Tivoli® Storage Manager for Advanced Copy Services

IBM

Version 6.1

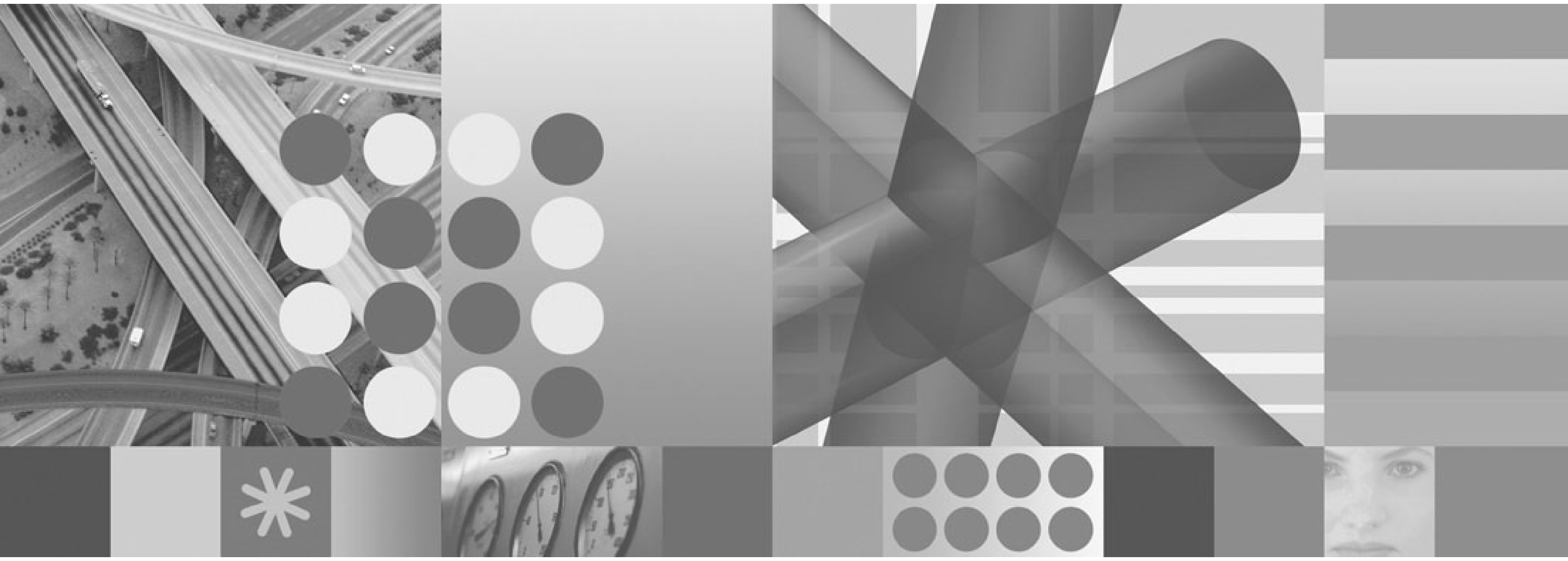
Data Protection for Snapshot Devices Installation and User's Guide

SC33-8331-00

Tivoli® Storage Manager for Advanced Copy Services

IBM

Version 6.1



Data Protection for Snapshot Devices Installation and User's Guide

SC33-8331-00

Note

Before using this information and the product it supports, read the information in "Notices" on page 365.

Edition notice

This publication is a replacement for

- *IBM Tivoli Storage Manager for Advanced Copy Services, Data Protection for Snapshot Devices for DB2 Advanced Copy Services, Installation and User's Guide* V5.5, SC33–8330–00.
- *IBM Tivoli Storage Manager for Advanced Copy Services, Data Protection for Snapshot Devices for mySAP™, Installation and User's Guide for Oracle* V5.4, SC33–8207–01.
- *Tivoli Storage Manager for Hardware, Data Protection for FlashCopy Devices for Oracle, Installation and User's Guide* V5.3, GC32–1772–00.

It applies to the following IBM Tivoli Storage Manager for Advanced Copy Services software components:

- Data Protection for Snapshot Devices for DB2 Advanced Copy Services, V6.1
- Data Protection for Snapshot Devices for *SAP® with Oracle*, V6.1
- Data Protection for Snapshot Devices for Oracle, V6.1

These components are offered as part of IBM Tivoli Storage Manager for Advanced Copy Services, V6.1, Program Number 5608-E10, which is available as a licensed program product, and to all subsequent releases and modifications until otherwise indicated in new editions.

Order publications through your IBM representative or the IBM branch office serving your area. Publications are not stocked at the addresses given below.

Address comments on this publication to:

IBM Deutschland Research and Development GmbH
Enterprise Solution Development
Dept. 3848
Schönaicher Str. 220
71032 Böblingen
Germany

FAX (Germany): 07031 16 3619
FAX (other countries): (+49) 7031 16 3619

Make sure to include the following in your comment or note:

- Title and order number of this document
- Page number or topic related to your comment

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Figures vii

Tables ix

Preface xi

About this publication xi
Who should read this publication xii
Publications xii
  Tivoli Storage Manager publications xii
Information sources xiv
  Tivoli Storage Manager information sources . . xiv
  IBM Tivoli Storage Manager for Advanced Copy Services information sources. xv
  IBM Tivoli Storage Manager for Enterprise Resource Planning information sources xv
  IBM Tivoli Storage Manager for Databases: Data Protection for Oracle information sources . . . xv
  AIX information sources xvi
  Common Information Model information sources xvi
  IBM storage systems information sources . . . xvi
  SAP information sources xvii
  Oracle information sources xvii
  DB2 for Linux, UNIX, and Windows information sources xvii
Support information. xviii
  Getting technical training xviii
  Searching knowledge bases xviii
  Contacting IBM Software Support xix
New for Data Protection for Snapshot Devices Version 6.1 xxi
  Functional Enhancements for V6.1 xxii

Chapter 1. Protection for Snapshot Devices 1

Overview of Data Protection for Snapshot Devices in an SAP environment. 1
  SAP with DB2 overview 1
  SAP with Oracle overview. 2
Overview of the integrated DB2 Advanced Copy Services and Data Protection for Snapshot Devices environment 3
  Common functions overview: DB2 Advanced Copy Services and Data Protection for Snapshot Devices 4
  Additional functions overview: Data Protection for Snapshot Devices for DB2 5
  Common Data Protection for Snapshot Devices components. 6
  Data Protection for Snapshot Devices for DB2 software environment 8
  Data Protection for Snapshot Devices for DB2 operating environment 8
Offload Agent (tsm4acs) functions 10
  Tivoli Storage Manager overview 10
  Integrated snapshot and Tivoli Storage Manager backup 11
  Incremental or "No Copy" FlashCopy backup and restore 12
  Seamless augmentation of the functions of Tivoli Storage Manager for Enterprise Resource Planning 12
  Integration with Tivoli Storage Manager media management functions. 12
  Centrally administered and scheduled backup operations 13
  IBM Subsystem Device Driver support 13
  Data consistency. 13
Data Protection for Snapshot Devices for Oracle overview 13
  Data Protection for Snapshot Devices for Oracle limitations 15
  Data Protection for Snapshot Devices for Oracle migration considerations 15
  Data Protection for Snapshot Devices for Oracle software environment 15
  Integration environment overview: Data Protection for Snapshot Devices and Data Protection for Oracle 16
  Data Protection for Snapshot Devices for Oracle features. 16
Data Protection for Snapshot Devices for *SAP with Oracle* overview 18
  Data Protection for Snapshot Devices for *SAP with Oracle* software environment 24
  IBM Subsystem Device Driver support 24
  Data consistency. 24
Data Protection for Snapshot Devices storage system overview 24
  Enterprise Storage Server 25
  Disk Storage subsystem 25
  SAN Volume Controller 26
  IBM System Storage N Series 27
  IBM XIV Storage System 29
CIM Agents used by Data Protection for Snapshot Devices. 30
  CIM Agent for DS Open API 30
  CIM Agent for SAN Volume Controller 31

Chapter 2. Planning for Snapshot Devices 33

Data Protection for Snapshot Devices backup methods 33
  Backup methods overview 33
  Overview of multiple backup generations (target sets) on disk 37
Data Protection for Snapshot Devices restore methods 43
  Restore methods overview 43

AIX Logical Volume Manager mirrored environments 48
  Overview of Data Protection for Snapshot Devices support for AIX Logical Volume Manager mirrored environments 48

Chapter 3. Installing Data Protection for Snapshot Devices 61
Installation process overview 62
Installation sequence 62
  Installation step 62
  Activation step 63
  Configuration step 63
Data Protection for Snapshot Devices installation prerequisites 66
  Preparing the disk layout. 67
  Hardware requirements 80
  Software requirements. 82
  Environment requirements 89
  Volume group requirements 90
  Logical Volume Manager mirroring requirements 90
  Recommended installation order 90
Installing Data Protection for Snapshot Devices . . 91
  Data Protection for Snapshot Devices installation procedure 91
  Installing Open SSL 96
  Installing the Common Information Model (CIM) components and related software 96
  Uninstalling Data Protection for Snapshot Devices 100
  Restoring backups from previous versions of DP for Snapshot Devices 101

Chapter 4. Configuring Data Protection for Snapshot Devices . . . 103
Configuring Data Protection for Snapshot Devices common components. 103
Configuring the Oracle environment. 104
  List of files installed by Data Protection for Snapshot Devices for Oracle 105
  Step 1. Register the workstations with the Tivoli Storage Manager server 105
  Step 2. Specify a Tivoli Storage Manager management class 105
  Step 3. Configure the disk storage environment 106
  Step 4. Configuring the Data Protection for Oracle environment 108
Mounting shared directories via NFS 116
Setting up source and target volumes for FlashCopy devices. 116
  Setting up source and target volumes in an ESS or DS configuration 116
  Setting up source and target volumes in a SAN Volume Controller configuration 117
  Guidelines for sharing target volumes 117

Chapter 5. Protecting data on snapshot devices. 119
Backing up data on snapshot devices 119
  Backing up a DB2 database. 119
  Backing up a native Oracle database 120
  Backing up an SAP with Oracle database . . . 124
Restoring data on snapshot devices 125
  Restoring from a snapshot on N Series devices with subsequent snapshots in the busy state . . 125
  Restoring from a snapshot on SVC devices . . 126
  Restoring a DB2 database 126
  Restoring an SAP with Oracle database. . . . 127
  Restoring a native Oracle database 127

Chapter 6. Data Protection for Snapshot Devices commands and scripts 133
Data Protection for Snapshot Devices commands and scripts 133
Installation setup script 134
Options for DB2 Advanced Copy Services and Data Protection for Snapshot Devices commands . 136
  Options parameters 138
Management Agent (acsd) 138
Device Agent for CIM Devices (acscim). 141
Device Agent for N Series Devices (acsnsan, acsnnas) 143
Device Agent for IBM XIV Storage System Devices (acsxiv) 145
Disk Mapper Script (acsdm.sh) 147
Volume Group Takeover Script (acsvg.sh) 147
XIV Adapter Java Archive (XivAdapter.jar) . . . 147
Production System User Interface for Data Protection for Snapshot Devices for Oracle (acsora). 147
Snapshot Object Manager for Oracle (acsutil) . . . 149
Data Protection for Snapshot Devices for *SAP with Oracle* ('backint') 151
Data Protection for Snapshot Devices Offload Agent (tsm4acs) 154
  -f tape_backup 155
  -f mount 157
  -f unmount 158

Chapter 7. Configuration files overview 159
Data Protection for Snapshot Devices profile description 160
  Data Protection for Snapshot Devices profile sections 160
  Overriding Data Protection for Snapshot Devices profile parameters 163
  Modifying the GLOBAL or ACSD sections of the Data Protection for Snapshot Devices profile. 164
  Data Protection for Snapshot Devices profile parameters 164
Data Protection for Snapshot Devices password file 188
Data Protection for Snapshot Devices Target Volumes File (.fct) 189
  Target volume parameter settings (ESS or DS configuration) 190
  Parameters for an SVC Configuration 191
SAP backint profile overview 192
  SAP Backint profile keyword definitions . . . 192
BR*Tools configuration profile (.sap). 193

Tivoli Storage Manager option files for native Oracle 194
  Tivoli Storage Manager option files used by Data Protection for Oracle 194
  Files for Data Protection for Snapshot Devices 194
Key files and directories 194

Appendix A. Data Protection for Snapshot Devices examples 199
Examples (DB2) 199
  Example overall disk layout for a DB2 environment. 199
  Example profile for Data Protection for Snapshot Devices for DB2 Advanced Copy Services 200
Examples (native Oracle) 201
  Example overall disk layout for a native Oracle environment. 201
  Example profile for Data Protection for Snapshot Devices for native Oracle 203
Examples (SAP with Oracle) 203
  Example overall disk layout for an SAP with Oracle environment 203
  Example profile for Data Protection for Snapshot Devices for *SAP with Oracle* 205
Example Target Volumes Files 205
  Example target volumes file (ESS or DS configuration) 205
  Example target volumes file (SAN Volume Controller configuration) 207
  Example target volume file (mirror setup on ESS or DS configuration) 209

Appendix B. Backup and restore cycles 213
Backup cycle 213
Restore cycle 214
Monitoring the FlashCopy background copy progress 215
Progress status indicator overview 216
Backup status indicator overview. 217
Restore status indicator overview. 218

Appendix C. Special tasks 221
Special tasks for native Oracle. 221
  Configuring system options files to use the same server 221
  Configuring multiple server stanzas 222
  Defining settings in the server script 222
  Restoring hdisks for Subsystem Device Drivers 223

Appendix D. Troubleshooting Data Protection for Snapshot Devices . . . 225
General troubleshooting procedure 225
Troubleshooting tips for Data Protection for Snapshot Devices for Oracle 226
  Guidelines for Oracle variables 227
  Data Protection for Snapshot Devices for Oracle miscellaneous errors 227
Log and trace files summary 228
  Data Protection for Snapshot Devices log and trace files. 228
  Storage system log and trace files 229
  CIM log and trace files 230
  Tivoli Storage Manager for ERP log and trace files 230

Appendix E. Internet Protocol Version 6 (IPv6) Support 231

Appendix F. Data Protection for Snapshot Devices Messages. 233
BKI Messages 233
EEO Messages 311
IDS Messages 332

Appendix G. Accessibility features for Tivoli Storage Manager 363

Notices 365

Glossary 367

Trademarks 375

Index 377

Figures

1. Overall Data Protection for Snapshot Devices and DB2 Environment Using CIM 9
2. Overall Data Protection for Snapshot Devices and native Oracle environment using CIM . . 14
3. Overall Data Protection for Snapshot Devices and SAP with Oracle Environment Using CIM . 20
4. Data Protection for Snapshot Devices and Copy Sets in an AIX LVM Mirror Environment 51
5. Overview of the Backup Scenario (DB2, Single Target Set) 69
6. Overview of the Backup Scenario (DB2, Multiple Target Sets) 69
7. Overview of the Backup Scenario (Oracle, Single Target Set) 71
8. Configuration File Relationships With Data Protection for Snapshot Devices and DP for SAP (DB2) 75
9. Example Overall Disk Layout 199
10. Example Overall Disk Layout 202
11. Example Overall Disk Layout 204

Tables

1. Abbreviations for database configurations xi
2. Tivoli Storage Manager server publications xii
3. Tivoli Storage Manager storage agent publications xiii
4. Tivoli Storage Manager client publications xiii
5. Tivoli Storage Manager Data Protection publications xiv
6. Tivoli Storage Manager information sources xiv
7. IBM Tivoli Storage Manager for Advanced Copy Services information sources. xv
8. IBM Tivoli Storage Manager for Enterprise Resource Planning (Tivoli Storage Manager for ERP) information sources xv
9. IBM Tivoli Storage Manager for Databases: Data Protection for Oracle information sources. xv
10. AIX information sources xvi
11. Common Information Model information sources. xvi
12. IBM storage systems information sources xvi
13. SAP information sources. xvii
14. Oracle information sources xvii
15. DB2 for Linux, UNIX, and Windows information sources xvii
16. Support for the Functional Enhancements for V6.1 xxii
17. Functional Comparison of DB2 Advanced Copy Services and Data Protection for Snapshot Devices 4
18. util_vol_access Parameter 23
19. Snapshot Backup Progress States 34
20. Commands Reporting Backup Progress States 35
21. Backup Usability States and Command Line Filter Options 35
22. Usability States Resulting from Snapshot Operations 36
23. Additional Parameter in the Data Protection for Snapshot Devices Target Volumes File for AIX LVM Mirrored Environments Using an ESS or DS 59
24. Additional Parameter in the Data Protection for Snapshot Devices Target Volumes File for AIX LVM Mirrored Environments Using SAN Volume Controller 60
25. Hardware Requirements Summary 80
26. Software Requirements Summary 83
27. Required Data Protection for Snapshot Devices TSM options and values 110
28. Required Data Protection for Oracle option values 112
29. Required Data Protection for Oracle environment variable settings 114
30. Summary of Backup Commands for DB2 119
31. Summary of Backup Commands for Native Oracle 120
32. Files used during a manual backup 123
33. Summary of Backup Commands (SAP with Oracle). 124
34. Summary of Restore Commands for DB2 126
35. Summary of Restore Commands for SAP with Oracle 127
36. Summary of Restore Commands for Native Oracle 127
37. Summary of Data Protection for Snapshot Devices commands and scripts. 133
38. Options Available 137
39. Options for Starting the Management Agent (acsd) as a Daemon Process 139
40. Options for Starting the Management Agent (acsd) (Password Function) 140
41. Options for Starting the Device Agent for CIM Devices (acscim) 142
42. Options for the Device Agent for N Series Devices (acsnsan/acsnnas) Command . . . 144
43. Options for the Device Agent for IBM XIV Storage System Devices (acsxiv) Command . 146
44. Parameters for Data Protection for Snapshot Devices Invocation as ’backint’. 151
45. Options for the Data Protection for Snapshot Devices ’tsm4acs’ Command 154
46. Data Protection for Snapshot Devices Profile Parameters 165
47. Actions Taken Depending on Values of LVM_FREEZE_THAW and TARGET_DATABASE_ SUSPEND. 188
48. Parameters of the ’volumes_set_x’ Topic (ESS or DS) 190
49. Parameters of the ’volumes_set_x’ Topic (SVC) 191
50. Key Files and Directories (DB2) 195
51. Key Files and Directories (Native Oracle) 196
52. Possible Progress Status Indicator (PSI) Values 216
53. Possible Backup Status Indicator (BSI) Values 217
54. Possible Restore Status Indicator (RSI) Values 218
55. DB2 Advanced Copy Services and Data Protection for Snapshot Devices Log and Trace Files 228

Preface

Material that applies to a particular database configuration or option is introduced by one of the following:

Table 1. Abbreviations for database configurations

Abbreviation	**Applies to**
(DB2)	Data Protection for Snapshot Devices for DB2 Advanced Copy Services
(Oracle) or (Native Oracle)	Data Protection for Snapshot Devices for Oracle
(SAP® with Oracle)	Data Protection for Snapshot Devices for *SAP® with Oracle*
(SAP®)	SAP® installation (DB2 or Oracle)
(TSM Server)	Use of Tivoli Storage Manager server

About this publication

This manual provides information on installing, configuring, administering, and using IBM Tivoli Storage Manager for Advanced Copy Services: Data Protection for Snapshot Devices, referred to hereafter as *Data Protection for Snapshot Devices*.

There are three database-dependent versions of Data Protection for Snapshot Devices V6.1:

- Data Protection for Snapshot Devices for DB2 Advanced Copy Services (for native or SAP®-based DB2 environments)
- Data Protection for Snapshot Devices for Oracle (for native Oracle environments)
- Data Protection for Snapshot Devices for *SAP® with Oracle* (for SAP®-based Oracle environments)

Data Protection for Snapshot Devices performs online or offline backups of DB2 or Oracle databases to snapshot-oriented storage systems and optionally Tivoli Storage Manager storage. The integration with the RMAN Media Management API maximizes the protection of data, thus providing a comprehensive storage management solution.

Tivoli Storage Manager is a client-server licensed product that provides storage management services in a multi-platform computer environment. It is required only if the offload tape backup function of Data Protection for Snapshot Devices is needed.

Who should read this publication

This publication is intended for system programmers and administrators who are responsible for implementing a backup solution in one of the supported database environments. It is assumed that you have an understanding of the following, as applicable:

- The IBM storage system used for the database:
  - TotalStorage® Enterprise Storage Server® (ESS) Model 800
  - TotalStorage Disk Storage Models DS6000™ and DS8000®
  - TotalStorage SAN Volume Controller (SVC)
  - IBM System Storage™ N Series
  - IBM XIV® Storage Systems
- AIX operating system and Logical Volume Manager (LVM)
- Linux for System x operating system
- Oracle or DB2 database administration
- Tivoli Storage Manager Application Program Interface (API)
- Oracle Server
- Tivoli Storage Manager server
- Tivoli Storage Manager backup-archive client
- Tivoli Storage Manager Application Program Interface

The target audience for this publication are system installers, system users, database administrators, and system administrators.

Publications

Tivoli® Storage Manager publications and other related publications are available online.

You can search all publications in the Tivoli Storage Manager Information Center: http://publib.boulder.ibm.com/infocenter/tsminfo/v6.

You can download PDF versions of publications from the Tivoli Storage Manager Information Center or from the IBM® Publications Center at http://www.ibm.com/shop/publications/order/.

You can also order some related publications from the IBM Publications Center Web site. The Web site provides information for ordering publications from countries other than the United States. In the United States, you can order publications by calling 800-879-2755.

Tivoli Storage Manager publications

Publications are available for the server, storage agent, client, and Data Protection.

