the SQL Server error log and the Windows event log as required, and then check the status of the OS or the SQL Server. If you cannot detect any abnormal status, contact your support center. |

| | | |
|---|---|---|
| DRM-11015 | Logging off from SQL Server... | The above message was returned while logging off from SQL Server. Check the error code and the details indicated in the message, refer to the SQL Server documentation, and then remove the cause of the error. Collect the SQL Server error log and the Windows event log as required, and then check the status of the OS or the SQL Server. If you cannot detect any abnormal status, contact your support center. |
| DRM-11016 | An attempt to open a metafile failed. | An attempt to open a metafile failed while backup or restore processing was being performed for the SQL Server database. Check whether you have permission to read or write to the metafile. You can use the drmsqlcat command to check the location of the metafile. |
| DRM-11017 | A timeout error occurred. | A timeout error occurred while waiting for resynchronization of either the backup, restore, or copy group. Wait a short while, and then re-execute the command. If the same message is displayed repeatedly, check and reset the timeout value by using the drmsqlinit command. |
| DRM-11018 | The user lacks appropriate permission to execute SQL statements. | A user who does not have permission to execute SQL statements attempted to execute a statement. Make sure that the user has the appropriate permissions, and then re-execute the command |
| DRM-11100 | The specified database is offline. | The specified database is offline, so backup processing cannot be executed. Put the database online, and then re-execute the command. |
| DRM-11011 | SQL Server terminated abnormally while executing a statement. | An unexpected internal error occurred during command execution. Check the error code and the details indicated in the message, refer to the SQL Server documentation, and then remove the cause of the error. Collect the SQL Server error log and the Windows event log as required, and then check the status of the OS or the SQL Server. If you cannot detect any abnormal status, contact your support center. |
| DRM-11012 | SQL Server terminated abnormally while performing logon processing. | An unexpected internal error occurred during command execution. Check the error code and the details indicated in the message, refer to the SQL Server documentation, and then remove the cause of the error. Collect the SQL Server error log and the Windows event log as required, and then check the status of the OS or the SQL Server. If you cannot detect any abnormal status, contact your support center. |
| DRM-11013 | Logging on to SQL Server... | The above message was returned while logging on to SQL Server. Check the error code and the details indicated in the message, refer to the SQL Server documentation, and then remove the cause of the error. Collect the SQL Server error log and the Windows event log as required, and then check the status of the OS or the SQL Server. If you cannot detect any abnormal status, contact your support center. |
| DRM-11014 | SQL Server terminated abnormally while logging off. | An unexpected error occurred and SQL Server terminated abnormally while logging off from SQL Server. Check the error code and the details indicated in the message, refer to the SQL Server documentation, and then remove the cause of the error. Collect the SQL Server error log and the Windows event log as required, and then check the status of the OS or the SQL Server. If you cannot detect any abnormal status, contact your support center. |
| DRM-11015 | Logging off from SQL Server... | The above message was returned while logging off from SQL Server. Check the error code and the details indicated in the message, refer to the SQL Server documentation, and then remove the cause of the error. Collect the SQL Server error log and the Windows event log as required, and then check the status of the OS or the SQL Server. If you cannot detect any abnormal status, contact your support center. |
| DRM-11016 | An attempt to open a metafile failed. | An attempt to open a metafile failed while backup or restore processing was being performed for the SQL Server database. Check whether you have permission to read or write to the metafile. You can use the drmsqlcat command to check the location of the metafile. |