Table 2. Tivoli Storage Manager server publications

Publication title	Order number
IBM Tivoli Storage Manager Messages	GC23-9787
IBM Tivoli Storage Manager Performance Tuning Guide	GC23-9788
IBM Tivoli Storage Manager Problem Determination Guide	GC23-9789
IBM Tivoli Storage Manager for AIX Installation Guide	GC23-9781

Table 2. Tivoli Storage Manager server publications (continued)

Publication title	Order number
IBM Tivoli Storage Manager for AIX Administrator's Guide	SC23-9769
IBM Tivoli Storage Manager for AIX Administrator's Reference	SC23-9775
IBM Tivoli Storage Manager for HP-UX Installation Guide	GC23-9782
IBM Tivoli Storage Manager for HP-UX Administrator's Guide	SC23-9770
IBM Tivoli Storage Manager for HP-UX Administrator's Reference	SC23-9776
IBM Tivoli Storage Manager for Linux Installation Guide	GC23-9783
IBM Tivoli Storage Manager for Linux Administrator's Guide	SC23-9771
IBM Tivoli Storage Manager for Linux Administrator's Reference	SC23-9777
IBM Tivoli Storage Manager for Sun Solaris Installation Guide	GC23-9784
IBM Tivoli Storage Manager for Sun Solaris Administrator's Guide	SC23-9772
IBM Tivoli Storage Manager for Sun Solaris Administrator's Reference	SC23-9778
IBM Tivoli Storage Manager for Windows Installation Guide	GC23-9785
IBM Tivoli Storage Manager for Windows Administrator's Guide	SC23-9773
IBM Tivoli Storage Manager for Windows Administrator's Reference	SC23-9779
IBM Tivoli Storage Manager Server Upgrade Guide	SC23-9554
IBM Tivoli Storage Manager for System Backup and Recovery Installation and User's Guide	SC32-6543

Table 3. Tivoli Storage Manager storage agent publications

Publication title	Order number
IBM Tivoli Storage Manager for SAN for AIX Storage Agent User's Guide	SC23-9797
IBM Tivoli Storage Manager for SAN for HP-UX Storage Agent User's Guide	SC23-9798
IBM Tivoli Storage Manager for SAN for Linux Storage Agent User's Guide	SC23-9799
IBM Tivoli Storage Manager for SAN for Sun Solaris Storage Agent User's Guide	SC23-9800
IBM Tivoli Storage Manager for SAN for Windows Storage Agent User's Guide	SC23-9553

Table 4. Tivoli Storage Manager client publications

Publication title	Order number
IBM Tivoli Storage Manager for UNIX and Linux: Backup-Archive Clients Installation and User's Guide	SC23-9791
IBM Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and User's Guide	SC23-9792
IBM Tivoli Storage Manager for Space Management for UNIX and Linux: User's Guide	SC23-9794
IBM Tivoli Storage Manager for HSM for Windows Administration Guide	SC23-9795
IBM Tivoli Storage Manager Using the Application Program Interface	SC23-9793
Program Directory for IBM Tivoli Storage Manager z/OS Edition Backup-Archive Client	GI11-8912

Table 4. Tivoli Storage Manager client publications (continued)

Publication title	Order number
Program Directory for IBM Tivoli Storage Manager z/OS Edition Application Program Interface	GI11-8911

Table 5. Tivoli Storage Manager Data Protection publications

Publication title	Order number
IBM Tivoli Storage Manager for Advanced Copy Services: Data Protection for Snapshot Devices Installation and User's Guide	SC33-8331
IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Installation and User's Guide	SC32-9059
IBM Tivoli Storage Manager for Databases: Data Protection for Oracle for UNIX and Linux Installation and User's Guide	SC32-9064
IBM Tivoli Storage Manager for Databases: Data Protection for Oracle for Windows Installation and User's Guide	SC32-9065
IBM Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP Installation and User's Guide for DB2	SC33-6341
IBM Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP Installation and User's Guide for Oracle	SC33-6340
IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino® for UNIX, Linux, and OS/400® Installation and User's Guide	SC32-9056
IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino for Windows Installation and User's Guide	SC32-9057
IBM Tivoli Storage Manager for Mail: Data Protection for Microsoft Exchange Server Installation and User's Guide	SC23-9796
Program Directory for IBM Tivoli Storage Manager for Mail (Data Protection for Lotus Domino)	GI11-8909

Information sources

Content regarding where to locate product, application, and component information is provided.

Tivoli Storage Manager information sources

Table 6. Tivoli Storage Manager information sources

Category	Publication or URL
Information Center	http://publib.boulder.ibm.com/infocenter/tsminfo/v6/index.jsp

IBM Tivoli Storage Manager for Advanced Copy Services information sources

Table 7. IBM Tivoli Storage Manager for Advanced Copy Services information sources

Category	**Publication or URL**
Product information:	
`http://www.ibm.com/software/tivoli/products/storage-mgr-advanced-copy-services/`	
Support:	
`http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliStorageManagerforAdvancedCopyServices.html`	
Release Notes:	
`http://publib.boulder.ibm.com/infocenter/tsminfo/v6/topic/com.ibm.itsmreadme.doc/relnote_acd610.html`	
Documentation for earlier version of the DB2 software (for a DB2 version earlier than 9.5).	*IBM Tivoli Storage Manager for Advanced Copy Services V5.4, Data Protection for Snapshot Devices for mySAP™, Installation and User's Guide for DB2 UDB,* SC33-8208-01.
Documentation for earlier version of the SAP® with Oracle software (for the splitint interface).	*IBM Tivoli Storage Manager for Advanced Copy Services V5.4, Data Protection for Snapshot Devices for mySAP™, Installation and User's Guide for Oracle, SC33-8207-01*
IBM Tivoli Storage Manager for Advanced Copy Services for DB2 UDB	*IBM Tivoli Storage Manager for Advanced Copy Services V5.3.3, Installation and User's Guide for DB2 UDB*, GC32–1780–00
Public FTP server	
`ftp://ftp.software.ibm.com/storage/tivoli-storage-management/patches/tivoli-data-protection/acs/`	

IBM Tivoli Storage Manager for Enterprise Resource Planning information sources

Table 8. IBM Tivoli Storage Manager for Enterprise Resource Planning (Tivoli Storage Manager for ERP) information sources

Category	**Publication or URL**
Product information	`http://www.ibm.com/software/tivoli/products/storage-mgr-erp/`
Information Center	`http://publib.boulder.ibm.com/infocenter/tsminfo/v6/index.jsp`
Installation and User's Guides	*IBM Tivoli Storage Manager for Enterprise Resource Planning: Installation and User's Guide for DB2*, SC33-6341*IBM Tivoli Storage Manager for Enterprise Resource Planning: Installation and User's Guide for Oracle*, SC33-6340

IBM Tivoli Storage Manager for Databases: Data Protection for Oracle information sources

Table 9. IBM Tivoli Storage Manager for Databases: Data Protection for Oracle information sources

Category	**Publication or URL**
Web Site	http://www-306.ibm.com/software/tivoli/products/storage-mgr-db

AIX information sources

Table 10. AIX information sources

Category	**Publication or URL**
Web Site	`http://www.ibm.com/systems/p/os/aix/`
Subsystem Device Driver (SDD, SDDPCM)	`http://www-1.ibm.com/servers/storage/support/software/sdd/`
AIX Toolbox for Linux Applications	`http://www.ibm.com/servers/aix/products/aixos/linux/download.html`

Common Information Model information sources

Table 11. Common Information Model information sources

Category	**Publication or URL**
Common Information Model	*AIX 5L™ 5.3 Common Information Model Guide*, SC23-4942
OpenPegasus	`http://www.openpegasus.org` `https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=dmp`
DMTF	`http://www.dmtf.org/standards/cim` and `http://www.dmtf.org/standards/wbem`
WBEM	`http://www.wbemsolutions.com/tutorials/CIM/cim.html`
OpenSSL	`http://www.openssl.org`
CIM Agent for DS Open API	`http://www.ibm.com/servers/storage/support/software/cimdsoapi` *IBM System Storage DS® Open Application Programming Interface Reference, Version 1 Release 2*, GC35–0516–01
CIM Agent for SVC	*IBM System Storage SAN Volume Controller, CIM Agent Developer's Reference, V4.10*, SC26–7904–00

IBM storage systems information sources

Table 12. IBM storage systems information sources

Category	**Publication or URL**
Web Site	http://www.ibm.com/storage
ESS	*IBM TotalStorage Enterprise Storage Server: Implementing CopyServices in an Open Environment*, SG24-5757.
ESS	*IBM TotalStorage Enterprise Storage Server Command-Line Interface User's Guide*, SG26-7494.
DS6000	*The IBM TotalStorage DS6000 Series: Concepts and Architecture*, SG24-6471.
DS8000	*The IBM TotalStorage DS8000 Series: Concepts and Architecture*, SG24-6452.
SAN Volume Controller	*IBM TotalStorage SAN Volume Controller: CIM Agent Developer's Reference*, SC26-7545
DS Open API and CIM Agent for DS Open API	*IBM TotalStorage DS Open Application Programming Interface Reference*, GC35-0493
SAN Volume Controller	*IBM TotalStorage SAN Volume Controller and SAN Integration Server*, SG24-6423.
SAN Volume Controller	*IBM TotalStorage SAN Volume Controller Planning Guide*, GA22-1052
SAN Volume Controller	*IBM TotalStorage SAN Volume Controller Configuration Guide*, SC26-7543
Multipathing	*IBM TotalStorage Multipath Subsystem Device Driver User's Guide*, SC30-4096
DS6000	*IBM TotalStorage DS6000 Introduction and Planning Guide*, GC26-7679

Table 12. IBM storage systems information sources (continued)

Category	Publication or URL
DS6000	*IBM TotalStorage DS6000 Messages Reference*, GC26-7682
DS8000	*IBM TotalStorage DS8000 Introduction and Planning Guide*, GC35-0495
DS8000	*IBM TotalStorage DS8000 Messages Reference*, GC26-7659
N Series	*IBM System Storage N Series*, SG24-7129.
Network Appliance (NetApp) Service and Support	https://now.netapp.com
N Series	*Quota Use Guide for NetApp Storage Systems*, Network Appliance, Inc. TR 3425
N Series	*Introduction to Data ONTAP 7G*, Network Appliance, Inc., TR 3356

SAP® information sources

Table 13. SAP® information sources

Category	Publication or URL
SAP® Service Marketplace	http://service.sap.com
SAP® Help	http://help.sap.com

Oracle information sources

Table 14. Oracle information sources

Category	Publication or URL
Web Site	http://www.oracle.com

DB2 for Linux, UNIX, and Windows information sources

Table 15. DB2 for Linux, UNIX, and Windows information sources

Category	Publication or URL
Web Site	`http://www.ibm.com/software/data/db2`
Information Center	`https://publib.boulder.ibm.com/infocenter/db2luw/v9r5/topic/com.ibm.db2.luw.doc/welcome.html`
Publications	`http://www-1.ibm.com/support/docview.wss?rs=71&uid=swg27009727`
High Availability Feature documentation	*Data Recovery and High Availability Guide and ReferenceIBM DB2 V9.5*, SC09-4831. This publication also covers DB2 Advanced Copy Services.
Native TSM Agent	*Using TSM to Back Up Databases*

Support information

You can find support information for IBM products from a variety of sources.

Getting technical training

Information about Tivoli technical training courses is available online.

Go to http://www.ibm.com/software/tivoli/education/.

Searching knowledge bases

If you have a problem with Tivoli Storage Manager, there are several knowledge bases that you can search.

You can begin with the Tivoli Storage Manager Information Center at http://publib.boulder.ibm.com/infocenter/tsminfo/v6. From this Web site, you can search all Tivoli Storage Manager publications.

Searching the Internet

If you cannot find an answer to your question in the Tivoli Storage Manager information center, search the Internet for the latest, most complete information that might help you resolve your problem.

To search multiple Internet resources, go to the support Web site for Tivoli Storage Manager at http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliStorageManager.html. From there, you can search a variety of resources including:

- IBM technotes
- IBM downloads
- IBM Redbooks®

If you still cannot find the solution to the problem, you can search forums and newsgroups on the Internet for the latest information that might help you resolve your problem. To share your experiences and learn from others in the user community, go to the Tivoli Storage Manager wiki at http://www.ibm.com/developerworks/wikis/display/tivolistoragemanager/Home.

Using IBM Support Assistant

At no additional cost, you can install on any workstation the IBM Support Assistant, a stand-alone application. You can then enhance the application by installing product-specific plug-in modules for the IBM products that you use.

The IBM Support Assistant helps you gather support information when you need to open a problem management record (PMR), which you can then use to track the problem. The product-specific plug-in modules provide you with the following resources:

- Support links
- Education links
- Ability to submit problem management reports

For more information, see the IBM Support Assistant Web site at http://www.ibm.com/software/support/isa/.

Finding product fixes

A product fix to resolve your problem might be available from the IBM Software Support Web site.

You can determine what fixes are available by checking the Web site:

1. Go to the IBM Software Support Web site at http://www.ibm.com/software/tivoli/products/storage-mgr/product-links.html.
2. Click the **Support Pages** link for your Tivoli Storage Manager product.
3. Click **Download**, and then click **Fixes by version**.

Getting e-mail notification of product fixes

You can get notifications about fixes and other news about IBM products.

To receive weekly e-mail notifications about fixes and other news about IBM products, follow these steps:

1. From the support page for any IBM product, click **My support** in the upper-right corner of the page.
2. If you have already registered, skip to the next step. If you have not registered, click **Register** in the upper-right corner of the support page to establish your user ID and password.
3. Sign in to **My support**.
4. On the My support page, click **Edit profiles** in the left navigation pane, and scroll to **Select Mail Preferences**. Select a product family and check the appropriate boxes for the type of information you want.
5. Click **Submit**.
6. For e-mail notification for other products, repeat steps 4 and 5.

Contacting IBM Software Support

You can contact IBM Software Support if you have an active IBM software maintenance contract and if you are authorized to submit problems to IBM.

Before you contact IBM Software Support, follow these steps:

1. Set up a software maintenance contract.
2. Determine the business impact of your problem.
3. Describe your problem and gather background information.

Then see “Submit the problem to IBM Software Support” on page xxi for information on contacting IBM Software Support.

Setting up a software maintenance contract

Set up a software maintenance contract. The type of contract that you need depends on the type of product you have.

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as IBM DB2® and IBM WebSphere® products that run on Microsoft® Windows® or UNIX® operating systems), enroll in IBM Passport Advantage® in one of the following ways:
  - **Online:** Go to the Passport Advantage Web page at http://www.ibm.com/software/lotus/passportadvantage/, click **How to enroll**, and follow the instructions.
  - **By Phone:** For the phone number to call in your country, go to the IBM Software Support Handbook Web page at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html and click **Contacts**.

- For server software products, you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for server software products, go to the IBM Technical support advantage Web page at http://www.ibm.com/servers/.

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. For a list of telephone numbers of people who provide support for your location, go to the Software Support Handbook page at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html.

Determine the business impact

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem you are reporting.

Severity 1	**Critical** business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
Severity 2	**Significant** business impact: The program is usable but is severely limited.
Severity 3	**Some** business impact: The program is usable with less significant features (not critical to operations) unavailable.
Severity 4	**Minimal** business impact: The problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.

Describe the problem and gather background information

When explaining a problem to IBM, it is helpful to be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently.

To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be recreated? If so, what steps led to the failure?
- Have any changes been made to the system? For example, hardware, operating system, networking software, and so on.
- Are you currently using a workaround for this problem? If so, be prepared to explain it when you report the problem.

Submit the problem to IBM Software Support

You can submit the problem to IBM Software Support online or by phone.

Online
Go to the IBM Software Support Web site at http://www.ibm.com/software/support/probsub.html. Enter your information into the appropriate problem submission tool.

By phone
For the phone number to call in your country, go to the contacts page of the IBM Software Support Handbook at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html.

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. If a workaround is possible, IBM Software Support provides one for you to implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the Tivoli Storage Manager product support Web site at http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliStorageManager.html, so that users who experience the same problem can benefit from the same resolutions.

New for Data Protection for Snapshot Devices Version 6.1

Please consult the README information and Release Notes for the current status of support for specific hardware and the full availability of specific new functionality described in this publication.

This publication is a replacement for
- *Tivoli Storage Manager for Hardware, Data Protection for FlashCopy Devices for Oracle, Installation and User's Guide* V5.3, GC32–1772–00.
- *Tivoli Storage Manager for Advanced Copy Services, Data Protection for Snapshot Devices for DB2 Advanced Copy Services, Installation and User's Guide* V5.5, SC33–8330–00.
- *Tivoli Storage Manager for Advanced Copy Services, Data Protection for Snapshot Devices, Installation and User's Guide for Oracle* V5.4, SC33–8207–01.

This information applies to the following TSM for ACS software components:
- Data Protection for Snapshot Devices for DB2 Advanced Copy Services, V6.1
- Data Protection for Snapshot Devices for *SAP® with Oracle*, V6.1
- Data Protection for Snapshot Devices for Oracle, V6.1

These components are offered as part of Tivoli Storage Manager for Advanced Copy Services, V6.1, Program Number 5608-E10, which is available as a licensed program product, and to all subsequent releases and modifications until otherwise indicated in new editions. They are successors to the following components, respectively:
- Data Protection for Snapshot Devices for DB2 Advanced Copy Services, V5.5
- Data Protection for Snapshot Devices for Oracle, V5.4
- Data Protection for Disk Storage and SAN Volume Controller for Oracle, V5.5.1

Functional Enhancements for V6.1

This section provides details of the functional enhancements for TSM for Advanced Copy Services V6.1

The following table lists the functional enhancements for V6.1 and the support provided for these functions by database environment. Ongoing indicates that support was introduced in a previous release.

Table 16. Support for the Functional Enhancements for V6.1

Enhancement	**DB2**	**Oracle**	**SAP® with Oracle**
Support for SAP® backint volume copy instead of splitint	-	-	New (see notes)
Support for native Oracle database	-	New	-
Support for raw logical volumes	-	New	-
Multiple snapshot backups	Ongoing	New	Ongoing
Add flexibility by eliminating the requirement for a TSM server in the case of snapshot backups and restores. If TSM is configured, a snapshot backup can optionally be backed up automatically to the TSM server. The TSM backup need not be scheduled.	Ongoing	New	New
Provide operations data on snapshot backups to the TSM for ERP Administration Assistant.	Ongoing	-	New
Support of IPv6	Ongoing	New	New
Support of LVM mirrored environments	Ongoing	New	Ongoing
Installation using InstallAnywhere	Ongoing	New	New
Support of incremental FlashCopy in an SVC configuration	New	New	New
Support for IBM XIV® Storage Systems	New	New	New
PPRC toleration (for ESS and DS devices only). TSM for Advanced Copy Services now permits a FlashCopy target to also be a PPRC primary.	New	New	New
Offloaded tape backup	Ongoing	New	New
New architecture for snapshot backup and restore	Ongoing	New	Ongoing

Table 16. Support for the Functional Enhancements for V6.1 (continued)

Enhancement	**DB2**	**Oracle**	**SAP® with Oracle**
N Series with NAS attachment	Ongoing	New (AIX only)	New
Notes: 1. Support for the ’splitint’ interface continues to be provided by Data Protection for Snapshot Devices for SAP® for Oracle, V5.4. 2. Support for DB2 releases prior to 9.5 continues to be provided by Data Protection for Snapshot Devices for SAP® for DB2, V5.4			

(Native Oracle) Oracle RMAN and Data Protection for Oracle continue to be employed for off-loaded tape backups and for restoring backups from TSM. They are required even if TSM is not used.

This revision also includes maintenance and editorial changes.

Other changes

- **General**
  - The information center URL has changed.
- **Changes since Data Protection for FlashCopy Devices for Oracle V5.5.1**
  - The parameters defined for the Data Protection for FlashCopy Devices for Oracle setup file have been incorporated in the Data Protection for Snapshot Devices profile. Colons are no longer used to separate the parameter name from its value.
  - The setup file is now referred to as the *profile*.
  - The profile parameter keyword PRIMARY_COPYSERVICES_SERVERNAME was changed to COPYSERVICES_PRIMARY_SERVERNAME.
  - The functions of hdworcp are now performed by the Production System User Interface (acsora).
  - The functions of hdworcb are now performed by the Offload Agent (tsm4acs).
  - The ’monitor’ function of hdworcp (now acsora) is no longer required.
  - The tracing interface implemented in Tivoli Storage Manager for Advanced Copy Services v5.5 is also employed for native Oracle.
  - Oracle Real Application Clusters (RAC) are not supported
  - The following parameters have been deleted from the profile (formerly setup file):
    - backup_destination (replaced by FLASHCOPY_TYPE and TSM_BACKUP)
    - target_volume (replaced by VOLUMES_DIR)
    - database_backup_type (replaced by extensions for TARGET_DATABASE_SUSPEND)
- **Changes since Tivoli Storage Manager for Advanced Copy Services for Oracle V5.4**
  - The profile parameter PRIMARY_COPYSERVICES_SERVERNAME was changed to COPYSERVICES_PRIMARY_SERVERNAME for naming consistency.

Chapter 1. Protection for Snapshot Devices

IBM Tivoli Storage Manager for Advanced Copy Services: Data Protection for Snapshot Devices protects DB2, SAP® with DB2, native Oracle, and SAP® with Oracle databases that reside on snapshot devices.

IBM Tivoli Storage Manager for Advanced Copy Services: Data Protection for Snapshot Devices provides online and offline backups of DB2 or Oracle databases to snapshot-oriented storage systems and Tivoli Storage Manager storage. Integration with the Oracle RMAN Media Management API maximizes the protection of data, thus providing a comprehensive storage management solution. Tivoli Storage Manager is a client-server licensed product that provides storage management services in a multiplatform computer environment. It is required only if the offload tape backup function of Data Protection for Snapshot Devices is needed. Data Protection for Snapshot Devices comprises these three database environments:

- DB2

  Note: This environment is based on DB2 Advanced Copy Services as either a native installation or one underlying an SAP installation.
- SAP® with Oracle
- Native Oracle

These databases must reside on a storage subsystem identified in "Data Protection for Snapshot Devices storage system overview" on page 24.

Overview of Data Protection for Snapshot Devices in an SAP® environment

Support for SAP® environments requires installation of the appropriate SAP-capable component of Data Protection for Snapshot Devices.

The SAP® with Oracle component requires IBM Tivoli Storage Manager for Enterprise Resource Planning. The DB2 component requires this product when an interface to Tivoli Storage Manager is needed.

SAP® with DB2 overview

Data Protection for Snapshot Devices uses specific DB2 commands for processing in an SAP® with DB2 environment.

DB2 implements the **db2 backup**, **db2 restore**, and **db2 rollforward** commands for a database backup and restore. The DB2 architecture provides these features:

- Integration of external data protection products (like Tivoli Storage Manager for ERP) to perform highly sophisticated backup and restore of DB2 data to and from a data protection server like Tivoli Storage Manager server.
- The use of an external program (like Data Protection for Snapshot Devices) or scripts. The program or script can create an image copy (by means of a FlashCopy operation of the source volumes) on the target volumes. SAP® terminology refers to this operation as splitting the disk mirrors. The program or script works with a hardware-level withdraw to release paired source volume

and target volume relationships. SAP terminology refers to this operation as a resynchronization of the disks for a new split.

Once the FlashCopy operation requested by **db2 backup** completes, the IBM Tivoli Storage Manager for Advanced Copy Services offload agent (tsm4acs) contacts DB2 in order to launch an external vendor library (such as Tivoli Storage Manager for ERP) to perform a Tivoli Storage Manager backup. Multipartition snapshot backups of SAP with DB2 databases are performed in parallel mode. The Tivoli Storage Manager for ERP and Data Protection for Snapshot Devices interfaces can be customized by modifying the profiles.

Related concepts

"Serial and parallel backup modes for DB2 database partitioning feature partitions" on page 120
DB2 backs up database partitioning feature (DPF) partitions in either serial mode or parallel mode.

"Data Protection for Snapshot Devices profile description" on page 160
Data Protection for Snapshot Devices relies on a profile in order to operate properly.

SAP® with Oracle overview

Data Protection for Snapshot Devices interfaces with BR*Tools utilities for processing in an SAP® with Oracle environment.

Oracle backup and restore

The SAP® database administration tools offer all the functions necessary to administer a database. The BR*Tools for Oracle, (BRBACKUP, BRARCHIVE, BRRESTORE, BRRECOVER) provide for online or offline, partial or full backup of tablespaces (done by BRBACKUP), backup of archived redo log files (done by BRARCHIVE) and system-guided restore and recover capabilities (done by BRRESTORE and BRRECOVER).

Data Protection for Snapshot Devices and BACKINT

BR*Tools use tables in the Oracle database and system data in order to record the status of the data file and logfile backups. This information will allow SAP to automatically restore the correct data files and their specific database transaction log files (redo log files), if necessary. The data files reside in the Oracle database (Oracle instance). Tivoli Storage Manager for Advanced Copy Services runs as a separate process, independently from the database environment. It receives the data through the BACKINT interface and saves the data to the Tivoli Storage Manager.

As of BR*Tools 7.10, Data Protection for Snapshot Devices interfaces with backint calls from BR*Tools that specify a volume (snapshot) copy.

A backup run will proceed as follows:

1. The BR*Tools utility BRBACKUP informs Oracle what data has to be backed up and puts the database into the proper backup state ('online' or 'offline').
2. BRBACKUP calls Data Protection for Snapshot Devices via the BACKINT interface with a list of volumes to be backed up.
3. Data Protection for Snapshot Devices performs the snapshot backup and reports back to BRBACKUP.

4. Data Protection for Snapshot Devices also saves the data to Tivoli Storage Manager (if this option was selected) via Tivoli Storage Manager for Enterprise Resource Planning.
5. BR*Tools update the file repository containing information on the backup status.

Overview of the integrated DB2 Advanced Copy Services and Data Protection for Snapshot Devices environment

Data Protection for Snapshot Devices operates in an environment integrated with the DB2 functional subset that is represented by DB2 Advanced Copy Services.

Data Protection for Snapshot Devices serves as a functional extension of DB2 Advanced Copy Services and offers the following enhancements:

- Offloaded transfer of backup data from the DB2 database server to Tivoli Storage Manager. The source for this transfer is a snapshot backup previously generated by DB2 Advanced Copy Services. The tape backup can be integrated with the request to generate the snapshot backup.
- Unlimited number of snapshot versions
- Incremental and ″no copy″ FlashCopy® variants (INCR, NOCOPY)
- Snapshot backup from a mirror set managed by the AIX® Logical Volume manager (LVM) mirroring function (except N Series devices), and corresponding snapshot restore
- Support for the Journaled File System (JFS)

The term *DB2 Advanced Copy Services* applies to the software components delivered by DB2 as part of the DB2 High Availability Feature. These components are updated when Data Protection for Snapshot Devices is installed and are then referred to as the *DB2 Advanced Copy Services components of Data Protection for Snapshot Devices*. Unless otherwise stated, information in this book not specifically related to the enhanced functions above applies to both Data Protection for Snapshot Devices and DB2 Advanced Copy Services. When *DB2 Advanced Copy Services* is used to refer to the software *without* Data Protection for Snapshot Devices, this is explicitly stated.

The DB2 version of IBM Tivoli Storage Manager for Advanced Copy Services (Data Protection for Snapshot Devices) is a licensed, functionally enhanced version of the DB2 Advanced Copy Services product initially provided with DB2 Enterprise version 9.5. Conversely, DB2 Advanced Copy Services can be regarded as a functionally restricted version of IBM Tivoli Storage Manager for Advanced Copy Services. An existing DB2 Advanced Copy Services installation can be upgraded to IBM Tivoli Storage Manager for Advanced Copy Services. Once IBM Tivoli Storage Manager for Advanced Copy Services has been installed, support for the basic DB2 Advanced Copy Services functionality and upgraded features are then provided within the context of IBM Tivoli Storage Manager for Advanced Copy Services and not DB2.

The following table lists the primary differences between these two environments:

Table 17. Functional Comparison of DB2 Advanced Copy Services and Data Protection for Snapshot Devices

Function	**DB2 Advanced Copy Services**	**IBM Tivoli Storage Manager for Advanced Copy Services: Data Protection for Snapshot Devices**
Multiple snapshot versions	Limited to 2	No limit imposed by software
Incremental or "no copy" FlashCopy	No support	Supported.
LVM mirroring	A snapshot of both mirrors will be done.	A snapshot from one mirror set is possible (except N Series devices)
Integrated snapshot and tape backup	No support	Supported
Backup from secondary host	No support	Supported
Support for Journaled File System (JFS)	No support (JFS2 only)	JFS (requires backup server) and JFS2

After installing or upgrading to IBM Tivoli Storage Manager for Advanced Copy Services, future updates are done through IBM Tivoli Storage Manager for Advanced Copy Services channels and not through DB2 fix packs.

Note: Customers requiring a version of DB2 prior to 9.5 can continue to use Data Protection for Snapshot Devices for DB2, V5.4.

Common functions overview: DB2 Advanced Copy Services and Data Protection for Snapshot Devices

Functionality shared between DB2 Advanced Copy Services and Data Protection for Snapshot Devices is identified.

High-availability DB2 database backup using snapshot techniques

The DB2 Advanced Copy Services component of Data Protection for Snapshot Devices accomplishes high-availability backups of a DB2 database implemented on snapshot devices. When performing the snapshot copy of all volumes involved, DB2 suspends all write activity on the production database but still allows the database to be read. The target volumes of the snapshot operation can then be backed up to tape (using `tsm4acs`, for example). Multiple disk copy backup sets (one set per backup run) can be created and kept for restore purposes. DB2 Advanced Copy Services limits the number of such sets to two.

High-availability DB2 database restore using snapshot techniques

DB2 Advanced Copy Services provides high-availability restore operations for a DB2 database implemented on snapshot devices. The program uses the volumes of a previous snapshot backup to restore the DB2 database on the production system. Afterward, the production system is cleaned up. This means that all database file systems are unmounted from the production system and all database volume groups are exported from the production system. After the cleanup, DB2 Advanced Copy Services initiates a FlashCopy of an existing snapshot backup from the target volumes to the production system source volumes. Then, all database volume groups are imported and all database file systems mounted again. This greatly reduces the downtime of the production database server. Depending on the storage system and possibly the microcode level, a snapshot type COPY or INCR (incremental) is used for the restore. INCR is not supported by DB2 Advanced

Copy Services and requires the use of Data Protection for Snapshot Devices. A restore or recovery operation must be performed on the production system using these components:

- Snapshot restore: use DB2 and DB2 Advanced Copy Services
- Restore of a native DB2 database from Tivoli Storage Manager: use DB2 and the DB2 native Tivoli Storage Manager agent
- Restore of an SAP database from Tivoli Storage Manager: use IBM Tivoli Storage Manager for Enterprise Resource Planning.

Support for environments set up with enhanced concurrent capable volume group(s)

When performing a snapshot restore on a production system that runs HACMP™ together with enhanced concurrent capable volume groups, all LVM changes are properly propagated to the takeover system. DB2 Advanced Copy Services and Data Protection for Snapshot Devices provide the 'acsvg.sh' script to accomplish this type of snapshot restore.

Related concepts

"Overview of multiple backup generations (target sets) on disk" on page 37
Information is provided to assist in maintaining multiple backup generations.

Related tasks

"Data Protection for Snapshot Devices installation prerequisites" on page 66
Storage system and microcode level requirements are provided in regard to snapshot COPY or INCR type restore operations.

Related reference

"Volume Group Takeover Script (acsvg.sh)" on page 147
Overview information regarding this script is provided.

Additional functions overview: Data Protection for Snapshot Devices for DB2

An overview of the functions provided by Data Protection for Snapshot Devices and its user interface (tsm4acs) are provided.

Data Protection for Snapshot Devices enhances the basic functions offered by DB2 Advanced Copy Services as follows:

- Integrated snapshot and Tivoli Storage Manager backup
- Tivoli Storage Manager backup from an existing snapshot copy
- Incremental FlashCopy backup and restore
- (SAP) Integrates with the operations monitor of the Tivoli Storage Manager for ERP Administration Assistant.
- Integration with Tivoli Storage Manager Media Management functions
- Multiple snapshot versions
- LVM mirroring support
- Support for JFS

Integrated snapshot and Tivoli Storage Manager backup

Data Protection for Snapshot Devices supports a combined request to back up a DB2 database as a snapshot and on tape using Tivoli Storage Manager. This is accomplished by setting the TSM_BACKUP parameter in the profile or defining it as a vendor option in the command line. For example:

```
db2 backup database...use snapshot...options "TSM_BACKUP"
```

When the snapshot backup has been completed, Data Protection for Snapshot Devices initiates the tape backup request by invoking Tivoli Storage Manager for ERP or the DB2 native Tivoli Storage Manager agent as the Tivoli Storage Manager interface. The source for this backup is the set of target volumes from the snapshot backup.

Incremental or ″no copy″ FlashCopy backup and restore

Data Protection for Snapshot Devices allows the point-in-time copy of a DB2 database implemented on directly attached ESS, DS, and SVC 4.2.1 systems using the Incremental FlashCopy or ″no copy″ features. This feature make it possible to perform a background copy between the source and target volumes without having to copy all the tracks in the process. This results in improved performance for the DB2 servers that are configured to the storage system. Incremental FlashCopy applies only to the storage hardware level copy (the FlashCopy operation performed between the source volumes and target volumes). It does not apply to the application level copy (the backup copy of the database to the Tivoli Storage Manager server).

An incremental or ″no copy″ FlashCopy backup is invoked with the respective values INCR or NOCOPY for FLASHCOPY_TYPE in the Data Protection for Snapshot Devices profile or the applicable DB2 command line OPTIONS string.

Note: Incremental or ″no copy″ FlashCopy is not supported by DB2 Advanced Copy Services.

LVM mirroring support

Data Protection for Snapshot Devices currently supports AIX LVM mirroring only for FlashCopy devices. The use of LVM mirroring in an SAN Volume Controller configuration requires that the mirror sets be in different SAN Volume Controller clusters.

Centrally Administered and Scheduled Backup Operations

Unattended DB2 backups can be scheduled via crontab or from the Tivoli Storage Manager server. You can select when the backups occur without waiting for off-peak hours or maintenance downtime.

Common Data Protection for Snapshot Devices components

A description of the software components that are shared by the individual database-platform versions of Data Protection for Snapshot Devices are provided.

Application Client

The Application Client provides the necessary support for implementing snapshot-based backup and restore.

(DB2) The client is implemented as the *Snapshot Backup Library* (referred to as a *vendor library* in DB2 terms). The library is also a component of DB2 Advanced Copy Services and is invoked by using the `"... use snapshot..."` phrase in the `'db2 backup database'` or `'db2 restore database'` commands.

(Oracle, SAP with Oracle) The client functions are integrated in the software.

Management Agent (acsd)
The Management Agent (acsd) coordinates the backup operation. It also coordinates multi-partition backups for DB2. It controls the backup flow and mediates between the application and device agents. The Management Agent also provides access to the snapshot backup repository which contains information about the valid snapshot backups and their relationships to snapshot-capable storage devices. There is one Management Agent per DB2 instance in a DB2 environment, is typically started from `/etc/inittab`, and must be started on one machine only. The Management Agent can also be run in password mode for the purpose of changing passwords related to the Data Protection for Snapshot Devices environment.

Device Agent for CIM Devices (acscim)
The Device Agent for CIM Devices (acscim) is the component that invokes a snapshot command on a FlashCopy device (such as ESS800, DS6000, DS8000 and SAN Volume Controller) using the CIM interface. This agent is also used to update the progress and usability information that is stored in the local snapshot backup repository.

Device Agent for N Series Devices (acsnnas, acsnsan)
The Device Agent for N Series Devices (acsnnas or acsnsan, depending on the attachment method) is the component that invokes a snapshot command on a snapshot capable device (such as N Series) using the NetApp ONTAPI interface. This agent is also used to update the progress and usability information that is stored in the local snapshot backup repository.

Device Agent for IBM XIV® Storage System Devices (acsxiv)
The Device Agent for IBM XIV® Storage System Devices (acsxiv) is the component that invokes a snapshot command on a snapshot capable device using XivAdapter.jar. This agent is also used to update usability information about the corresponding snapshot backup that is stored in the (local) snapshot backup repository.

XIV Adapter Java Archive (XivAdapter.jar)
The XIV Adapter is used in conjunction with the Device Agent for IBM XIV® Storage System Devices (acsxiv). It communicates with acsxiv and issues commands to the XIV® command line interface (xcli).

Disk Mapper script (acsdm.sh)
The Disk Mapper (acsdm.sh) is a shell script that provides disk mapping information such as the DS device volume serial numbers that are linked to AIX vpaths and hdisks. This script is called by acscim or acsnsan during snapshot backup and restore operations.

Volume Group Takeover script (acsvg.sh)
The Volume Group Takeover utility (acsvg.sh) is a shell script that is required only in special high-availability scenarios in which enhanced concurrent capable volume groups are used on production systems. In these situations, this script exports and re-imports the volume groups on an HACMP takeover system after a snapshot restore is performed. This process is necessary in order to synchronize the AIX Object Data Manager (ODM) on the production and HACMP takeover systems.

Offload Agent (tsm4acs)
The primary role of the Offload Agent is to provide a single user interface

for backing up an existing snapshot to Tivoli Storage Manager. In the DB2 version, the Offload Agent provides additional functionality similar to DB2 Advanced Copy Services. Data Protection for Snapshot Devices for DB2 Advanced Copy Services includes a license file that enables use of the enhanced functions of the Offload Agent in conjunction with DB2 Advanced Copy Services. The Offload Agent must be installed on each backup system in the system landscape. On a backup server, it also calls the device agent for mount and unmount operations.

Data Protection for Snapshot Devices for DB2 software environment

Data Protection for Snapshot Devices requires specific software to be available in a DB2 environment.

Data Protection for Snapshot Devices for DB2 Advanced Copy Services runs in the following software environment:

- AIX
- Linux®
- DB2 V9.5 (or higher)
- DB2 Advanced Copy Services (included in the DB2 High Availability Feature)
- Tivoli Storage Manager server (optional)
- IBM Tivoli Storage Manager for Advanced Copy Services
- Common Information Model (CIM), for FlashCopy devices
- SAP (optional)
- IBM Tivoli Storage Manager for Enterprise Resource Planning is required by the SAP with Oracle component. It is needed in the DB2 environment if offloaded backups of snapshots to Tivoli Storage Manager are desired.
- DB2 native Tivoli Storage Manager Agent (required in a native DB2 environment for offloaded backup of snapshot to Tivoli Storage Manager)

Data Protection for Snapshot Devices for DB2 operating environment

Data Protection for Snapshot Devices uses a backup system and a production system in a DB2 operating environment.

The operating environment consists of the DB2 relational database management system (RDBMS) running on a server attached to one of the supported storage systems. This server is referred to as the *production system*. Another server, referred to as the *backup system*, can also be attached to the same storage system. The backup system is used to verify the consistency of a DB2 database backup implemented on volumes within a Journaled File System (JFS), participating in AIX logical volume manager mirroring, or for offloading the DB2 database snapshot backup to a Tivoli Storage Manager server. Data Protection for Snapshot Devices initiates appropriate external commands that invoke the Tivoli Storage Manager interface. In an SAP environment, this is provided by IBM Tivoli Storage Manager for Enterprise Resource Planning Tivoli Storage Manager for ERP. In a native DB2 environment, this is provided by the DB2 native Tivoli Storage Manager agent.

The following illustration displays a CIM setup in which the DB2 Advanced Copy Services vendor library (libacsdb2) and the DB2 Advanced Copy Services device agent (acscim) are collocated with the DB2 Advanced Copy Services management agent (acsd) and a device agent running in daemon mode. The IBM Tivoli Storage

Manager for Advanced Copy Services offload agent (tsm4acs) must be installed on the backup servers. On the backup server, tsm4acs calls the device agent for operations such as mount and unmount.

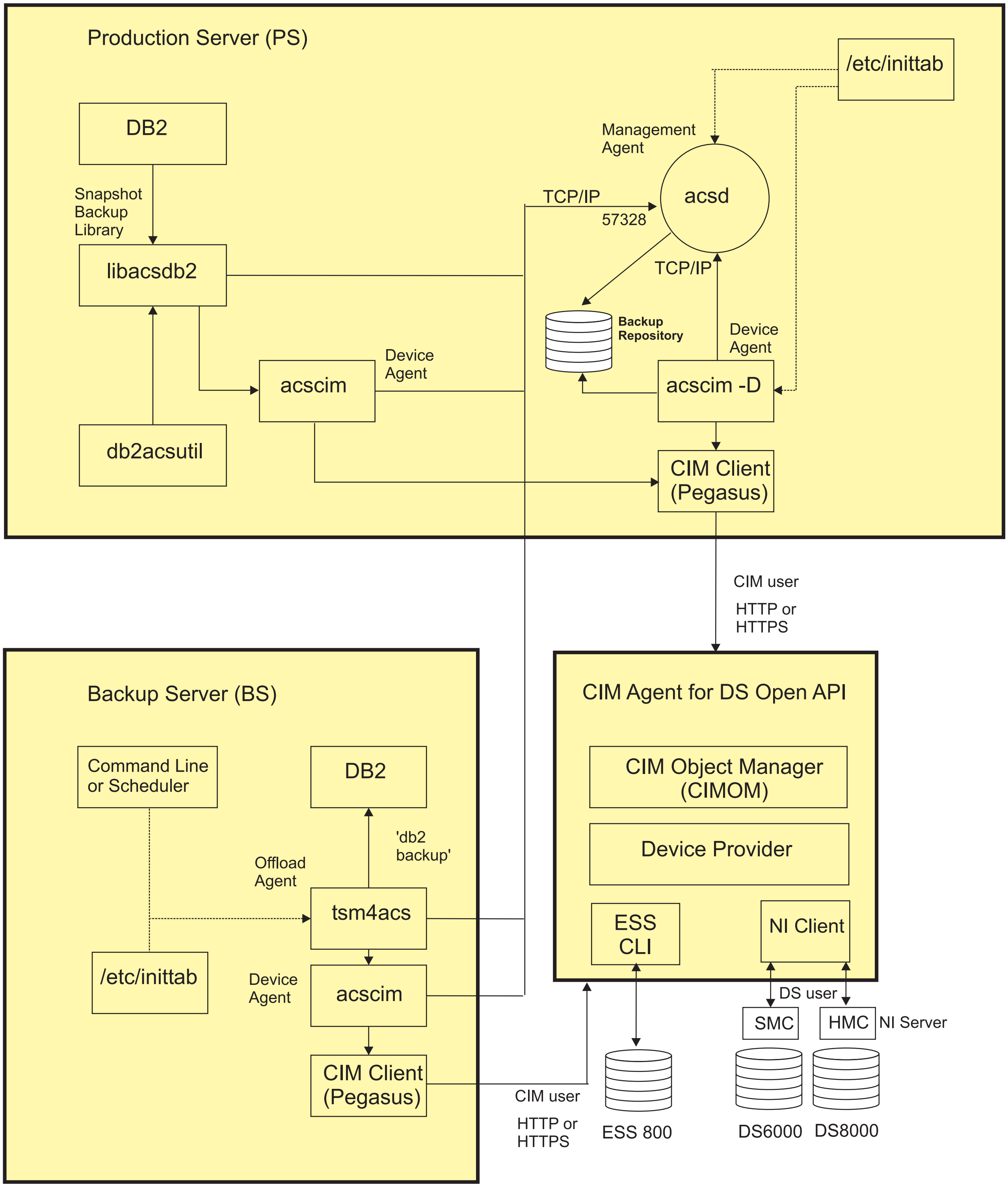


Figure 1. Overall Data Protection for Snapshot Devices and DB2 Environment Using CIM

Offload Agent (tsm4acs) functions

The Offload Agent (tsm4acs) augments the basic capabilities provided by DB2 Advanced Copy Services in a DB2 environment.