| | | |
|---|---|---|
| DRM-11017 | A timeout error occurred. | A timeout error occurred while waiting for resynchronization of either the backup, restore, or copy group. Wait a short while, and then re-execute the command. If the same message is displayed repeatedly, check and reset the timeout value by using the drmsqlinit command. |
| DRM-11018 | The user lacks appropriate permission to execute SQL statements. | A user who does not have permission to execute SQL statements attempted to execute a statement. Make sure that the user has the appropriate permissions, and then re-execute the command |
| DRM-11100 | The specified database is offline. | The specified database is offline, so backup processing cannot be executed. Put the database online, and then re-execute the command. |
| DRM-11101 | The specified database is currently restored. | The specified database has been restored, but not recovered. Perform recovery processing on the database. |
| DRM-11102 | The specified database is being recovered. | The specified database is currently being recovered and cannot be used in the query. Wait a short while, and then re-execute the command. |
| DRM-11103 | The specified database could not be recovered. | The database could not be recovered. Check the status of the database to continue. |
| DRM-11104 | The file name of the specified database could not be found. | For some reason, the file name of the specified database could not be found. To continue, check the status of the database. |
| DRM-11105 | The attribute of the specified database is read-only. | Check the status of the target database, and then re-execute the command. |
| DRM-11106 | The recovery model of the specified database is “simple”. | Check the status of the database. If you must use the drmsqlrecover command to perform roll-forward processing, back up the transaction log by using the following procedure:<br>1. Change the database recovery model to other than Simple.<br>2. Use the drmsqlbackup command to obtain a backup again.<br>3. Use the drmsqllogbackup command to back up the transaction log.<br>4. Redirect the output result of the drmsqllogbackup command with the -v option specified to a target definition file for transaction logs.<br>5. Specify the file created in step 4 in the drmsqlrecover command as a transaction-log target definition file. |
| DRM-11107 | The specified database information could not be obtained. | This message appears if the information for the target database could not be obtained. Check the status of the target database, and then re-execute the command. |
| DRM-11109 | The specified database is in stand-by mode. | This message appears when the specified database is in the standby mode. Execute the drmsqlrecover command without specifying the -undo option to recover the database. |
| DRM-11500 | Exchange Server information could not be acquired. | Exchange Server information could not be obtained when the user executed a command. Check the settings for Exchange Server. If the settings are incorrect, check that the service used to start Exchange Server is running. |
| DRM-11501 | The system has been returned to pre-failure status. | Since an attempt to perform restore processing has failed, the following files have been returned to their previous statuses:<br>▪ Data files (*.edb or *.stm)<br>▪ Transaction log files (*.log)<br>▪ Check point files (*.chk)<br>Remove the cause of the error, and re-execute the restore command. |

| | | |
|---|---|---|
| DRM-11502 | Mounting cannot take place, since a database inconsistency exists. | Restore processing has failed because an inconsistency exists in the database.<br>Remove the cause of the error, and then re-execute the restore command. |
| DRM-11503 | An attempt to execute the ESEUTIL command failed. | An error occurred when an attempt was made to check the compatibility of the database.<br>Remove the cause of the error, and then re-execute the command. |
| DRM-11504 | An internal error occurred. | Refer to the documentation for Exchange Server and correct the error according to the error code and detailed message that appear with this message. You may have to check the statuses of the OS and Exchange Server in the Windows event log as required. If there is no problem in the OS or Exchange Server, contact your support center. |
| DRM-11505 | An error occurred during the Information Store Service processing. | This can be due to any of the following:<br>▪ The Information Store Service is not functioning properly.<br>▪ A timeout occurred during an Information Store Service status change.<br>▪ An unexpected status was entered because an external operation was performed on the Information Store Service while the command was executed.<br>▪ In a cluster environment, even though the information store of the cluster resource was online, the Information Store Service was not running.<br>See the Exchange Server documentation, and check whether the Information Store Service is operating properly.<br>If the message DRM-11508 is output as the cause, adjust the values of the SVC_RETRY_TIME or SVC_RETRY_WAIT field in the init.conf file. If another cause is indicated, check as indicated. |
| DRM-11506 | An attempt to start the Information Store Service has failed. | This message is output when an attempt to start the Information Store Service fails. Make sure that the Information Store Service is running correctly.<br>If the message DRM-11508 is output as the cause, adjust the values of the SVC_RETRY_TIME or SVC_RETRY_WAIT field in the init.conf file. If another cause is indicated, check as indicated. |
| DRM-11507 | An exception occurred with the status of the Information Store Service. | This can be due to any of the following:<br>▪ An unexpected status was entered because an external operation was performed on the Information Store Service while the command was executed.<br>▪ In a cluster environment, even though the information store of the cluster resource was online, the Information Store Service was not running.<br>Make sure that no external operations are performed on the Information Store Service while the command is executing. Also, make sure that the Information Store Service is running when the information store of the cluster resource is online. |
| DRM-11508 | A timeout occurred. | This message is output when a timeout occurs.<br>Check the other message output at the same time, and act accordingly. |
| DRM-11600 | An error occurred during Active Directory processing. | The system could not connect to the domain controller. Determine if you can establish connection to the domain controller using the logon user name and password. Alternatively, determine if the domain controller, the DNS service, and the network are operating properly. If required, collect event log information from the server that runs this program, the domain controller, and the DNS service, and check the operating system status. |
| DRM-11601 | An error occurred during registry processing. | The system outputs this message when an error has occurred during registry processing.<br>Verify the authority of the login user. If required, collect event log information, and check the operating system status. If you cannot resolve this problem, see 6. Troubleshooting, and collect necessary data. Then contact your support center. |