- Integrated snapshot and Tivoli Storage Manager backup
- Tivoli Storage Manager backup from an existing snapshot copy
- Incremental FlashCopy backup and restore
- (SAP) If Tivoli Storage Manager for ERP is being used, providing data to the Tivoli Storage Manager for ERP Administration Assistant concerning snapshot backups and restores. Seamless augmentation of the functions of Tivoli Storage Manager for ERP.
- Integration with Tivoli Storage Manager Media Management functions
- Multiple snapshot versions
- LVM mirroring support
- Support for JFS

Note: (DB2) tsm4acs augments the basic capabilities provided by DB2 Advanced Copy Services.

Tivoli Storage Manager overview

Tivoli Storage Manager is a client and server program that provides storage management services in a multivendor, multiplatform computer environment.

Tivoli Storage Manager provides these services:

Reduces Network Complexity

Tivoli Storage Manager reduces network complexity with interfaces and functions that span network environments. This provides consistency across different operating systems and hardware.

Increases Administrator Productivity

Tivoli Storage Manager can reduce the cost of network administration by allowing administrators to:

- automate repetitive processes
- schedule unmanned processes
- administer Tivoli Storage Manager from anywhere in the network

Reduces the Risk of Data Loss

Many users do not back up their data. Other users apply stand-alone backup techniques with diskettes and tapes as the only protection for business data. These backup systems often produce disappointing results during recovery operations. Tivoli Storage Manager schedules routine backups that enable users to recover from accidental data deletion without administrator involvement.

Backup and Restore Services

Backup and restore services allow backup-archive clients to generate backup copies of data at specified intervals and restore the data from these copies when required. These services protect against workstation or file server media failure, accidental file deletion, data corruption, data vandalism, or site-wide disasters.

Archive and Retrieval Services

Archive and retrieval services provide backup-archive clients with image copies of data for long-term storage. (SAP) Tivoli Storage Manager uses these services to generate backup copies of data at specific intervals and restore the data from these copies when required. These services protect against workstation or file server media failure, accidental file deletion, data corruption, data vandalism, or site-wide disasters.

Automation Services

Tivoli Storage Manager administrators can increase productivity by automating common storage administration tasks.

Administration Services

Tivoli Storage Manager administration services provide support for routine monitoring, administration, and accounting. Administrators can manage the server from another system or the same system. The Tivoli Storage Manager utilities allow the administrator to perform these functions:

- Define devices
- Label tape volumes
- Add clients
- Format storage volumes
- Set client and server options

Tivoli Storage Manager monitors scheduled operations and maintains status information in the database. An administrator can export data to removable media. This data can be imported by another server, making the export and import features a convenient utility for moving server data. The administrator can specify the accounting option generated at the end of each client session.

Security Services

Security services control user access to Tivoli Storage Manager data, storage, policy definitions, and administrative commands.

Disaster Recovery Services

Disaster recovery services help the administrator implement a comprehensive backup and recovery procedure for important business applications, data, and records.

Integrated snapshot and Tivoli Storage Manager backup

Data Protection for Snapshot Devices supports a combined (integrated) request to back up a database as a snapshot and also on tape through Tivoli Storage Manager.

This is accomplished by setting the TSM_BACKUP (or TSM_BACKUP_FROM_SNAPSHOT) parameter in the profile or defining it as an option in the command line. When the snapshot backup has been completed, Data Protection for Snapshot Devices initiates the tape backup request by invoking the following as the Tivoli Storage Manager interface:

- Tivoli Storage Manager for ERP in an SAP environment (DB2 or Oracle)
- the DB2 native Tivoli Storage Manager agent in a native DB2 environment
- Oracle RMAN in a native Oracle environment

The source for this backup is the set of target volumes from the snapshot backup.

Incremental or ″No Copy″ FlashCopy backup and restore

Data Protection for Snapshot Devices using the FlashCopy incremental or ″no copy″ features to create a point-in-time copy of a database implemented directly on attached FlashCopy or SAN Volume Controller systems.

This feature makes it possible to perform a background copy between the source volumes and target volumes without having to copy all of the tracks in the process. This results in improved performance for the database servers that are configured with the storage system. Incremental FlashCopy applies only to the storage hardware level copy (the FlashCopy done between the source volumes and target volumes). It does not apply to the application level copy, which id the backup copy of the database to the Tivoli Storage Manager server.

An incremental or ″no copy″ FlashCopy backup is invoked with the respective values INCR or NOCOPY for FLASHCOPY_TYPE in the Data Protection for Snapshot Devices profile or the applicable command line OPTIONS string.

Incremental or ″no copy″ FlashCopy is not supported by DB2 Advanced Copy Services.

Seamless augmentation of the functions of Tivoli Storage Manager for Enterprise Resource Planning

Seamless augmentation is an important Tivoli Storage Manager for Enterprise Resource Planning feature.

In an SAP® environment, on request of tsm4acs, Tivoli Storage Manager for Enterprise Resource Planning running on another system (backup system) can perform the backup of the database from the target volumes, which are images of the source volumes.

Related concepts

"Overview of Data Protection for Snapshot Devices in an SAP® environment" on page 1
Support for SAP® environments requires installation of the appropriate SAP-capable component of Data Protection for Snapshot Devices.

Integration with Tivoli Storage Manager media management functions

Tivoli Storage Manager for Enterprise Resource Planning supports many Tivoli Storage Manager functions.

In an SAP environment, working together with Tivoli Storage Manager for Enterprise Resource Planning, all Tivoli Storage Manager storage devices and media management capabilities can be utilized. The devices can be shared for other backups or to give DB2 exclusive use of certain devices and media. Life cycle management of the media and generation of tape copies for off-site vaulting are also supported.

Centrally administered and scheduled backup operations

Consider using scheduled backup operations in your backup strategy.

Unattended database backups can be scheduled using the `crontab` command or from the Tivoli Storage Manager server. You can select when the backups occur without waiting for off-peak hours or maintenance downtime.

IBM Subsystem Device Driver support

Data Protection for Snapshot Devices provides support for IBM Subsystem Device Driver (SDD).

SDD resides on the host servers (production system and backup system) with the native device driver for the storage system. SDD uses redundant connections between the host server and disk storage in a storage system to provide enhanced performance and data availability. Refer to your SDD documentation for further information. Note that SDD is required for SAN VC. Use SDD only if your configuration has two or more paths to the storage subsystem from each host. SDD does not support a single path to the storage subsystem.

Data consistency

Data Protection for Snapshot Devices backup processing can fail when file systems used during snapshot processing are inconsistent.

To guarantee the consistency of the data processed by Data Protection for Snapshot Devices, several techniques are utilized. JFS2 file systems offer the capability to stop all I/O operations on the file systems on request. This process is called *freeze* and is activated using the profile parameter LVM_FREEZE_THAW. For file systems that do not provide such capabilities, the volumes are imported on the backup server and the file systems are mounted to verify their consistency.

Data Protection for Snapshot Devices for Oracle overview

Data Protection for Snapshot Devices performs backup and restore functions for a native Oracle (non-SAP) database environment.

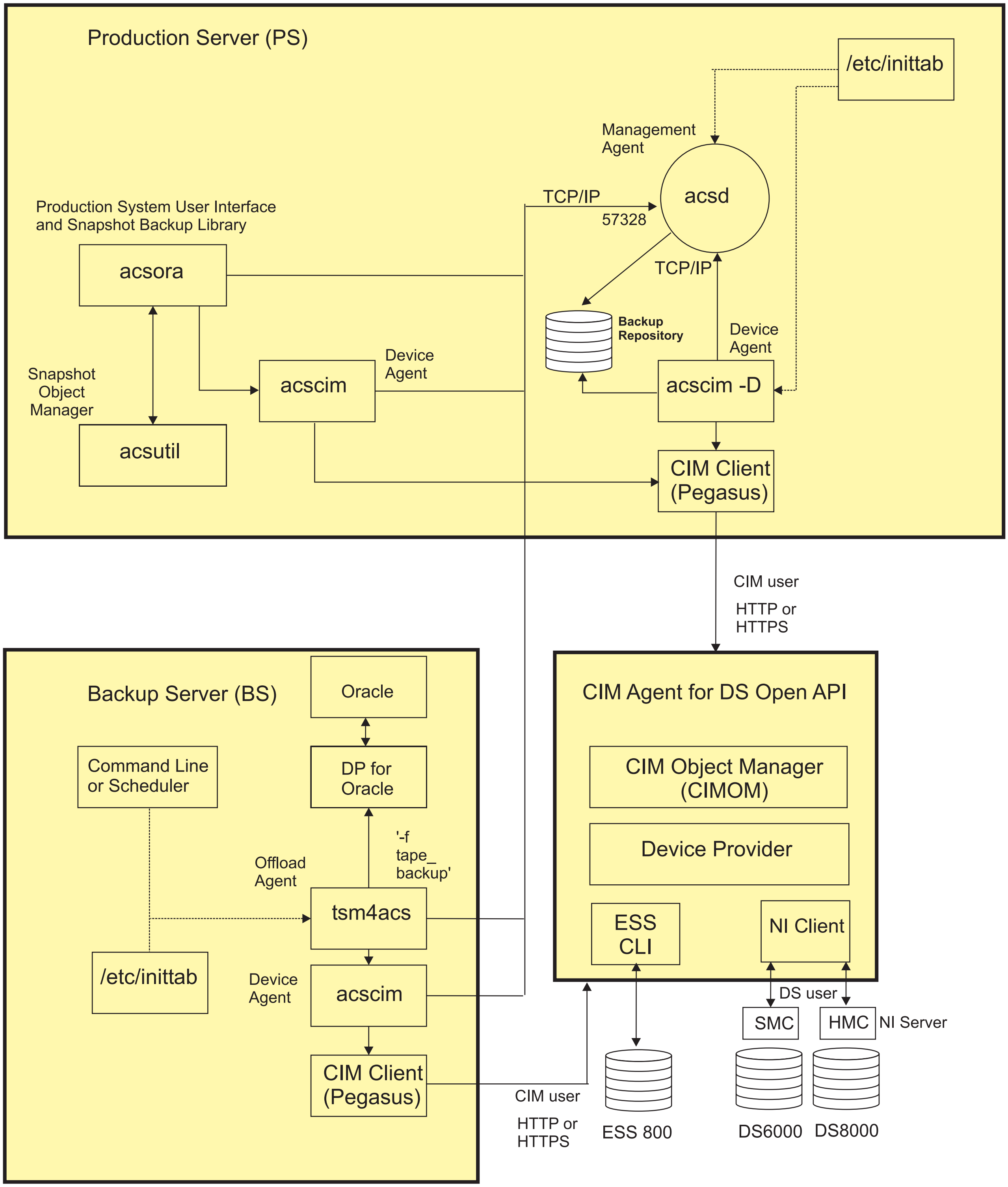


Figure 2. Overall Data Protection for Snapshot Devices and native Oracle environment using CIM

Data Protection for Snapshot Devices for a native (non-SAP) Oracle database environment provides these functions:

- Back up Oracle databases with minimal impact and downtime on the production Oracle database server.
- Back up as snapshots or to Tivoli Storage Manager, or both

- Restore Oracle databases from Tivoli Storage Manager storage to the production system.
- Perform a *snapshot restore* of your Oracle database from the backup image on the target volumes to the production system.
- Automate backup operations.
- Integrate with Tivoli Storage Manager Media Management functions, if Tivoli Storage Manager is used.
- Support IBM Subsystem Device Driver (SDD) functions.

Data Protection for Snapshot Devices for Oracle limitations

There are certains limitations to consider for Data Protection for Snapshot Devices in a native Oracle environment.

The Data Protection for Snapshot Devices for Oracle configuration imposes the following restrictions:

- Symbolic links are not supported in the Oracle database directory structure.
- When a configuration consists of Oracle database files in one volume group and Oracle control and redo log files in another volume group, Data Protection for Snapshot Devices does not support the nesting of Oracle control and redo log files as a mounted file system within the file system containing the Oracle database files.
- Oracle database files cannot be distributed between SVC 4.2.0 and 4.2.1.

Data Protection for Snapshot Devices for Oracle migration considerations

There are specific guidelines to consider when migrating Data Protection for Snapshot Devices in a native Oracle environment.

Databases backed up with a previous version of Data Protection for Snapshot Devices in a native Oracle environment cannot be restored directly with Data Protection for Snapshot Devices Version 6.1. These existing databases can be restored using one of the following methods:

- Use RMAN and Data Protection for Oracle to restore the databases from Tivoli Storage Manager storage.
- You can use Data Protection for Snapshot Devices for Oracle 5.5 and Data Protection for Snapshot Devices for Oracle 6.1 concurrently, until the target set used with Data Protection for Snapshot Devices for Oracle 5.5 is used to create a new backup with Data Protection for Snapshot Devices for Oracle 6.1.

Data Protection for Snapshot Devices for Oracle software environment

Data Protection for Snapshot Devices requires specific software when operating in a native Oracle environment.

Data Protection for Snapshot Devices for native Oracle operates in the following software environment:

- AIX
- Oracle
- Oracle RMAN
- Tivoli Storage Manager server (optional)

- IBM Tivoli Storage Manager for Advanced Copy Services (Data Protection for Snapshot Devices)
- Common Information Model (CIM), for FlashCopy devices
- Tivoli Storage Manager for Databases Data Protection for Oracle

Integration environment overview: Data Protection for Snapshot Devices and Data Protection for Oracle

Data Protection for Oracle supports Oracle databases with the RMAN utility.

RMAN backs up and restores Oracle databases in both online and offline settings. When RMAN initiates a backup or restore, Data Protection for Oracle acts as the interface to the Tivoli Storage Manager server by translating Oracle API commands into Tivoli Storage Manager API calls to the Tivoli Storage Manager server. The Tivoli Storage Manager server then applies administrator-defined storage management policies to the data.

Data Protection for Snapshot Devices for Oracle features

Oracle database backup

Data Protection for Snapshot Devices can backup single or multiple Oracle databases.

Although Data Protection for Snapshot Devices uses a single backup system, you can perform a snapshot backup of multiple Oracle databases. These databases can reside on either a single production system or multiple production systems. However, you cannot back up multiple databases concurrently using a single backup system. Backups of multiple databases must be serialized when using a single backup system.

Oracle snapshot backup:

Data Protection for Snapshot Devices uses snapshot copy techniques to create a point-in-time copy of database volumes from the Oracle production system.

The copied database volumes are then optionally made available for back up to a Tivoli Storage Manager server by a secondary host (backup system) running Data Protection for Oracle. Because the backup system performs most of the processing, the production system can dedicate processor time to other applications. This greatly reduces any backup-related performance impact on the production system.

Although Data Protection for Snapshot Devices uses a single backup system, you can perform a snapshot backup of multiple Oracle databases. These databases can reside on either a single production system or multiple production systems. However, you cannot back up multiple databases concurrently using a single backup system. Backups of multiple databases must be serialized when using a single backup system.

Oracle database restore

Data Protection for Snapshot Devices can restore single or multiple Oracle databases.

Oracle snapshot restore:

Data Protection for Snapshot Devices uses snapshot copy techniques to restore an Oracle database from a selected snapshot image available on the target volumes.

This feature provides a quick recovery of the production database in the event of a major failure. It also provides a restore of the storage structures of the operating system that may have been lost after the original backup, such as the table space containers or file systems.

Restore from Tivoli Storage Manager:

Data Protection for Snapshot Devices uses the Oracle RMAN utility, in conjunction with Data Protection for Oracle, to perform restore procedures from Tivoli Storage Manager server storage.

After initiating a restore with the RMAN utility, Data Protection for Oracle uses the Tivoli Storage Manager API to interface with the Tivoli Storage Manager server to transmit data. As a result, Data Protection for Snapshot Devices supports multiple parallel restores.

Incremental snapshot backup and restore

Data Protection for Snapshot Devices allows the point in time copy of an Oracle database using the IBM incremental FlashCopy feature.

This feature makes it possible to perform a background copy between the source and target volumes without having to copy all the tracks from the source volumes to the target volumes. This results in improved performance for the Oracle servers that are configured with FlashCopy devices. Incremental FlashCopy applies only to the storage hardware level copy (the FlashCopy made between the source volumes and target volumes). Incremental FlashCopy does not apply to the application level copy (the backup copy of the database to the Tivoli Storage Manager server).

Use the incremental FlashCopy for backups and restores during normal production operations. FlashCopy background copy processing normally takes several hours to complete, and this time can increase with larger databases. With FlashCopy, the production database server is available immediately after the FlashCopy is initiated (a process that lasts only a few minutes). As a result, background copy processing does not affect the availability of the production database server. However, you cannot perform a snapshot restore or another FlashCopy backup while the background copy for the previous backup is still processing. Thus by using the incremental FlashCopy feature, you can have a backup version available for snapshot restore sooner and are also able to schedule backups more frequently. Note that if an entire database is lost, the snapshot restore will be a full volume background copy. Use of the incremental FlashCopy feature also improves the performance of the storage subsystem as there is less data to be copied from the source volumes to the target volumes.

Scheduled backups

You can schedule automated Oracle backups from the Tivoli Storage Manager server.

You can select when the backups occur without waiting for off-peak hours or maintenance downtime.

Integration with Tivoli Storage Manager

All Tivoli Storage Manager storage devices and media management capabilities are available to Data Protection for Snapshot Devices.

You can share the devices used for other backups or give Oracle exclusive use of certain devices and media. Data Protection for Snapshot Devices supports media and tape management for off-site vaulting.

IBM Subsystem Device Driver support

Data Protection for Snapshot Devices provides support for IBM Subsystem Device Driver (SDD).

SDD resides on the host servers (production system and backup system) with the native device driver for the storage system. SDD uses redundant connections between the host server and disk storage in a storage system to provide enhanced performance and data availability. Refer to your SDD documentation for further information. Note that SDD is required for SAN VC. Use SDD only if your configuration has two or more paths to the storage subsystem from each host. SDD does not support a single path to the storage subsystem.

Data consistency

Data Protection for Snapshot Devices backup processing can fail when file systems used during snapshot processing are inconsistent.

To guarantee the consistency of the data processed by Data Protection for Snapshot Devices, several techniques are utilized. JFS2 file systems offer the capability to stop all I/O operations on the file systems on request. This process is called *freeze* and is activated using the profile parameter LVM_FREEZE_THAW. For file systems that do not provide such capabilities, the volumes are imported on the backup server and the file systems are mounted to verify their consistency.

Data Protection for Snapshot Devices for *SAP® with Oracle* overview

Data Protection for Snapshot Devices in SAP® environments with Oracle databases uses the backint interface extensions provided by BR*Tools 7.10 and higher.

Notes:

- Tivoli Storage Manager for Enterprise Resource Planning V6.1 is a prerequisite for using this Data Protection for Snapshot Devices component.
- Customers who want to use the ’splitint’ interface instead of ’backint’ should use Tivoli Storage Manager for Advanced Copy Services V5.4 instead.

This interface is conceptually similar to that employed by IBM Tivoli Storage Manager for Enterprise Resource Planning in that Data Protection for Snapshot Devices presents itself as the executable file ’backint’, which is called by SAP when one of these BR*Tools utilities is invoked by the user:

- BRBACKUP
- BRRESTORE

- BRARCHIVE
- BRRECOVER

The previous versions of Data Protection for Snapshot Devices for Oracle (through version 5.4) employed a different SAP interface (’splitint’) to implement snapshot backups and restores. As a result, Data Protection for Snapshot Devices version 6.1 is a new implementation although the storage system interface is basically the same.

The following figure depicts the overall Data Protection for Snapshot Devices configuration in an SAP environment with an Oracle database:

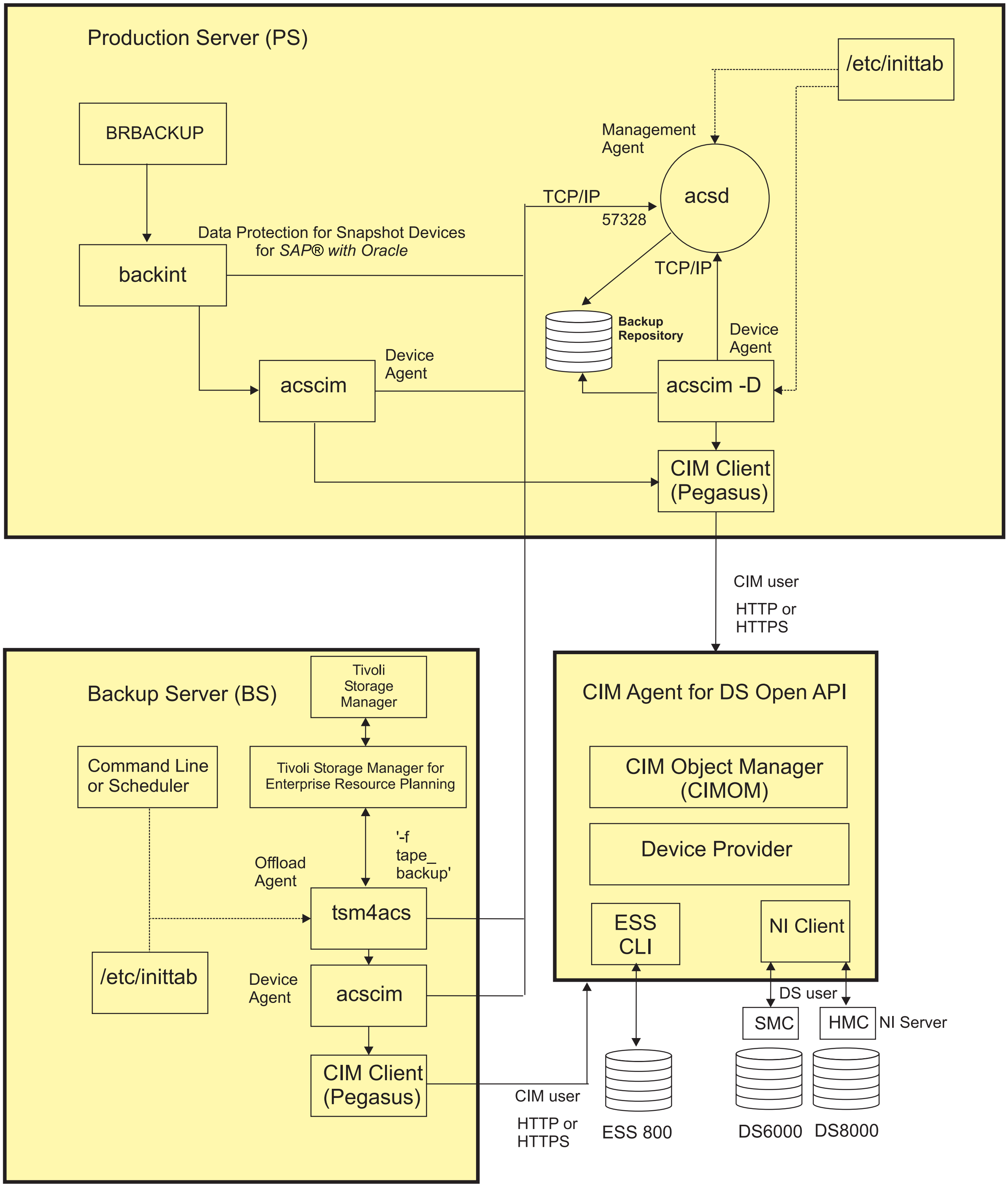


Figure 3. Overall Data Protection for Snapshot Devices and SAP with Oracle Environment Using CIM

Beginning with BR*Tools 7.10, SAP provides an extension to the backint interface that allows the direct creation of snapshot backups. These extensions to the BACKINT interface have the following objectives:

- Better support of snapshot and cloning technology, which is increasingly becoming the industry standard

- Simplified interface
- Stronger integration with SAP.
- Ability to handle more complex restore scenarios.
- Use of BRRECOVER procedures for backup based on snapshot and cloning technologies

Compared to the splitint interface, the backint interface supports snapshot restore operations more directly. In addition, the new interface is more naturally integrated into the conventional backup procedures and thus simplifies operations from a user perspective.

The interface has the following objectives:
- A user who purchases IBM Tivoli Storage Manager for Enterprise Resource Planning Tivoli Storage Manager for Enterprise Resource Planning can perform conventional backups to a Tivoli Storage Manager server
- A user who purchases both IBM Tivoli Storage Manager for Enterprise Resource Planning and IBM Tivoli Storage Manager for Advanced Copy Services can create both conventional and snapshot backups. The snapshot backups can also be used to offload a backup from a local system to a remote machine.
- In accordance with the backint specification, SAP invokes both traditional and snapshot backups through a single backint application. The backint executable file in this case calls IBM Tivoli Storage Manager for Enterprise Resource Planning or IBM Tivoli Storage Manager for Advanced Copy Services depending on the settings in the BR*Tools configuration file or the setting of the ′-t′ option in the original BR*Tools command entry. If Tivoli Storage Manager for Advanced Copy Services is installed, the options ′-t volume′ and ′t volume_online′ (recommended) are available.

The BR*Tools specification 7.10 allows all backint functions (backup, inquire, restore, delete) to be invoked with the option ″-t volume″. In this case it is expected that backint operates on snapshot backups instead of traditional Tivoli Storage Manager backups. For backups, there is an additional option for creating snapshot backups, which minimizes the time during which Oracle operates in degraded mode. When invoked with the option ″-t volume_online″, backint needs to inform BR*Tools, before and after backing up a set of files, through the same protocol that is already used for traditional backups that are invoked with option ″-t file_online″.

In order to enable database integrity checking, SAP also requires the ability to mount snapshots on a local or a remote system, or to be able to restore portions of the data to a temporary location. Among these options, Data Protection for Snapshot Devices currently supports only the ability to mount a snapshot on a remote system. In environments with a Tivoli Storage Manager server, the ability to mount a snapshot on a remote system can also be used to create a Tivoli Storage Manager backup from a snapshot. In this case the Tivoli Storage Manager backup is performed through backint. By using the same backup-id for both the snapshot and Tivoli Storage Manager backup, BR*Tools will enable access to either one.

The following new functions can be performed using the backint interface:
- Support of multiple snapshot backup generations
- Support for full and partial database snapshot backups. Snapshot backups of redo-logs (i.e. snapshot backups via BRARCHIVE) are not supported.
- Support of LVM mirrored environments

- Off-loaded tape backups can be invoked synchronously or scheduled independent of the production system.

IBM Tivoli Storage Manager for Advanced Copy Services requires three types of profiles:

- A **device-specific profile** that can be shared among various SAP systems. This file contains all sections that are required by the IBM Tivoli Storage Manager for Advanced Copy Services daemon and device agent, i.e. the GLOBAL, ACSD, and *device* sections.
- A **SAP backint profile** (.utl file). This file can be shared with a IBM Tivoli Storage Manager for Enterprise Resource Planning configuration and is normally the IBM Tivoli Storage Manager for Enterprise Resource Planning profile itself
- A **profile for offloaded Tivoli Storage Manager backups**, which is integrated with the device specific profile.

The device specific profile employs the SAP backint profile rather than the CLIENT section that is present for other database configurations of Data Protection for Snapshot Devices.

Version management:

Tivoli Storage Manager for Advanced Copy Services counts only full backups as valid versions. Partial backups are removed as soon as a subsequent full backup is deleted. Tivoli Storage Manager for ERP accepts versions created on either side during version counting.

Although Tivoli Storage Manager for Advanced Copy Services is used to create a FlashCopy of the database, the control file run is still made using Tivoli Storage Manager for ERP. For that reason it is important to retain control file backups at least as long as FlashCopy backups.

Snapshots of additional files:

The BR*Tools specification requires IBM Tivoli Storage Manager for Advanced Copy Services to fail immediately if non-application files reside on a volume that is to undergo a snapshot, unless such a file is explicitly permitted by entering it in the so-called *negative list*.

There is a new option ″–n <negative-list>″ via which this negative list of non-application files (which otherwise would not be permitted) can be included in the snapshot operation. The negative list can contain files or directories, in which case the entire directory as well as all subdirectories are considered to be included in the list. The user can specify files that are in the negative list in a new BR*Tools parameter, util_vol_nlist. See see “BR*Tools configuration profile (.sap)” on page 193 for more information.

Backint can also be invoked with the option ″-n no_check″, in which case backint continues even if non-database files are involved in the snapshot backup. If backint terminates with an error, because non-application files would otherwise participate in the snapshot operation, BR*Tools expects backint to report only the first 100 files non-database files that need to be added to the negative list.

Refer to the SAP documentation for more information.

Processing of additional files during snapshot restore:

The BR*Tools 7.10 specification supports snapshot restores from backups that were created with the options ″-t volume″ and ″-t volume_online″, in which case backint would be invoked with the options ″-f restore -t volume″. Similar to backups, additional care has to be taken in situations where additional files would be affected by the restore operation. Negative lists will be needed during restore.

For inquire or delete operations, SAP invokes inquire and delete with the option ″-t volume″ if a snapshot volume is involved.

Offloaded Tivoli Storage Manager backups:

The BR*Tools 7.10 specification recognizes the need to create a secondary (such as Tivoli Storage Manager) backup from a snapshot. Backups to Tivoli Storage Manager that were created from a backup server with Tivoli Storage Manager for ERP are recognized by SAP and get the same backup ID as the FlashCopy backup.

Offloaded Tivoli Storage Manager backups are performed by invoking the IBM Tivoli Storage Manager for Advanced Copy Services Offload Agent (tsm4acs), which is part of the IBM Tivoli Storage Manager for Advanced Copy Services package. This program will mount snapshots that have the TAPE_BACKUP_PENDING flag set in the IBM Tivoli Storage Manager for Advanced Copy Services repository and can invoke an application-specific backup method to perform the backup. Backint has been added as a new backup method to tsm4acs and extended to allow the backup ID of the Tivoli Storage Manager backup to be set during command invocation.

Mount and unmount:

In order to be able to perform database integrity checks, the BR*Tools 7.10 specification requires backint to be capable of mounting and unmounting snapshots on either the local or remote machine. For this purpose, SAP has introduced a new parameter ″util_vol_access″ in the BR*Tools configuration file, which can have the values

Table 18. util_vol_access Parameter

Value of util_vol_access	Meaning
′none′	It is not possible to access a snapshot backup on the current machine.
′copy′	It is possible to copy snapshot backups to a temporary location on the local machine.
′mount′	It is possible to mount snapshots in read-only mode on the local machine.
′both′	The options ″copy″ and ″mount″ are both valid.

If ″util_vol_access″ is set to ″none″ on the machine where the snapshot was created, the ability is provided to mount the snapshot on another host. As AIX does not allow mounting a snapshot image of a SAN volume on the local machine, IBM Tivoli Storage Manager for Advanced Copy Services requires the parameter ″util_vol_access=none″ on the local machine.

Data Protection for Snapshot Devices for *SAP® with Oracle* software environment

Data Protection for Snapshot Devices requires specific software when operating in an SAP® with Oracle environment.

Data Protection for Snapshot Devices for *SAP® with Oracle* operates in the following software environment:

- AIX
- Oracle 10, 11
- Tivoli Storage Manager server(optional)
- IBM Tivoli Storage Manager for Advanced Copy Services (Data Protection for Snapshot Devices)
- Common Information Model (CIM), for FlashCopy devices
- SAP
- SAP BR*Tools 7.10 or higher
- IBM Tivoli Storage Manager for Enterprise Resource Planning (Tivoli Storage Manager for ERP) (required for offloaded backup of snapshot to Tivoli Storage Manager)

IBM Subsystem Device Driver support

Data Protection for Snapshot Devices provides support for IBM Subsystem Device Driver (SDD).

SDD resides on the host servers (production system and backup system) with the native device driver for the storage system. SDD uses redundant connections between the host server and disk storage in a storage system to provide enhanced performance and data availability. Refer to your SDD documentation for further information. Note that SDD is required for SAN VC. Use SDD only if your configuration has two or more paths to the storage subsystem from each host. SDD does not support a single path to the storage subsystem.

Data consistency

Data Protection for Snapshot Devices backup processing can fail when file systems used during snapshot processing are inconsistent.

To guarantee the consistency of the data processed by Data Protection for Snapshot Devices, several techniques are utilized. JFS2 file systems offer the capability to stop all I/O operations on the file systems on request. This process is called *freeze* and is activated using the profile parameter LVM_FREEZE_THAW. For file systems that do not provide such capabilities, the volumes are imported on the backup server and the file systems are mounted to verify their consistency.

Data Protection for Snapshot Devices storage system overview

Data Protection for Snapshot Devices exploits the snapshot capabilities of several storage systems.

Data Protection for Snapshot Devices supports the following IBM storage systems:

- Disk Storage DS6000 series subsystem
- Disk Storage DS8000 series subsystem
- SAN Volume Controller

- System Storage N Series
- Enterprise Storage Server (ESS) Model 800
- IBM XIV® Storage System

Only one of these systems must be configured for Data Protection for Snapshot Devices, and the database must reside completely on this system. However, the use of SAN Volume Controller allows it to manage one or more ESS or DS systems (as well as non-IBM storage hardware) within the framework of the SAN Volume Controller configuration.

Considering the similarity of point-in-time copy functionality (FlashCopy or device-inherent snapshot) provided by these storage-system options, this publication provides common documentation for the individual software components provided for the specific database and storage system environments. The generic term *Data Protection for Snapshot Devices* is used to apply to any or all of these components.

Note: Any use of *FlashCopy* or *snapshot restore* in the sections of this publication applying to non-FlashCopy devices (such as N Series) should be interpreted as meaning the corresponding snapshot generation or restore function of these devices. Also, multiple target sets are also referred to as *frequent snapshots* in an N Series context.

Enterprise Storage Server

The IBM TotalStorage Enterprise Storage Server (ESS) architecture provides unmatchable functions for all the IBM family of e-business servers, and also for the non-IBM (that is, Intel®-based and UNIX-based) families of servers.

Across all of these environments, the ESS features unique capabilities that allow it to meet the most demanding requirements of performance, capacity, and data availability that the computing business may require. The move to on demand business presents companies with both extraordinary opportunities and significant challenges. Consequently, companies also face an increase in critical requirements for more information that is universally available online, around the clock, every day of the year. To meet the requirements of on demand business, where massive swings in the demands placed on your systems are common, and continuous operation is imperative, you need very high-performance and intelligent storage technologies and systems, which can support any server application in your business, today and into the future. The IBM TotalStorage Enterprise Storage Server has set new standards in function, performance, and scalability in these most challenging environments.

Disk Storage subsystem

The IBM TotalStorage Disk Storage (DS) family is a follow-on Enterprise Storage Server generation with a new architecture and enhanced performance and features.

The most recent members of the DS family, the DS6000 and DS8000, give customers the freedom to choose the right combination of solutions for their current needs and the flexibility to help their infrastructure evolve as their needs change. The TotalStorage DS family is designed to offer high availability, multiplatform support and simplified management tools, all to help the customers to cost effectively adjust to an on demand world.

The IBM TotalStorage DS Family, and the DS6000 and DS8000 series as members of this family, supports enterprise-class data backup and disaster recovery capabilities. As part of the IBM TotalStorage Resiliency Family of software, IBM TotalStorage FlashCopy point-in-time copy capabilities back up data in the background, while allowing users nearly instant access to information on both the source and target volumes.

Note: The DS4000® is *not* supported.

Note: FlashCopy backups taken from an ESS configuration cannot be restored directly to a DS environment. Restore from a Tivoli Storage Manager backup, or an intermediate migration from ESS to DS, is required.

DS6000

The DS6000 series offers a new era in price, performance and scalability. Now for the first time customers have the option for a midrange priced storage subsystem with all the features and functions of an enterprise storage subsystem. Some customers do not like to put large capacities of storage behind one storage controller. In particular, the controller part of a high end storage system makes it expensive. Now you have the option of choice, you can build very cost efficient storage systems by adding expansion enclosures to the DS6800 controller, but since the DS6800 controller is not really expensive, you can also grow horizontally by adding other DS6800 controllers. You have the option to easily grow into the DS8000 series by adding DS8000 systems to your environment or by replacing DS6000 systems.

DS8000

The IBM TotalStorage DS8000 is a high-performance, high-capacity series of disk storage systems. It offers balanced performance, which is up to 6 times higher than the ESS Model 800. The capacity scales linearly from 1.1 TB up to 192 TB. With the implementation of the POWER5™ Server Technology in the DS8000, it is possible to create storage system logical partitions (LPARs) that can be used for completely separate production, test, or other unique storage environments.

The DS8000 series is designed for 24x7 environments in terms of availability, and it still provides the industry leading advanced copy services to ensure business continuity.

SAN Volume Controller

The SAN Volume Controller is a virtualization layer that allows addressing a heterogeneous configuration of IBM and non-IBM open-system storage devices through one interface to an open-systems host.

In a conventional SAN, the logical unit numbers (LUNs) that are defined within the storage subsystem are directly presented to the host or hosts. Symmetrical virtualization, also known as block aggregation or in-band virtualization, essentially means having an appliance in the data path that can take physical storage from one or more storage subsystems and offer it to hosts in the form of a virtual disk. The SAN Volume Controller provides symmetric virtualization by creating a pool of managed disks from the attached storage subsystems, which are then mapped to a set of virtual disks for use by attached host computer systems.

System administrators can view and access a common pool of storage on the SAN, which enables them to use storage resources more efficiently and provides a common base for advanced functions.

With SAN Volume Controller support, IBM Tivoli Storage Manager for Advanced Copy ServicesS offers three major customer benefits:

- price/performance optimization of storage used for FlashCopy solutions
- removal of restrictions caused by database layout or subsystem capacity limitations
- accommodation of non-IBM storage subsystems into a homogeneous FlashCopy operation.

Limitations:

- Except for incremental FlashCopy, DP for Snapshot Devices supports multiple target sets on an SVC indirectly. The agent that monitors the background copy processes will withdraw the FlashCopy relationships when the processes complete.

Aside from these exceptions, the full FlashCopy functionality (FlashCopy backup and restore) provided for the ESS and DS subsystems is also available with an SAN Volume Controller configuration. With the SAN Volume Controller, a FlashCopy can be performed from one storage subsystem to another, and this therefore permits moving the production database from hardware provided by one vendor to hardware provided by another vendor. In addition, multiple target sets are also supported for an SAN Volume Controller configuration.

Back-end storage:

The SAN Volume Controller allows a great deal of flexibility in creating virtual disks and mapping these to the back end storage. It is important that sufficient back end storage be configured to support the anticipated load. The list of the SAN Volume Controller supported storage and associated firmware levels is very large and detailed.

Related reference

"IBM storage systems information sources" on page xvi

IBM System Storage N Series

The IBM System Storage N Series implements a Network Appliance, Inc. (frequently abbreviated as 'NetApp') storage system supported by Data Protection for Snapshot Devices.

Currently, the models N3700, N5000, and N7000 are available. For details, refer to *IBM System Storage N Series*.

A Network Appliance storage system, also called a *filer*, offers database administrators many advantages in terms of backup and recovery. NetApp snapshot technology, combined with the capabilities of IBM Tivoli Storage Manager for Advanced Copy Services for integration and management of point-in-time techniques, can dramatically optimize the application server backup/recovery activities. Handling multiple on-line NetApp snapshot images allows the system administrator to restore file systems without the necessity of restoring from tape in many circumstances. Backup and recovery performance is dramatically improved over that of conventional local disk, improving mean time to recovery (MTTR) intervals.

A NetApp snapshot is a ″frozen,″ read-only copy of a volume that provides easy access to old versions of files, directory hierarchies, and/or LUNs (logical unit numbers). A snapshot is retained locally. A volume represents an entire file system. The filer uses a copy-on-write technique to create snapshots very quickly without consuming any disk space. Only as blocks in the active file system are modified and written to new locations on disk does the snapshot begin to consume extra space.

N Series devices can be attached within a SAN environment or as *network attached storage* (NAS) and accessed using several different protocols. Data Protection for Snapshot Devices currently supports NFS as the protocol.

NAS attachment is required to use Linux on System x.

NetApp snapshot technology is a feature of the WAFL (Write Anywhere File Layout) storage virtualization technology that is part of Data ONTAP, the microkernel that is delivered with each NetApp storage system. A NetApp snapshot takes only a few seconds to create—typically less than one second, regardless of the size of the volume or the level of activity on the NetApp storage system. After a snapshot copy has been created, changes to data objects are reflected in updates to the current version of the objects, as if snapshot copies did not exist. Meanwhile, the snapshot version of the data remains completely stable. Since a NetApp snapshot incurs no performance overhead; users can comfortably store up to 255 snapshot copies per WAFL volume, all of which are accessible as read-only and online versions of the data.

Unlike FlashCopy devices, which require the target disks to be predefined, the N Series system creates the target disks for a copy operation on request. N Series volumes are conventionally referred to as *flexible volumes*, and the target volumes are clones of the source, or parent, volumes. A clone is a flexible volume that is a writable snapshot of another volume. Initially, the clone and its parent share the same storage. Only as one volume or the other changes is more storage space consumed. Only flexible volumes have the FlexClone feature used by IBM Tivoli Storage Manager for Advanced Copy Services. Therefore, for the mount function of TSM for ACS, which is based on clone volumes, flexible volumes are required.

By coupling Data Protection for Snapshot Devices and NetApp snapshot, the customer benefits by:

- the ability to create frequent snapshot backups of the volumes constituting the database (equivalent to the multiple target set functionality for FlashCopy devices)
- the ability to have as many snapshots as NetApp can support (up to 256 per NetApp volume)
- the ability to utilize the NetApp function of reverting to a particular snapshot.

IBM System Storage N Series restrictions

These general restrictions apply to the use of N Series devices in this release of Data Protection for Snapshot Devices.

Consider these requirements:

- The N Series hardware must either
  - reside in a SAN environment, in which the filer exports data as blocks (LUNs) via FCP or iSCSI (the LUNs can then be used by the AIX LVM), or
  - be configured as network-attached storage (NAS) and accessed via NFS
- LVM mirroring is not supported by Data Protection for Snapshot Devices on N Series hardware.
- The database must reside within one filer (single cluster).
- A SnapRestore license is required to perform a snapshot restore using Data Protection for Snapshot Devices.
- *NetApp allows storage overallocation, such that the creation of a snapshot can potentially disrupt production operations in case of out-of-space conditions.*
- When restoring a snapshot, all snapshots taken subsequent to the one that is restored are lost.
- The restore will fail if there is a clone associated with a newer snapshot that prevents this snapshot from being destroyed.
- Incremental backup is not supported.
- The JFS2 file system is required for SAN-attached N Series devices. Only this file system supports the use of the freeze and thaw functions required for the snapshot process.

IBM XIV® Storage System

The IBM XIV® Storage System is a SAN-attached system that includes a very fast and space efficient redirect-on-write snapshot mechanism which allows for thousands of snapshots of a volume or volume group to be created.

IBM Tivoli Storage Manager for Advanced Copy Services 6.1 support for IBM XIV® Storage System snapshot features uses the existing DB2, Oracle, and SAP® with Oracle interface to perform fast, zero-impact snapshot backups of production databases during standard production operations. The IBM XIV® Storage System provides an alternative to block-level continuous data protection (CDP). This is due to its high performance snapshot implementation and space efficiency attributes, which allow a backup strategy of frequent snapshots to be practical and realistic. The IBM XIV® Storage System consistency group support enables a snapshot of multiple volumes to be made together in a consistent fashion. Disaster recovery operations can also be implemented by using the IBM XIV® Storage System to restore the production database from an existing snapshot backup.

These IBM XIV® Storage System functions are provided:

- Ability to retain and catalog snapshot copies and allow restore from local snapshot images:
  - Back up to local snapshot.
  - Restore from local snapshot.
  - Query available backup versions.
  - Configure connection information.
- Support integrated backup to Tivoli Storage Manager (if available):
  - Back up to Tivoli Storage Manager from snapshot image.