| | | |
|---|---|---|
| DRM-11602 | An internal error occurred. | An unknown internal error occurred.<br>See 6. Troubleshooting, and collect necessary data. Then contact your support center. |
| DRM-12500 | An attempt to access the remote directory failed. | An attempt to access the remote directory on the FTP server failed. Check the message that is displayed together with this message to determine whether or not the directory exists or data can be written. |
| DRM-12501 | File does not have execution permission. | Command execution failed because there is no execution permission for the command. Check to see if the specified file can be executed or the user has permission to execute the specified file. |
| DRM-12502 | The target backup catalog file does not exist on FTP server. | The target backup catalog file was not found in the specified directory on the FTP server. Check to see if the target backup catalog file exists on the FTP server. If it does not exist, create or copy the backup catalog file and then re-execute the command. |

## 8.7 Actions Taken for the Message KAVX0070-W

In HP-UX, the message KAVX0070-W appears when a disconnected path is found in a multi-path environment for logical volumes. The following describes how to recover the disconnected physical path.

To recover the disconnected path:

1. Recover the disconnection status of the physical path.
2. Log in to the host as a root user.
3. Check the Protection Services message log file for the following message (the message may consist of more than one line).

   The location of the Protection Services trace log file:
   `/var/opt/drm/log/drm_pp_trace[*].log`

   Output message:
   `Enter do_vgreduce. target_vg=[`*XXXX*`] target_reduce_device=[`*XXXX*`]`
4. Check the character strings output after **target_vg=** and **target_reduce_device=** that you found in step 3. Their meanings are as follows:

   **target_vg**: Volume group name
   **target_reduce_device**: Device name

5. Execute the **vgdisplay** command to check information about the LVM volume group.
   ```
   # vgdisplay -v volume-group-name
   ```
   In ***volume-group-name***, specify the volume group name that you checked in step 4. The following shows an example of output from the **vgdisplay** command.

```
--- Volume groups ---
VG Name                     /dev/pvlnkvg01
VG Write Access             read/write
VG Status                   available
Max LV                      255
Cur LV                      1
Open LV                     1
Max PV                      16
Cur PV                      2
Act PV                      2
Max PE per PV               1016
VGDA                        4
PE Size (Mbytes)            4
Total PE                    1058
Alloc PE                    529
Free PE                     529
Total PVG                   1
Total Spare PVs             0
Total Spare PVs in use      0

   --- Logical volumes ---
   LV Name                      /dev/pvlnkvg01/lvol1
   LV Status                    available/syncd
   LV Size (Mbytes)             2116
   Current LE                   529
   Allocated PE                 529
   Used PV                      1

   --- Physical volumes ---
   PV Name                      /dev/dsk/c12t3d1
   PV Status                    available
   Total PE                     529
   Free PE                      0
   Autoswitch                   On

   PV Name                      /dev/dsk/c12t3d2
   PV Status                    available
   Total PE                     529
   Free PE                      529
   Autoswitch                   On

   --- Physical volume groups ---
   PVG Name                     bus2
   PV Name                      /dev/dsk/c12t3d1
   PV Name                      /dev/dsk/c12t3d2
```

6. Execute the following command to add the device to the LVM volume group:
   ```
   # vgextend volume-group-name device-name
   ```
   In ***volume-group-name*** and ***device-name***, specify the values you checked in step 4.

   If the message output to the Protection Services trace log file consists of more than one line (see step 3), execute the command once for each device.