- Offload backup processing to Tivoli Storage Manager to a secondary host.
- Reconcile snapshot version on Tivoli Storage Manager server with versions on Filer (Local Snapshot Manager).
- Restore from Tivoli Storage Manager or local snapshot.

There is no special support needed for incremental or space-efficient snapshots as these features are provided in the IBM XIV® Storage System architecture. Also, a reconciliation algorithm synchronizes the backup catalog with the snapshot copies that are available on the IBM XIV® Storage System. This synchronization is needed as the IBM XIV® Storage System snapshot technique is designed so that the oldest snapshot copies are automatically replaced by newly created ones when the snapshot reserve space is full.

CIM Agents used by Data Protection for Snapshot Devices

Separate CIM Agents are employed by Data Protection for Snapshot Devices.

These CIM Agents are employed by Data Protection for Snapshot Devices: one for ESS and DS configurations and one for the SAN Volume Controller. While these versions implement Copy Services in an SMI-S compliant manner, they are different in the following areas:

- parameters and specification modes in certain software components
- properties for monitoring background copy processes
- procedures for querying information from the storage system
- approaches to the point-in-time copy process

CIM Agent for DS Open API

The ESS 800, DS6000, and DS8000 are supported by a CIM Agent that implements the DS Open API.

The DS Open API is an industry standard API that is SMI-S- and CIM-compliant. The ESS Network Interface (NI) Client (to support Copy Services) and the LIC (microcode with FlashCopy feature) for the ESS or DS are required. The CIM Agent product includes the CIMOM, device provider, SLP, and ESS NI client. The ESS NI server is preinstalled with the Storage Hardware Management Console (HMC) shipped with the DS8000 and the Storage Management Console (SMC) of the DS6000. The interface to the ESS 800 is provided by the ESS Copy Services Command Line Interface (CLI), which resides on the machine hosting the CIM Agent for DS Open API.

Note: With an ESS Model 800 configuration only, the ESS CLI must be installed prior to the CIM Agent for DS Open API.

For more information on this agent (including installation and configuration), see *IBM TotalStorage DS Open Application Programming Interface Reference*, GC35-0493 .

CIM Agent for SAN Volume Controller

The CIM Agent for a SAN Volume Controller is provided as part of the software shipped with the SAN Volume Controller Master Console.

For more information see *IBM TotalStorage SAN Volume Controller CIM Agent Developer's Reference*, SC26-7545, and *IBM TotalStorage SAN Volume Controller Configuration Guide*, SC26-7543.

Note: The CIM Agent provided with SVC 4.2.1 complies with the SMI-S specification V1.2.

Chapter 2. Planning for Snapshot Devices

Review this information when planning for backup and restore operations on Snapshot Devices.

Data Protection for Snapshot Devices backup methods

Data Protection for Snapshot Devices provides two basic backups methods.

Backup methods overview

Data Protection for Snapshot Devices allows full database backups only.

Large database files can be distributed over many physical volumes in a variety of ways. Considering these distribution challenges in the context of using Logical Volume Managers, online and offline backup and restore or recovery procedures can become complicated when using disk-based backup techniques. In order to provide a simple strategy for image disk backups, Data Protection for Snapshot Devices allows full database backups only and supports two basic types of backups:

- snapshot backups from disk
- tape backups to a Tivoli Storage Manager server

The image disk backups are the result of the FlashCopy function of Copy Services or the corresponding snapshot functionality of other devices such as N Series. It is also possible to back up tablespaces or offline log files without involving image disk backup techniques.

(DB2) As of DB2 version 9.5, the DB2 Data Partitioning Feature (DPF) has a single system view (SSV) mode to back up a multi-partition database with a single command entry.

Related concepts

"Subdividing the disk environment for DB2" on page 68
Instructions for setting up the disk environment for DB2.

"Subdividing the disk environment for Oracle" on page 70
Instructions for setting up the disk environment for Oracle.

"Snapshot backup overview" on page 34
General snapshot backup information.

"Tivoli Storage Manager overview" on page 10
Tivoli Storage Manager is a client and server program that provides storage management services in a multivendor, multiplatform computer environment.

"Backups without snapshot backup disks" on page 120
Partial backups of a database (such as tablespace backups) can be performed on the production system.

"Restore methods overview" on page 43
Data Protection for Snapshot Devices allows a database to be restored from one of two locations.

Snapshot backup overview

Data Protection for Snapshot Devices supports full database disk backups through the snapshot function of the storage system.

It is required to have all disks on which the database files reside set up in such a way that the following conditions are met for all source volumes and target volumes:

- FlashCopy devices:
  - A source volume and its equivalent target volume are on the same storage system.
  - A source volume and its equivalent target volume are the same size.
- Source volumes contain only files that are part of the Tivoli Storage Manager backup that follows the snapshot backup operation (if requested).

When Data Protection for Snapshot Devices is installed, a tape backup can be requested simultaneously with the request for the snapshot backup. This is occasionally referred to as an *integrated tape backup*. See the applicable database-specific section for more information. (DB2) Snapshot backup is described in more detail in the DB2 High Availability Feature documentation. The ’db2 backup database’ command with the ’use snapshot’ option is described in the DB2 *Command Reference*.

Target set states:

Target sets can be available in only one of two states.

A target set can have one of the following states:

AVAILABLE
The initial state of the target set after you have set up the target set in the storage system and the target volumes file (.fct). A target set will also be assigned this state when it has been freed by a withdraw operation.

IN_USE
The state once Data Protection for Snapshot Devices has used it within a snapshot backup and it has not been freed as noted above.

Monitoring states:

The state of a snapshot backup is monitored to document its progress.

The following states are maintained to document the progress of a snapshot backup:

Table 19. Snapshot Backup Progress States

State	Meaning
IN_PROGRESS	Background copy or tape backup pending or in progress
SUCCESSFUL	Background copy completed, or not required.
FAILED	Error encountered during copy.

These states are reported by different commands depending on the database configuration:

Table 20. Commands Reporting Backup Progress States

Component	Command
DB2	db2acsutil (part of DB2 Advanced Copy Services)
Oracle	acsutil
SAP with Oracle	acsutil, and backint -f inquire_detail

Related reference

"Snapshot Object Manager for Oracle (acsutil)" on page 149
The Snapshot Object Manager for Oracle (acsutil) provides a snapshot backup query and restore interface for native Oracle environments..

"Data Protection for Snapshot Devices Offload Agent (tsm4acs)" on page 154
The Offload Agent provides a single user interface for all functionality associated with the IBM Tivoli Storage Manager for Advanced Copy Services package.

Usability states:

The usability state of a snapshot backup is observed to determine how it can be used by other functions.

A target set can have one or more of the following states to indicate how the set can or must be used by other Data Protection for Snapshot Devices functions. These states can also be used as filter values (option ′-a′) when invoking the device agent.

Table 21. Backup Usability States and Command Line Filter Options

Usability state	CLI ′-a′ option value	Meaning
LOCALLY_MOUNTABLE		Backup data can be mounted from the local machine.
REMOTELY_MOUNTABLE		Backup data can be mounted from a remote machine.
REPETITIVELY_RESTORABLE		Backup data can be restored (the image can be used multiple times)
DESTRUCTIVELY_RESTORABLE		Data can be restored (upon restore, other backups are potentially destroyed)
SWAP_RESTORABLE		Restore is possible by using the backup volumes directly rather than copying the data back to the source volumes. For storage systems like ESS, DS or SVC this means that, in the restore case, the target volumes can be assigned to the system on which the restore should be performed. This will thus avoid the background copy process in the storage volume.
PHYSICAL_PROTECTION		The snapshot guarantees protection from physical failures on the source volumes, i.e., there is no longer a dependency on the source volumes. This does not necessarily mean that a FULL_COPY has to be created with each snapshot. For example, block-level continuous data protection (CDP) mechanisms typically replicate the data once and then record only changes.
FULL_COPY		A full copy of the data has been generated.

Table 21. Backup Usability States and Command Line Filter Options (continued)

Usability state	**CLI '-a' option value**	**Meaning**
INCOMPLETE		A portion of the data that has been backed up has been deleted and can no longer be restored. This can happen, for example, after a partial restore of an old backup that is only DESTRUCTIVELY_RESTORABLE.
FORCED_MOUNT	4096	Since the freeze/thaw mechanism does not exist for AIX JFS filesystems, the file system consistency of a database residing on JFS filesystems must be checked on a backup system after the snapshot backup has been performed. This state indicates a snapshot backup that must be checked. When this consistency check on the backup system has been performed (and the file systems can be mounted without error), the snapshot backup state will be changed to PHYSICAL_PROTECTION. Likewise, the consistency of LVM mirrors must be verified by such a mounting process.
MOUNTING		Mount has been requested on the backup server.
MOUNTED		Mounting is complete.
DELETING		Indicates that a backup is marked for deletion (i.e., deletion was requested).
DELETED	1	Indicates that the backup has been deleted. For N Series, this is a physical deletion.
BACKGROUND_MONITOR _PENDING	8	Indicates that a required background copy process is not yet active or not yet finished. The device agent will check for backups with this state and monitor the associated volumes until the background copy is finished. This state will then be replaced by FULL_COPY.
TAPE_BACKUP_PENDING	2	Indicates that a requested tape backup has not yet started or is not yet finished. The Offload Agent will check for backups with this state and perform the requested tape backup. After the tape backup has finished successfully, this state will be reset. If the tape backup terminates with an error, the TAPE_BACKUP_PENDING state will remain set, TAPE_BACKUP_IN_PROGRESS will be reset, and the retry counter will be incremented.
TAPE_BACKUP_IN_PROGRESS		Indicates that the DP for Snapshot Devices Offload Agent has started the requested tape backup. If the backup fails, only this state is reset.

The following table shows the relationships of the backup usability and progress states for the various types of snapshot backup:

Table 22. Usability States Resulting from Snapshot Operations

Snapshot Technology	**Background Monitoring Needed**	**Progress State**	**Usability States**
N Series NAS	No	SUCCESSFUL	REPETITIVELY_RESTORABLE, DESTRUCTIVELY_RESTORABLE, REMOTELY_MOUNTABLE
N Series SAN	No	SUCCESSFUL	REPETITIVELY_RESTORABLE, DESTRUCTIVELY_RESTORABLE, REMOTELY_MOUNTABLE

Table 22. Usability States Resulting from Snapshot Operations (continued)

Snapshot Technology	Background Monitoring Needed	Progress State	Usability States
NOCOPY FlashCopy	No	SUCCESSFUL	REMOTELY_MOUNTABLE, SWAP_RESTORABLE
COPY, INCR FlashCopy	Yes	IN_PROGRESS	REMOTELY_MOUNTABLE, SWAP_RESTORABLE
		SUCCESSFUL	REMOTELY_MOUNTABLE; REPETITIVELY_RESTORABLE, PHYSICAL_PROTECTION, FULL_COPY, SWAP_RESTORABLE

Overview of multiple backup generations (target sets) on disk

Support for multiple backup generations is inherent on N Series devices and is frequently referred to as frequent snapshots.

For SAN Volume Controller, see the README information for the current status of support for multiple FlashCopy backups on multiple target sets in an SAN Volume Controller environment.

(DB2) DB2 Advanced Copy Services limits the number of target sets to two. Data Protection for Snapshot Devices does not limits the number of target sets.

To minimize the database restore processing window, the time between backups can be decreased by having fewer log files to apply. This will reduce the time needed for forward recovery processing. Multiple backup generations must be kept on disk in order to support snapshot restore. Data Protection for Snapshot Devices supports this by managing multiple target sets. More than one set of target volumes can become the target set (or data container) for one snapshot backup of the source volumes with Data Protection for Snapshot Devices.

Configuring multiple target sets as backup generations on disk increases the availability of a well-oredered backup on disk for snapshot restore. For example, consider the following backup schedule:

Daily Backup Number	Time	Target Set	FlashCopy Type	Backup Type
1	12:00 a.m.	1	INCR	Disk-only
2	4:00 a.m.	2	COPY	Disk and tape (TSM)
3	8:00 a.m.	1	INCR	Disk-only
4	12:00 p.m.	1	INCR	Disk-only
5	4:00 p.m.	2	COPY	Disk-only
6	8:00 p.m.	1	INCR	Disk-only

Maintaining multiple backup generations provides these benefits:

- Increases the probability that the database administrator has a snapshot backup available for a snapshot restore.
- Provides the database administrator with the option of running the fast snapshot restore from older snapshot backups. This might be necessary when the latest

disk backup cannot be used. Earlier releases of Data Protection for Snapshot Devices provided only one latest available backup.
- Improves the recovery time because now the database administrator can perform incremental backups more frequently, regardless of high database activity. When low database activity occurs, a full disk copy backup to a target set other than the target set used during high database activity can be performed.

When using an AIX LVM mirrored setup, multiple disk backups can be retained on the hardware unit and two multiple disk backups can be created by using the FlashCopy incremental-backup versions retained on the storage system. This provides the ability to perform fast FlashCopy backups alternately to two disk copies, thus reducing the downtime when a restore or recovery is required.

The maximum number of target sets allocated for the database depends on the following conditions:
- The size of the database that resides on the source volumes and logically represents a source data container.
- The number of target sets that can be allocated in the hardware unit.
- The maximum number of target sets supported by the hardware supports. Refer to your hardware marketing representative for correct information regarding of target sets.
- In a DB2 environment, whether Data Protection for Snapshot Devices is installed as DB2 Advanced Copy Services limits the number of target sets to two.

Related concepts

"Overview of Data Protection for Snapshot Devices support for AIX Logical Volume Manager mirrored environments" on page 48

Selection algorithm

Algorithms are used to help select target sets.

When more than one target set is implemented in a backup and restore strategy, deciding which target set is to be used with the various FlashCopy backup types can difficult. Data Protection for Snapshot Devices provides an algorithm for automated target set selection, where the database administrator allows Data Protection for Snapshot Devices to determine which of several target sets are to be used. This depends on the value of the FLASHCOPY_TYPE parameter. Target set selection is performed only if the backup system is in a state that allows a new backup to be started. This requires that the target set not be mounted on the backup system or that the snapshot backup has been deleted (with or without the DELETE_FORCE option). The Data Protection for Snapshot Devices 'unmount' function must be used to perform the unmount operation.

Setting up multiple target sets in the Target Volumes file

The target volumes file (.fct) contains information that determines which target sets can be used.

The file is composed of multiple volumes_set_x topics. Each topic comprises all the target volumes that will be used within one FlashCopy backup, and these volumes are considered one target set. Each topic (and thus each target set) is identified by a topic name comprised of a prefix (volumes_set_) and a user-defined target set ID. In Data Protection for Snapshot Devices messages, the target set ID is also referred to as a data container ID.

After Data Protection for Snapshot Devices is installed, the database administrator must set up the target volumes file (.fct) with at least one target set. As a result, the file contains at least one target set topic (for example, 'volumes_set_1'). In case the initial environment is extended by one or more additional target sets, target set topics need to be added to the FlashCopy target volumes file (.fct). In the event a target set is to be changed or removed from the FlashCopy backup process, you must first issue a `tsm4acs -f unmount` and/or `db2acsutil delete` (with the DELETE_FORCE vendor option), `acsutil delete`, or `backint -f delete` to ensure that, based on the usage of this target set:

- any existing source/target relationships (such as INCR or NOCOPY) are withdrawn and no potential problems remain for succeeding snapshot restores and FlashCopy backups.
- any mounted file systems on the backup system will be released (unmount fs, ..., exportvg)

Related tasks

"Data Protection for Snapshot Devices Target Volumes File (.fct)" on page 189
Detailed description of how to set up the target volumes file.

Related reference

"Example Target Volumes file in a mirrored environment" on page 57
The HARDWARE_ID_LVM_MIRROR parameter must be specified in the target volumes file when operating in a mirrored environment.

Target set states:

Target sets defined in the target volumes file are available in only one of two states.

Each target set defined in the target volumes file (.fct) can have one of the following two states:

AVAILABLE
This is the initial state of the target set after you have set up the target sets in the hardware unit(s) and the target volumes file (.fct). A target set will also be set to this state once you release a target set with state IN_USE by issuing `'db2acsutil delete'` (with the DELETE_FORCE vendor option), `acsutil delete`, or `backint -f delete`.

IN_USE
This is the target set state after Data Protection for Snapshot Devices within a FlashCopy backup has determined one of the following:

- Select a target set which has the state AVAILABLE and add it to a logical FlashCopy group (INCR, COPY or NOCOPY) that matches the intended FLASHCOPY_TYPE.
- Reuse a target set with the state IN_USE in an existing logical FlashCopy group.

A target set with the state IN_USE is always associated with a FlashCopy type (INCR, COPY or NOCOPY) used for a previous FlashCopy backup. Such a target set cannot be reused if the FLASHCOPY_TYPE value of a new FlashCopy backup does not match the FLASHCOPY_TYPE value associated with the selected target set using the specific target set algorithm.

Logical FlashCopy group descriptions:

A logical FlashCopy group consists of one or more target sets associated with the same FLASHCOPY_TYPE value.

A target set with state AVAILABLE, when selected in a FlashCopy backup, is added to a logical FlashCopy group associated with a certain FLASHCOPY_TYPE value when the following two conditions are met:

- The FLASHCOPY_TYPE value matches the FLASHCOPY_TYPE value of the current FlashCopy backup.
- The maximum number of target sets of the selected logical FlashCopy has not been reached.

The number of target sets used in the various logical FlashCopy groups depends mainly on the FLASHCOPY_TYPE value associated with the group:

- A COPY group can have more than one target set.
- An INCR group can have only one target set.

  When using the Data Protection for Snapshot Devices functionality for AIX mirrored environments, two INCR target sets can be used because the set of AIX mirrored source volumes can be divided into two source copy sets, with each one set up in a separate hardware unit. Only one source copy set will be involved within a FlashCopy backup and only one target set in the same hardware unit as the source copy set can be used for INCR FlashCopy backup.
- A NOCOPY group can have more than one target set if a used target set is unmounted prior to the next FlashCopy backup and other target sets would be used for a FlashCopy backup. However, use the `'db2acsutil delete'` function (with the DELETE_FORCE vendor option), `acsutil delete`, or `backint -f delete` if the FlashCopy backup runs with FLASHCOPY_TYPE NOCOPY. This will release the source volumes and target volume relationships. In this way, after a FlashCopy backup, the temporarily used target set again receives the status AVAILABLE. Another reason not to have target sets left IN_USE with FLASHCOPY_TYPE NOCOPY is the potential for conflicts when performing a snapshot restore.

The upper limit for a logical FlashCopy group is the limit which is given by the capacity of the hardware unit(s) (or SAN Volume Controller cluster) and the number of source volume and target volume relationships for one source volume imposed by the storage system. This number needs to be adjusted to the number already planned or used in the other logical FlashCopy groups.

Related concepts

“Overview of Data Protection for Snapshot Devices support for AIX Logical Volume Manager mirrored environments” on page 48

“Multiple target sets and snapshot restore implications” on page 41
Consider these implications when using multiple target sets with a snapshot restore.

Preventing simultaneous snapshot backups:

The target set involved with the copy cannot be used for a snapshot restore as long as the background copy initiated by a FlashCopy backup is active.

This requires that Data Protection for Snapshot Devices prevent the database administrator from accidentally running too many backups simultaneously, with the risk that there are no disk backups available if a snapshot restore is needed.

In order to control snapshot backups, when a new snapshot backup is requested, DB2 Advanced Copy Services checks for any background copies still running on behalf of a previous backup request. DB2 Advanced Copy Services prevents a new FlashCopy from an existing logical FlashCopy group (INCR or COPY[1]) from being started if a background copy is still running for the same logical FlashCopy group. However, any target set (state AVAILABLE) which does not yet belong to a logical FlashCopy group could be selected if this is not in a conflict with the algorithm for the FlashCopy type.

Multiple target sets and snapshot restore implications

Consider these implications when using multiple target sets with a snapshot restore.

Required checks prior to snapshot restore

When several target sets are eligible for a snapshot restore, the snapshot restore steps are the same as when a setup consists of one target set only. First, check whether a background copy is still running for the backup to be used for a snapshot restore. The background copy must complete before proceeding. Otherwise, the process can be terminated by issuing `'db2acsutil delete'` (with the DELETE_FORCE vendor option), `acsutil delete`, or `backint -f delete`.

However, a basic FlashCopy requirement when using several target sets for one source set is that a target volume cannot have multiple source volume and target volume relationships. As a result, a FlashCopy backup cannot be performed to the original source volume (which is now the target volume) as long as a source volume and target volume relationship exists for the original source. This restriction requires that prior to a Data Protection for Snapshot Devices snapshot restore, the database administrator needs to check for any relationships the original source volumes have. Issuing the `'db2acsutil query'` command provides this information.

Such source volume and target volume relationships are created when FLASHCOPY_TYPE INCR or NOCOPY is used in the backup and a background copy is running. For each backup with FLASHCOPY_TYPE COPY, there is a temporary source volume and target volume relationship. As soon as the background copy completes, this relationship is withdrawn.

The conditions and consequences for breaking (or not breaking) the source volume and target volume relationships are as follows:

---

[1] Since NOCOPY never generates a FlashCopy backup whose target set can be used for a snapshot restore, the use of multiple target sets is a hypothetical case, although this is technically possible. For this reason, such a procedure will not be discussed further.

1. If the backup or background copy of a backup you want to restore is still running, you must wait until both have completed. In the meantime, however, you can check whether other existing source volume and target volume relationships must be withdrawn.
2. If a NOCOPY source volume and target volume relationship exists for the original source, its target set cannot be used in a snapshot restore anyway. The required action in any case is: to withdraw the NOCOPY relationship using `'db2acsutil delete'` (with the DELETE_FORCE vendor option), `acsutil delete`, or `backint -f delete`.
3. If the backup or the background copy is still running and this is not the backup you want to use for a snapshot restore, the required action on the backup system is to terminate (kill) the backup or terminate the source volume and target volume relationship by running `'db2acsutil delete'` (with the DELETE_FORCE vendor option), `acsutil delete`, or `backint -f delete`.
4. If an INCR source volume and target volume relationship exists for the original source, and the backup level on this target set is the one you want to select for a snapshot restore, then no action is required. This assumes that you have resolved either of the first two conditions if they are applicable.
5. If an INCR source volume and target volume relationship exists for the original source and the backup level on this target set is not the one you want, then only other target sets created with FLASHCOPY_TYPE COPY and in the state IN_USE can be used for a snapshot restore. However, in this case, the required action to break the source volume and target volume relationship is `'db2acsutil delete'` (with the DELETE_FORCE vendor option).
6. If a source volume and target volume relationship exists for the original source because a background copy is still running as a result of a FlashCopy backup using FLASHCOPY_TYPE COPY, you cannot run a snapshot restore to this source. In this case, you either wait for completion or run `'db2acsutil delete'` (with the DELETE_FORCE vendor option), `acsutil delete`, or `backint -f delete`.

In case an AIX-mirrored database is the subject of a snapshot restore, the storage system restriction on multiple source volume and target volume relationships to an original source volume must be followed for the source copy set that will be involved in the snapshot restore. The FlashCopy backups of the other (source) copy set and its target sets do not need any check for multiple source volume and target volume relationships as long they will not be chosen for a snapshot restore.

Running the snapshot restore

As soon as the database administrator has checked and resolved any conflicting source volume and target volume relationships, the Data Protection for Snapshot Devices snapshot restore function is used to initiate a restore. For the restore itself, there is no difference between a setup with one target set and one with multiple target sets.

Performing a snapshot restore rerun with a different target set

Depending on the existing backups on the various target sets in a multiple target set setup, the database administrator could run a restore from a target set different from the one used in the initial restore. This also requires checking for existing source volume and target volume relationships. In case your environment on the production system does not have database file systems mounted and the database logical volumes do not exist, you cannot rerun a restore with a backup for which you do not have a valid disk-copy backup on a target set (for example, if there is only a Tivoli Storage Manager backup available on the Tivoli Storage Manager server).

Related concepts

"Overview of Data Protection for Snapshot Devices support for AIX Logical Volume Manager mirrored environments" on page 48

Data Protection for Snapshot Devices restore methods

Data Protection for Snapshot Devices provides two basic restore methods.

Restore methods overview

Data Protection for Snapshot Devices allows a database to be restored from one of two locations.

Data Protection for Snapshot Devices provides these methods to restore a database:

- Restore using the snapshot features of the storage system.
- Restore from Tivoli Storage Manager.

Make sure to try the restore and recovery on a test system similar to the production system. Repeat this test regularly, especially after you have modified your system or the restore and recovery strategy.

Related concepts

"Tivoli Storage Manager overview" on page 10
Tivoli Storage Manager is a client and server program that provides storage management services in a multivendor, multiplatform computer environment.

What is snapshot restore?

A snapshot restore provides unique features.

A snapshot restore uses the snapshot feature provided on these storage systems:

- FlashCopy for ESS, DS, and SAN Volume Controller devices
- SnapRestore for N Series devices[2]
- IBM XIV® Storage System

A snapshot restore will restore a database *directly* from the volumes of a corresponding snapshot backup (target volumes) on the storage system to the original source volumes on the production system. The volumes then undergo a DB2 rollforward recovery to recover the database state to a particular point in time.

Why use snapshot restore?

A snapshot restore provides several advantages.

Snapshot restore provides these features:

- A quick restore of the production database in the event of a major failure.
- A restore of a database along with the storage structures of the operating system that may have been lost after the original backup, such as the table spaces, file systems, and volume groups.
- With the capability to perform snapshot backup to multiple target sets, several disk backup levels can be created.

---

[2] SnapRestore is a licensed feature.

- When using an AIX LVM mirrored setup, (for this special environment) it is possible to run a snapshot restore from one target set back to the one (source) copy set from which it was created. Thus, at least two target sets, one for each copy set, can be selected for a snapshot restore. Data Protection for Snapshot Devices allows more than one target set for one (source) copy set in the various snapshot backups. The database administrator has the option of selecting one of several target sets for a snapshot restore to a copy set.

Related concepts

"Overview of multiple backup generations (target sets) on disk" on page 37
Support for multiple backup generations is inherent on N Series devices and is frequently referred to as frequent snapshots.

"Overview of Data Protection for Snapshot Devices support for AIX Logical Volume Manager mirrored environments" on page 48

When not to use snapshot restore

A snapshot restore is not always the best restore to be used when certain conditions exist.

Snapshot restore must not be used in the following situations:

- If the source volumes on the production system specified by the TARGET_VOLUME parameter in the target volumes file (.fct) used for the snapshot restore differ from the source volumes that were specified by the TARGET_VOLUME parameter in the target volumes file and used for the original backup, and not all are still available. Snapshot restore to a new location is not supported.
- If you are unsure of what backup images are on the target volumes that you plan to restore using snapshot restore.
- If the source volume configuration on the production system to be used in the snapshot restore differs from the source volume configuration that existed during the original backup, and you want to preserve the current source volume configuration. Some original source volumes may have been given to another application. In such a case you might only be able to use a Tivoli Storage Manager backup for a restore, if all necessary tablespace containers are available for restore and recovery.
- If the last backup of the database was performed using the FLASHCOPY_TYPE parameter value NOCOPY.
- If the background copy process initiated by the Data Protection for Snapshot Devices has not yet physically completed and the process is therefore not yet ready for a snapshot restore.
- If, after a snapshot backup was performed, a double volume assignment condition has been created due to environment changes and, at the time of the snapshot restore, the following situation exists for a physical disk (volume) that was part of the database snapshot backup:
  - The disk has been removed on the production system from a database volume group; and
  - its AIX device and vpath has not been removed; and
  - it is still assigned to the production system; and
  - it has been assigned to another system.

  Data Protection for Snapshot Devices cannot detect such an improperly managed environment change.

What is a snapshot restore rerun?

A snapshot restore rerun provides unique features.

Under certain conditions, Data Protection for Snapshot Devices allows a snapshot restore rerun even if the FlashCopy process running in the background has not yet finished for the latest snapshot restore. Data Protection for Snapshot Devices will first check whether a snapshot restore was previously requested and allow the database administrator to restart this snapshot restore with profile parameter RESTORE_FORCE set to YES. The reason for such a rerun can be that the forward recovery of the previous restore or recovery proceeded too far and there is a need for another point-in-time forward recovery, or that the FlashCopy failed.

Related concepts

"Multiple target sets and snapshot restore implications" on page 41
Information on rerunning a snapshot restore from a target set other than the one used in the initial restore is provided.

Conditions for a snapshot restore rerun

A snapshot restore rerun is available when certain conditions exist.

Data Protection for Snapshot Devices allows a snapshot restore to be restarted as long as the same Backup ID that was used for the preceding snapshot restore is used. Rerunning such a snapshot restore is the only case in which Data Protection for Snapshot Devices automatically runs a withdraw of all background copy processes started by the last snapshot restore, should this still be required. In general, only one Backup ID is available for snapshot restore. When running in AIX LVM mirrored environments or when multiple target sets are configured, one of a number of target sets can be selected for a snapshot restore.

Related concepts

"Multiple target sets and snapshot restore implications" on page 41
Consider these implications when using multiple target sets with a snapshot restore.

Related tasks

"AIX Logical Volume Manager mirrored environments" on page 48
Data Protection for Snapshot Devices currently supports AIX LVM mirroring only for FlashCopy devices.

Reasons for a snapshot restore rerun

A snapshot restore rerun is best used when certain conditions exist.

The following situations might be a reason a snapshot restore rerun:

- The snapshot restore runs successfully, but after restarting the database application (such as SAP®), it is determined that the database was rolled forward too far. This case can now be resolved quickly by restarting the snapshot restore with the same Backup ID and performing a rollforward to the correct point in time.
- There was a hardware problem after the snapshot restore was initiated. For example, the snapshot restore fails after unmounting all file systems, exporting all volume groups, and while starting the FlashCopy process for all source volume and target volume pairs. If the volume groups consist of 10 source volume and target volume pairs, one reason could be that, after establishing the FlashCopy for the first 6 pairs, the Copy Services server returns an error when attempting to establish the FlashCopy relation for volume pair 7. Once the reason for the storage system failure is resolved, the snapshot restore can be restarted using the same Backup ID.

Snapshot restore considerations for N Series devices

A snapshot restore for N Series devices requires that certain conditions exist.

What is snapshot restore for native Oracle?

A snapshot restore for native Oracle provides unique features.

Data Protection for Snapshot Devices uses the IBM FlashCopy feature to back up an Oracle database from the production system to Tivoli Storage Manager server storage. snapshot restore uses the FlashCopy feature to restore your Oracle database *directly* from the backed up volumes on the snapshot devices (instead of from the Tivoli Storage Manager server) to the original source volumes on the production system.

Why use snapshot restore for native Oracle?

A snapshot restore for native Oracle provides several advantages.

The snapshot restore function provides the following benefits:

- A quick recovery of the production database in the event of a major failure.
- A restore of the Oracle database along with the storage structures of the operating system that may have been lost after the original backup, such as the table space containers or file systems.
- The ability to not have to back up to Tivoli Storage Manager server storage every time. As an alternative, a back up to Tivoli Storage Manager server storage can be performed once for every specified number of backups to the snapshot devices.

When not to use snapshot restore for native Oracle?

A snapshot restore for native Oracle is not always the best restore to be used when certain conditions exist.

The snapshot restore function cannot be used in the following situations:

- If the source volumes specified by the TARGET_VOLUME parameter in the profile used for the snapshot restore *differ* from the source volumes specified by the TARGET_VOLUME parameter in the profile used for the original backup. snapshot restore to a new location is not supported.
- If you are unsure of what backup images you have on the target volumes that you plan to restore using snapshot restore.
- If the source volumes configuration on the production system to be used in the snapshot restore *differs* from the source volumes configuration that existed during the original backup *and* you want to preserve the current source volumes configuration.
- If the last backup of the database was performed using Data Protection for Snapshot Devices with the FLASHCOPY_TYPE parameter specified as *nocopy*.
- If the databases (to be restored) were backed up with Data Protection for Enterprise Storage Server for Oracle Version 5.2.2 (or earlier).

Related concepts

"Data Protection for Snapshot Devices for Oracle migration considerations" on page 15
Provides suggested restore methods for databases backed up with Data Protection for Enterprise Storage Server for Oracle.

Snapshot restore limitations for native Oracle databases

Consider these limitations before performing a snapshot restore for native Oracle.

Be aware of the following limitations before performing a snapshot restore:

- Any time you make configuration changes to the database (for example, adding new physical disks, new file systems or new table space containers), you must perform a FlashCopy backup of the database to the FlashCopy storage device before continuing to use the database. If you made configuration additions and failed to perform a Data Protection for Snapshot Devices backup, Data Protection for Snapshot Devices detects these additions during snapshot restore processing and prompts you to ask if you want to continue with the restore. It is recommended that you specify NO at this point to stop restore processing. Then, back up the file system and try snapshot restore again. This time, specify yes when prompted. Data Protection for Snapshot Devices will remove the newly added file system during snapshot restore processing. After the restore is complete, you will have to create the new file system again, restore its data, and then perform rollforward recovery to bring the database to its current state. Failing to perform a FlashCopy backup to the FlashCopy storage device after making such configuration changes prevents the ability to use snapshot restore to recover the database.
- Snapshot restore processing overwrites Oracle redo log files. As a result, it is recommended that you create Oracle control files and redo log files in dedicated volume groups separate from Oracle datafiles. If your Oracle control files are in the same volume group as your Oracle datafiles, specify DATABASE_CONTROL_FILE_RESTORE:*yes* in your profile. This allows the overwritten Oracle control files to be replaced by the control files residing in Tivoli Storage Manager server storage.
- Snapshot restore only restores a database that was backed up with the FLASHCOPY_TYPE parameter set to *copy* or *incr*.
- Snapshot restore cannot restore a database that was backed up with an earlier version of Data Protection for Snapshot Devices. Such a database can only be restored from the Tivoli Storage Manager server using RMAN as described in the “Restoring a native Oracle database from Tivoli Storage Manager” on page 130 section.
- The database to be restored must not be brought online on the backup system after it has been backed up by Data Protection for Snapshot Devices. This ensures the database state remains at the latest backup image and is available for a snapshot restore. As a result, you must determine how you will maintain the database copy on the target volumes.
- The database administrator must maintain the integrity of the target volumes used in the backup during FlashCopy processing. Data Protection for Snapshot Devices does not maintain the integrity of the volumes (used during FlashCopy processing) that reside on the FlashCopy storage device subsystem. Once a set of FlashCopy storage device target volumes are made available for a Data Protection for Snapshot Devices backup, you must only use Data Protection for Snapshot Devices commands to handle these target volumes and their associated source volumes. Do not use the FlashCopy storage device Web interface or FlashCopy storage device Copy Services CLI to manipulate these source/target pairs as this could compromise the integrity of the backed up data on the target volumes. For example, avoid using the Web interface to withdraw persistent FlashCopy relationships between one or more source/target pairs. Instead use the Data Protection for Snapshot Devices commands for withdrawing the persistent FlashCopy relationships between all the source target pairs for a given database.

- If you receive a FlashCopy-related error during snapshot restore processing, view the Copy Services logs on the FlashCopy storage device.
- The combined length of the database name and the profile name cannot exceed the maximum character length allowed for a file name on the operating system.
- The restore metadata file generated during a Data Protection for Snapshot Devices backup is uniquely identified by the profile name and database name combination.

AIX Logical Volume Manager mirrored environments

Data Protection for Snapshot Devices currently supports AIX LVM mirroring only for FlashCopy devices.

Overview of Data Protection for Snapshot Devices support for AIX Logical Volume Manager mirrored environments

In a DB2 environment, support for this function is provided only by Data Protection for Snapshot Devices. There is no support in DB2 Advanced Copy Services for LVM mirroring.

Data Protection for Snapshot Devices currently supports AIX LVM mirroring only for FlashCopy devices. The use of LVM mirroring in an SVC configuration requires that the mirror sets be in different SVC clusters. Refer to the README and Release Notes information for the current status of the support for this requirement.

Related reference

"IBM Tivoli Storage Manager for Advanced Copy Services information sources" on page xv

Logical Volume Manager advantages

The LVM mirroring functionality offers the following advantages:

- Only *one* of the 2 AIX LVM LV mirrors becomes the subject of a triggered FlashCopy process, which
  - saves the number of needed target volumes
  - shortens the FlashCopy process
  - avoids unnecessary performance degradation within the storage system
  - avoids AIX LVM conflicts when at least one stale physical partition is produced within one or more AIX LVs on the backup system.
- Late failures within the FlashCopy operation due to unsuitable setups can be avoided; by checking the proper disk setup and customization, Data Protection for Snapshot Devices terminates in case of unsuitable conditions and therefore avoids unnecessary cleanup activities on the backup system.
- All AIX LVM mirrors on the production system therefore stay synchronized during the FlashCopy backup process. The FlashCopy backup process at no time compromises the high availability purpose the AIX mirrors were set up for. It is not necessary to resynchronize the LVs after the FlashCopy backup request.
- Online or offline FlashCopy backups can be taken in the same manner as before; there is no change in the backup/restore procedures as outlined in the applicable chapters.
- Data Protection for Snapshot Devices provides information about asymmetrical AIX LVM mirror setups when encountered, which can not only prevent the FlashCopy backup from running in unfavorable situations but can also reveal a general deficiency of the high availability setup as well.
- The software allows one copy set to be used in a FlashCopy backup to more than one target set in one hardware unit (see "Overview of multiple backup

generations (target sets) on disk" on page 37), thus increasing the earlier maximum number of disk backup levels from 2 to n[3].

- Data Protection for Snapshot Devices needs only one of the 2 copy sets for a snapshot restore, thereby
  - offering the possibility that 'n' FlashCopy backup versions can be eligible for a snapshot restore
  - enabling much faster return to production mode after an outage (everything for the synchronization of the VG will be prepared in advance; however the synchronization can be initiated by the DBA at a more suitable time later).

Logical Volume Manager functions

The targeted environment is an AIX LVM mirroring setup within which Data Protection for Snapshot Devices now provides the possibility of a much more economic backup strategy. This AIX LVM mirroring setup is considered to have the DB server on a production system running either

- in a single machine environment, or
- in a 2-machine environment (either as the primary or takeover machine) using HACMP (as shown in Figure 4 on page 51 or Figure 4 on page 51), where the mirrors are properly distributed within 2 hardware units (when working with 2 copy sets).[4]

The latter is often referred to as a disaster-tolerant solution. Both environments will have the two sets of copies, each residing in a different hardware unit and managed by AIX LVM. Such an AIX LVM mirrored environment is used in such a way that in case of the loss of one site (for example, the local machine and local hardware unit) the other site (with the remote machine and remote hardware unit) can still operate and perform a takeover. If the failure of the disk subsystem is just temporary, the AIX LVM takes care of the synchronization after the disk subsystem comes up again. In case of a single-machine setup, the environment is protected only against the outage of one of the 2 hardware units.

The goal of the Data Protection for Snapshot Devices support for the LVM mirroring functionality is to leave the general DB backup/restore procedures (as described in "Backup methods overview" on page 33 and "Restore methods overview" on page 43) unchanged, but to allow a customer having a setup with AIX LVM mirrors to deal with much fewer target volumes within a FlashCopy backup request compared to previous Data Protection for Snapshot Devices code levels.

Logical Volume Manager snapshot backup process: The snapshot backup request will be started on the production system. Identify which of the 2 (source) copy sets will be part of the snapshot backup; this depends on the parameters of started backup and the conditions from preceding backups.

A target set is identified in the target volumes file (.fct) by

- a target set ID 'x' (part of the topic name 'volumes_set_x'), and
- a hardware unit number or SVC cluster ID (value of the HARDWARE_ID_LVM_MIRROR parameter).

---

[3] This number is limited by the maximum number of concurrent FlashCopy relationships a source volume in the various hardware models can have and by the capacity of the hardware unit(s) used.

[4] It is clear that, in order to be protected against any physical loss, the hardware units and also the HA machines should be kept in different physical locations.

The existence of the HARDWARE_ID_LVM_MIRROR parameter enables Data Protection for Snapshot Devices to use its special functionality to back up, using FlashCopy, only one of the two copy sets.

Logical Volume Manager snapshot restore process: In addition to snapshot restore, the Data Protection for Snapshot Devices functionality for AIX LVM mirrored environments has been extended to

- allow the selection from 'n' snapshot backups (each representing a snapshot backup of one of the two copy sets to one of the 'n' target sets[5]) for a restore, assuming the device agent has signaled that the background copy has completed for the source/target volume pairs in the relevant copy set.
- (Oracle, SAP with Oracle) offer the administrator the capability to run Data Protection for Snapshot Devices tsm4acs to see which of the n target sets are eligible and ready to be selected for a snapshot restore (the brbackup run log file name and backup ID will be shown).
- perform the Data Protection for Snapshot Devices snapshot restore and the DB recovery with the volumes of the target set of the selected snapshot backup, for performance reasons; in addition, the snapshot restore function will run all the commands required to prepare the AIX LVM environment again for the second mirror; the administrator will be informed by message EEO0299I in the device agent log file that the VGs are ready for synchronization, which he can run later at a more suitable time.

  Note: The administrator must examine the log files for these messages. They will not be displayed on the screen.

Data Protection for Snapshot Devices and copy sets in an AIX logical volume manager mirror environment

In a Data Protection for Snapshot Devices FlashCopy configuration that uses AIX logical volume manager (LVM) mirrors, the production and takeover systems access the two sets of source volumes and the backup system accesses the target volumes.

The following figure shows a typical setup as it could run with the Data Protection for Snapshot Devices mirroring functionality:

---

[5] Assuming 'n' target sets with either FLASHCOPY_TYPE of INCR or COPY are available.