7. Execute the **vgdisplay** command to display the LVM management information.

```
# vgdisplay -v volume-group-name

--- Volume groups ---
VG Name                     /dev/pvlnkvg01
VG Write Access             read/write
VG Status                   available
Max LV                      255
Cur LV                      1
Open LV                     1
Max PV                      16
Cur PV                      2
Act PV                      2
Max PE per PV               1016
VGDA                        4
PE Size (Mbytes)            4
Total PE                    1058
Alloc PE                    529
Free PE                     529
Total PVG                   2
Total Spare PVs             0
Total Spare PVs in use      0

   --- Logical volumes ---
   LV Name                      /dev/pvlnkvg01/lvol1
   LV Status                    available/syncd
   LV Size (Mbytes)             2116
   Current LE                   529
   Allocated PE                 529
   Used PV                      1

   --- Physical volumes ---
   PV Name                      /dev/dsk/c14t3d1
   PV Name                      /dev/dsk/c12t3d1 Alternate Link *
   PV Status                    available
   Total PE                     529
   Free PE                      0
   Autoswitch                   On

   PV Name                      /dev/dsk/c14t3d2
   PV Name                      /dev/dsk/c12t3d2 Alternate Link *
   PV Status                    available
   Total PE                     529
   Free PE                      529
   Autoswitch                   On

   --- Physical volume groups ---
   PVG Name                     bus2
   PV Name                      /dev/dsk/c12t3d1
   PV Name                      /dev/dsk/c12t3d2
```

* ***Note:*** In the above example, the following lines below Physical volumes indicate that the devices have been added.

```
PV Name                     /dev/dsk/c12t3d1 Alternate Link
PV Name                     /dev/dsk/c12t3d2 Alternate Link
```

8. Execute the following command to set the LVM physical volume group.
   `# vgextend -g physical-volume-group-name device-name`

   In ***physical-volume-group-name***, specify a value other than those defined in the LVM management information (including **bus*X***, where ***X*** is a numeric serial value) that you displayed in step 7. In ***device-name***, specify the device name you specified in the command in step 6.

9. Re-execute the **vgdisplay** command to display the LVM management information.
   `# vgdisplay -v volume-group-name`

10. Make sure that the physical volume group has been added to the LVM management information.

    The following shows an output example of the **vgdisplay** command. If the last eight lines in this example (**Physical volume groups** and the subsequent lines) are output, the disconnected path has been restored.

```
--- Volume groups ---
VG Name                     /dev/pvlnkvg01
VG Write Access             read/write
VG Status                   available
Max LV                      255
Cur LV                      1
Open LV                     1
Max PV                      16
Cur PV                      2
Act PV                      2
Max PE per PV               1016
VGDA                        4
PE Size (Mbytes)            4
Total PE                    1058
Alloc PE                    529
Free PE                     529
Total PVG                   2
Total Spare PVs             0
Total Spare PVs in use      0

   --- Logical volumes ---
   LV Name                      /dev/pvlnkvg01/lvol1
   LV Status                    available/syncd
   LV Size (Mbytes)             2116
   Current LE                   529
   Allocated PE                 529
   Used PV                      1


   --- Physical volumes ---
   PV Name                      /dev/dsk/c14t3d1
   PV Name                      /dev/dsk/c12t3d1 Alternate Link
   PV Status                    available
   Total PE                     529
   Free PE                      0
   Autoswitch                   On

   PV Name                      /dev/dsk/c14t3d2
   PV Name                      /dev/dsk/c12t3d2 Alternate Link
   PV Status                    available
   Total PE                     529
   Free PE                      529
   Autoswitch                   On

   --- Physical volume groups ---
```

```
PVG Name                bus1
PV Name                 /dev/dsk/c14t3d1
PV Name                 /dev/dsk/c14t3d2

PVG Name                bus2
PV Name                 /dev/dsk/c12t3d1
PV Name                 /dev/dsk/c12t3d2
```

# Acronyms and Abbreviations

| | |
|---|---|
| API | application program interface |
| ASCII | American Standard Code for Information Interchange |
| CCI | Command Control Interface |
| CPU | central processing unit |
| DBMS | database management system |
| DKC | disk controller |
| FS | file system |
| FTP | file transfer protocol |
| GUID | global unique identifier |
| ID | identifier, identification |
| IIS | Internet Information Services |
| LDEV | logical device |
| LUN | logical unit number |
| LVM | Logical Volume Manager, logical volume manager |
| MB | megabyte |
| MU | mirror unit |
| OCI | Oracle call interface |
| ODBC | open database connectivity |
| OS | operating system |
| P-VOL | primary volume |
| RAID | redundant array of inexpensive disks |
| SMPL | simplex |
| SQL | structured query language |
| S-VOL | secondary volume |
| TCO | total cost of ownership |
| TID | target ID |
| VDI | Virtual Device Interface |
| VxVM | VERITAS Volume Manager VERITAS Volume Manager |