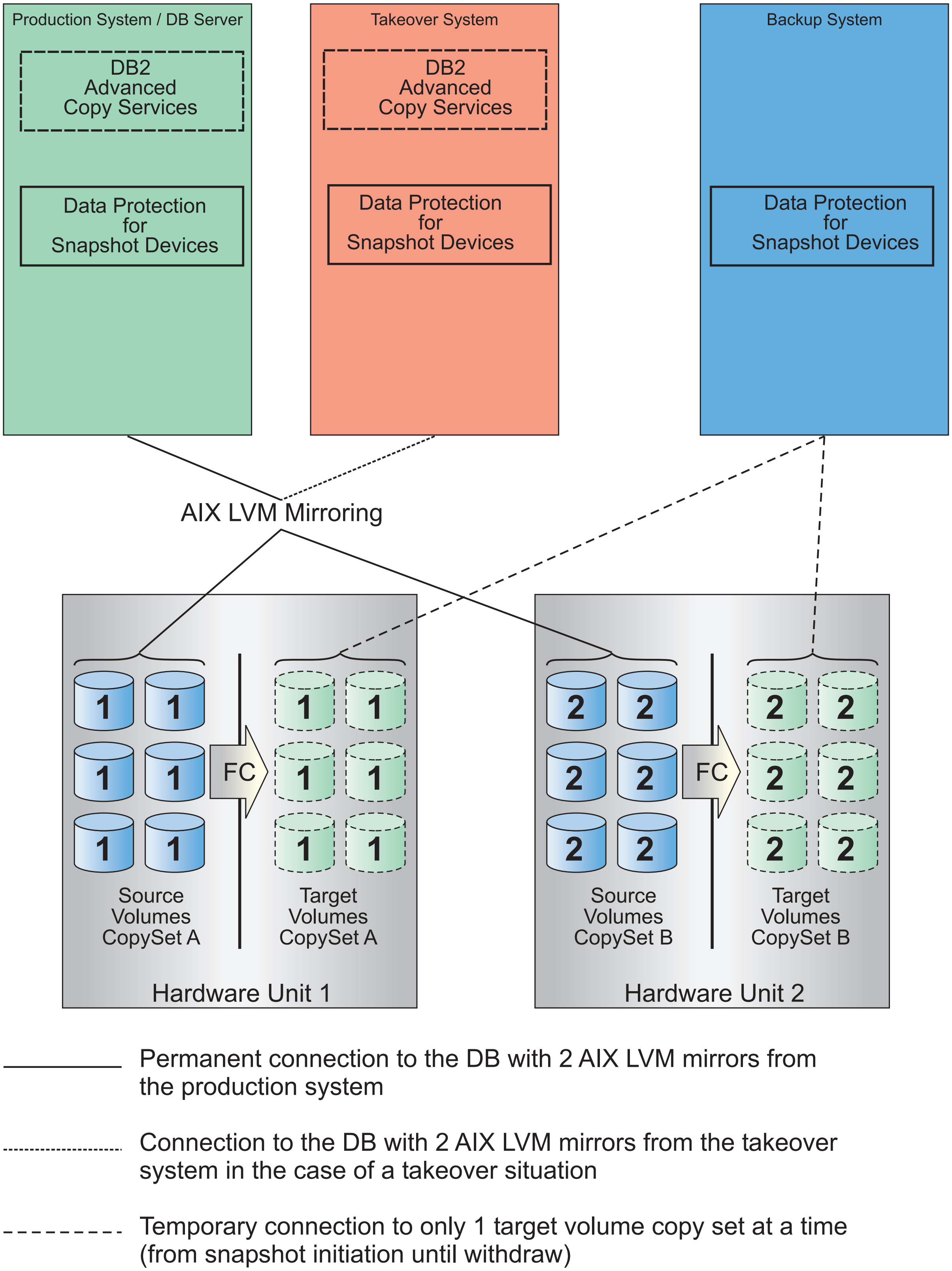

Production System / DB Server
DB2 Advanced Copy Services
Data Protection for Snapshot Devices
Takeover System
DB2 Advanced Copy Services
Data Protection for Snapshot Devices
Backup System
Data Protection for Snapshot Devices
AIX LVM Mirroring
1
FC
Source Volumes CopySet A
Target Volumes CopySet A
Hardware Unit 1
2
FC
Source Volumes CopySet B
Target Volumes CopySet B
Hardware Unit 2
Permanent connection to the DB with 2 AIX LVM mirrors from the production system
Connection to the DB with 2 AIX LVM mirrors from the takeover system in the case of a takeover situation
Temporary connection to only 1 target volume copy set at a time (from snapshot initiation until withdraw)

Figure 4. Data Protection for Snapshot Devices and Copy Sets in an AIX LVM Mirror Environment

This is a high-availability environment with 2 AIX mirrors distributed over 2 hardware units using HACMP and running production on the primary machine. Note that instead of the 2 machines running with HACMP, a single-machine environment could also be used for the database server activities connected to an AIX LVM mirror setup. The takeover machine currently does not perform any database related activities; however, in case of an HACMP takeover, there are no special considerations for this machine compared to the primary system discussion.

The database files that are the object of the FlashCopy backup process reside on logical volumes (LVs) that are mirrored by the AIX LVM. Because all file systems are running as JFS or JFS2, a mirrored jfslog LV for each volume group is required as well. The sum of all these LVs in one of the mirrors constitutes a complete copy set; a copy set resides on a set of source volumes, which themselves, when a symmetrical setup is in place, are completely located within one of the two hardware units. The other copy set is located with its source volumes in the other unit.

Both copy sets can be used alternately in different FlashCopy backup runs when Data Protection for Snapshot Devices initiates the FlashCopy process.

Although both copy sets are consistently mirrored on the production system by AIX LVM, only one will be required for the FlashCopy process and the subsequent Data Protection for Snapshot Devices backup running on the backup system. [6]

In order to focus on the Data Protection for Snapshot Devices functionality for AIX mirrored environments, this chapter will discuss a setup with 2 copy sets, each one having only one target set as shown in Figure 4 on page 51, even if Data Protection for Snapshot Devices would permit more target sets to be used.

The decision as to which of the two copy sets will be used by Data Protection for Snapshot Devices for the FlashCopy backup is done automatically by Data Protection for Snapshot Devices. The selected target set, as defined in one of the two topics of the target volumes files (.fct), can be used only for a FlashCopy backup of one (source) copy set if

- for an ESS or DS configuration, both sets reside in the same hardware unit, and the HARDWARE_ID_LVM_MIRROR parameter specifies the number of this unit.
- for an SAN Volume Controller configuration, both sets reside in the same SAN Volume Controller cluster and the HARDWARE_ID_LVM_MIRROR parameter specifies an ID for this cluster.

If the selected hardware unit does not contain a complete copy set of all LVs (in which the database files are allocated that are the object of the FlashCopy backup), Data Protection for Snapshot Devices will terminate; the same will occur if certain attributes have not been given either to the LVs or the involved volume groups (VG). The requirements for proper setup and customization are summarized later in this chapter.

Data Protection for Snapshot Devices, having started the FlashCopy operation on the production system, will continue on the backup system with `recreatevg/fsck/mount` with only those target volumes in the hardware unit specified in the HARDWARE_ID_LVM_MIRROR parameter within the topic (of the Data Protection for Snapshot Devices target volumes file) pointed to by the value of the chosen target set parameter. In the preceding figure, either the target volumes with copy set A in hardware unit 1 or the other target volumes with copy set B in hardware unit 2 will be selected.

---

[6] You could also consider using an additional backup system so each site would have its own complete environment in case a disaster hits one site.

Supported AIX Logical Volume Manager mirrored environments

Logical volume mirrors can be set up as symmetrical or asymmetrical environments.

The symmetrical environment is the most favorable.

Symmetrical environment

A symmetrical setup of all logical volumes (which are part of the database) is imperative for the high availability offered by AIX LVM mirroring, such that, if another subsystem with a mirror is still available, full operation can be maintained even in the case of the physical loss of a complete subsystem. Such a symmetrical setup would be the use of 2 hardware units with equal distribution of 2 AIX LVM mirrors for the database relevant logical volumes (LVs). It requires that one complete set of the first mirror of all LVs (also called a complete copy set) be allocated in one hardware unit and the second mirror of those LVs in the other unit. Two copy sets are located as an entity, each set in a separate hardware unit. Therefore, only target volumes for one copy set within one unit need to be specified for one FlashCopy backup request.[7] Since the symmetrical environment not only provides the highest availability for the database but also allows Data Protection for Snapshot Devices to work with the lowest possible number of target volumes in the FlashCopy backup process, it is the ideal setup for a production environment.

Within this target set, the HARDWARE_ID_LVM_MIRROR parameter matches the unit name in which the copy set resides. For each source volume of the one copy set, a target volume must be planned and set up.

Asymmetrical Environment

In contrast to the symmetrical database setup, the asymmetrical setup by its nature would never cover the outage of either of the 2 hardware units. The following combinations of such an asymmetrical setup and the impacts/implications on the high availability requirement as well as on the capabilities of the Data Protection for Snapshot Devices support for the LVM mirroring capability are summarized in the following:

- One unit (determined through either the specific or automated target set selection, and the topic and HARDWARE_ID_LVM_MIRROR parameter value derived therefrom) has a complete copy set and in addition one or more LV copies of the second copy set.

  Impact on high availability target:

  - The outage of this unit, with the complete copy set, would cause a production outage because of the incomplete database within the other unit

  Action taken by Data Protection for Snapshot Devices with the LVM mirroring functionality:

  - The unit contains a complete copy set of all LVs and one or more LV mirrors from the other copy set; FlashCopy backup can be done, but more target volumes than in the symmetrical case are required because the selection will be done against all source volumes that make up the VG residing in the selected unit and including the database files to be backed up.

---

[7] For the same copy set, however, additional target sets can be set up if multiple targets are desired for different FlashCopy backups.

- The unit (determined through either the specific or automated target set selection, and the topic and HARDWARE_ID_LVM_MIRROR parameter value derived therefrom) has an incomplete copy set, because the other unit (see 1.) has a complete copy set and parts of the 2nd copy set.

  Impact on high availability target:

  – The loss of this unit (which has fewer than half of all database LV mirrors) leaves the production operation working with a complete database copy set in the other unit.

  Action taken by Data Protection for Snapshot Devices with the LVM mirroring functionality:

  – Data Protection for Snapshot Devices cannot perform a FlashCopy backup process for this unit when it is selected, because the copy set of the source volumes making up the database in this unit is incomplete.
- Each unit has an incomplete copy set.

  One unit might have 2 AIX copies of an LV, and the other unit might form another LV with its 2 AIX copies. Neither of the 2 units now would have a complete copy set of its own.

  Impact on high availability target:

  – The outage of one of the 2 units would result in an outage of the database. Such a setup is the worst of all possibilities because there is really no protection against an outage should one of the 2 units be physically lost.

  Action taken by Data Protection for Snapshot Devices with the LVM mirroring functionality:

  – Data Protection for Snapshot Devices cannot perform a FlashCopy backup with either unit when one of the two incomplete copy sets has been selected via the target set selection algorithm. Running such a setup is certainly the least desirable alternative and must be resolved without delay by the system administrator.

Note: Asymmetrical setups must be avoided in order to prevent unforeseen problems. If such setups occur over time for the sake of

- high availability and
- the planned FlashCopy backup capabilities

an asymmetrical setup should be restored to a symmetrical one.

AIX Logical Volume Manager mirrors configuration requirements

An LVM mirror environment requires specific configuration tasks and settings in order to function properly with Data Protection for Snapshot Devices.

In order to run a sound high availability environment, certain requirements are imposed on such an environment; others are specifically needed to allow the FlashCopy of only such source volumes containing one LVM mirror of the logical volumes when they are the subject of a FlashCopy backup request using the Data Protection for Snapshot Devices functionality.

The following summarizes the database setup requirements which must be fulfilled when using an AIX 2-mirror environment:

1. The topic within the target volumes file (determined through automated target set selection for the FlashCopy backup) needs the parameter HARDWARE_ID_LVM_MIRROR to specify the hardware unit in which the FlashCopy is to be performed. In addition, a complete copy set (all LVs must have at least 1 mirror in this copy set) is required.

Data Protection for Snapshot Devices action: Terminates immediately if the HARDWARE_ID_LVM_MIRROR parameter has not been set.

2. Each file that is the object of the FlashCopy backup request 2) must reside on an LV which has its physical disks (hdisks, or vpaths in case of SDD) in a hardware unit. These disks are referred to as the source volumes.

   Data Protection for Snapshot Devices action: Terminates immediately if a file is not found on a volume.

   The same applies to the jfslog LV associated with the aforementioned LV.
3. Each of the above database LVs and its jfslog LV must have 2 mirrors.

   Data Protection for Snapshot Devices action: Terminates immediately if other values are found.
4. All source volumes which belong to one LV mirror must reside in the same hardware unit.

   Data Protection for Snapshot Devices action: Terminates immediately if other conditions are found and this is the unit specified in 1.
5. All source volumes which belong to the other LV mirror should reside in another unit.

   Data Protection for Snapshot Devices action: Terminates immediately if unsuitable conditions are found.
6. Two hardware units are required (this is the maximum supported by Data Protection for Snapshot Devices in an AIX 2-mirror environment)

   Data Protection for Snapshot Devices action: Data Protection for Snapshot Devices will terminate if it cannot find a complete copy set in the selected unit (see 1.) If one of the 2 units is temporarily not available and the other is properly set up, production and the FlashCopy backup process are not functionally impacted (symmetrical environment) if the target set is used that resides in the available unit; the HARDWARE_ID_LVM_MIRROR parameter matches the unit name.
7. All source volumes of one copy set (the entity of one AIX LVM mirror of all involved LVs) are highly recommended to be in the same unit; accordingly, the other complete copy set needs to be set up in the other unit); this addresses the symmetrical environment, which is the one the system administrator should implement.

   Data Protection for Snapshot Devices action: For details, see "Supported AIX Logical Volume Manager mirrored environments" on page 53.
8. A logical volume (LV) must have a complete mirror with the same mirror number for all of its physical partitions on a set of logical volumes within the selected hardware unit. The command `lsvg -M <vgname>` displays various information concerning mirrored logical volumes, including the mirror number.

   Within one hardware unit, the mirror numbers of the various LVs might be different.

   Data Protection for Snapshot Devices action: Terminates immediately if a complete LV is not found within the specified hardware unit (see 1.) and the PPs of this LV in this hardware unit do not have the same copy number (see Copynum value in the output of the lsvg -M <vgname> command).
9. Target volumes must have been
   - set up in the above specified hardware unit and
   - defined in the Data Protection for Snapshot Devices .fct file for each source volume in the selected unit (see 1.).

Data Protection for Snapshot Devices action: Terminates immediately if not set up or the .fct file is incomplete.

10. It is highly recommended not to have LVs other than the database LVs and the required jfslog LVs in the VGs because, if they have source volumes in the selected unit, they require target volumes to be specified as well. In addition, this can result in unforeseen problems such as impacts of the metastructure of their embedded JFS or JFS2 structure.

    Data Protection for Snapshot Devices action: Ignores this situation within the FlashCopy backup process as long as enough target volumes have been defined.
11. The volume group (VG) that hosts the LVs (database and jfslogs) must have been set up with the parameters:

    ```
    MIRROR WRITE CONSISTENCY  = YES
    QUORUM                    =  NO          (turned off)
    ```

    Data Protection for Snapshot Devices action: Terminates immediately if other values are found.
12. Each of the involved LVs (database and logs) must have been set up with

    ```
    COPIES         : 2
    SCHED POLICY   : PARALLEL, PARALLEL/SEQUENTIAL, PARALLEL/PARALLEL, STRIPED
    ```

    Note: (SAP only). According to SAP requirements (as stated in *mySAP.com Fundamentals of Database Layout (8/2000)*) when using a database setup with striping, the stripe size should be a multiple of the data block size (8K) and at least 16K. Data Protection for Snapshot Devices imposes the same requirement.

    Each of the jfslog LVs used by the database logical volumes must have been set up with

    ```
    COPIES         : 2
    SCHED POLICY   : PARALLEL, PARALLEL/SEQUENTIAL, PARALLEL/PARALLEL, STRIPED
    ```

    All of its LPs for one copy must be allocated to one OS disk (AIX physical volume) only.

    Data Protection for Snapshot Devices action: Terminates immediately if other values are found. The schedule policy SEQUENTIAL is not supported with Data Protection for Snapshot Devices.

    Note: In order to have the 2 LVM mirrors of the LVs allocated on separate logical volumes and located in different hardware units, suitable source volumes must be chosen when creating the LVs.
13. The LVs of the involved copy set are not permitted to have stale physical partitions (PP), either prior to or immediately after the FlashCopy operation.

    Data Protection for Snapshot Devices action: Terminates immediately if any stale PPs are found.

Related concepts

"Supported AIX Logical Volume Manager mirrored environments" on page 53
Provides information regarding symmetrical and asymmetrical environments.

"AIX Logical Volume Manager mirrors configuration requirements" on page 54
Provides information regarding mirror requirements.

Target set selection guidelines

The target volumes that are used for one copy set of source volumes need to be specified with the Data Protection for Snapshot Devices target volumes file.

If one copy set will be re-used for a FlashCopy backup, depending on the FLASHCOPY_TYPE (INCR, COPY, or NOCOPY), the Data Protection for Snapshot Devices unmount function, or ’db2acsutil delete’ with the DELETE_FORCE vendor option, must be done first.

At restore time, a target set does not need to be specified. The copy set and target set to be selected are automatically determined with the backup you selected for a restore. A snapshot restore from a FlashCopy target set of a copy set can only be started when the background copy, initiated by FlashCopy backup (INCR or COPY) running with this copy set, has completed.

Parameters required for a later snapshot restore for native Oracle databases

The FLASHCOPY_TYPE parameter requires specific values when planning to perform a snapshot restore at a later date.

If you plan to use the target set(s) for a snapshot restore, you have to ensure when running Data Protection for Snapshot Devices within the `brbackup` that the FLASHCOPY_TYPE is specified as INCR or COPY in the Data Protection for Snapshot Devices profile with the FLASHCOPY_TYPE parameter.

A detailed description of all parameters of the Data Protection for Snapshot Devices profile is shown in “Data Protection for Snapshot Devices profile parameters” on page 164.

For details about snapshot restore, see “Restore methods overview” on page 43; also see “Overview of multiple backup generations (target sets) on disk” on page 37 when using multiple target sets for one copy set.

Example Target Volumes file in a mirrored environment

The HARDWARE_ID_LVM_MIRROR parameter must be specified in the target volumes file when operating in a mirrored environment.

The structure of this file is similar to that described in “Data Protection for Snapshot Devices Target Volumes File (.fct)” on page 189, with the exception of the HARDWARE_ID_LVM_MIRROR parameter.

The parameter HARDWARE_ID_LVM_MIRROR is specified for each target set, in the respective target set topic.

For the AIX LVM mirrored setup – assuming both copy sets, each with one target set, will be used for backup/FlashCopy – the two topics look as follows:

```
>>>volumes_set_1
HARDWARE_ID_LVM_MIRROR  XXXXX
TARGET_VOLUME ...
...
...
TARGET_VOLUME ...
<<<volumes_set_1



>>>volumes_set_2
HARDWARE_ID_LVM_MIRROR  YYYYY
TARGET_VOLUME ...
...
...
TARGET_VOLUME ...
<<<volumes_set_2
```

where XXXXX and YYYYY reflect the serial numbers of the 2 hardware units or the IDs of the SAN Volume Controller clusters.

Target Volume file parameters for ESS and DS:

Specific values must be specified when operating Data Protection for Snapshot Devices on ESS or DS storage subsystems in an LVM mirrored environment.

Each target volume planned for use must be specified by its serial number as shown in "Data Protection for Snapshot Devices Target Volumes File (.fct)" on page 189. When Data Protection for Snapshot Devices is executing the FlashCopy function, it will, for each source volume which was identified as a candidate for a FlashCopy, look for

- a source/target volume correlation, or
- a target-volume-only specification

In addition, Data Protection for Snapshot Devices will - when it finds the HARDWARE_ID_LVM_MIRROR parameter in the selected target set — check for a proper setup of the AIX LVM mirrors of the LVs used for the database.

Table 23. Additional Parameter in the Data Protection for Snapshot Devices Target Volumes File for AIX LVM Mirrored Environments Using an ESS or DS

Parameter Name	**Value**
HARDWARE_ID_LVM_MIRROR *unit name*	In an AIX LVM mirror environment, specifies the serial number of the ESS or DS device that contains a complete set of at least one copy of all database logical volumes (LVs) that are subject to the backup process. Only the source volumes of the specified hardware unit will be used on the production system by Data Protection for Snapshot Devices for the FlashCopy process. *unit_name* must match the unit name that is part of the target volume serial number specified on the TARGET_VOLUME parameters that follow the HARDWARE_ID_LVM_MIRROR parameter. This parameter can be used only if an appropriate setup of the logical volumes of the database has been done as defined in "Overview of Data Protection for Snapshot Devices support for AIX Logical Volume Manager mirrored environments" on page 48. Default: None. Not used if not defined.

Samples of the different setup possibilities for the TARGET_VOLUME parameter are shown in "Example target volume file (mirror setup on ESS or DS configuration)" on page 209.

Target Volume file parameters for SAN Volume Controller:

Specific values must be specified when operating Data Protection for Snapshot Devices on SAN Volume Controller in an LVM mirrored environment.

Each target volume planned for use must be specified by its virtual disk name as shown in "Data Protection for Snapshot Devices Target Volumes File (.fct)" on page 189. When Data Protection for Snapshot Devices is executing the FlashCopy function, it will, for each source volume which was identified as a candidate for a FlashCopy, look for

- a source/target volume correlation, or
- a target-volume-only specification

In addition, Data Protection for Snapshot Devices will — when it finds the HARDWARE_ID_LVM_MIRROR parameter in the selected target set — check for a proper setup of the AIX LVM mirrors of the LVs used for the database.

Table 24. Additional Parameter in the Data Protection for Snapshot Devices Target Volumes File for AIX LVM Mirrored Environments Using SAN Volume Controller

Parameter Name	**Value**
HARDWARE_ID_LVM_MIRROR *cluster name*	In an AIX LVM mirror environment, specifies the name of the cluster that contains a complete set of at least one copy of all database logical volumes (LVs) that are subject to the backup process. Only the source volumes of the specified cluster will be used on the production system by Data Protection for Snapshot Devices for the FlashCopy process. This parameter can be used only if an appropriate setup of the logical volumes of the database has been done as defined in "Overview of Data Protection for Snapshot Devices support for AIX Logical Volume Manager mirrored environments" on page 48. Default: None. Not used if not defined.

Samples of the different setup possibilities for the TARGET_VOLUME parameter are shown in "Example target volumes file (SAN Volume Controller configuration)" on page 207.

Chapter 3. Installing Data Protection for Snapshot Devices

Data Protection for Snapshot Devices is delivered as a platform-specific InstallAnywhere package. Configuration tasks are required after successful installation.

(DB2) As soon as Data Protection for Snapshot Devices for DB2 Advanced Copy Services has been installed and the DB2 instance is updated, DB2 will no longer update DB2 Advanced Copy Services within a DB2 fix pack installation. The database administrator must upgrade Data Protection for Snapshot Devices separately with the IBM Tivoli Storage Manager for Advanced Copy Services PTFs or releases. DB2 will check for the existence of the license file (`<DB2 instance directory>/acs/tsmacs.lic`) to verify that Data Protection for Snapshot Devices is installed. If this file is detected during a DB2 instance upgrade, the DB2 Advanced Copy Services modules will not be upgraded.

Installation recommendations

- Refer to the hardware and software requirements Web page in the Release Notes to verify that all installation prerequisites have been satisfied.
- Refer also to the summary of the major files and directories involved in the installation process.
- Data Protection for Snapshot Devices must be installed on all production (database nodes) and the backup system.
- (DB2) Each production system running Data Protection for Snapshot Devices to a common backup system must use a different DB2 system identifier (SID).
- The version and maintenance level of Data Protection for Snapshot Devices that is used for the snapshot copy of one database (SID) must be the same on the production and backup systems.
- After the installation of Data Protection for Snapshot Devices, you must run the setup script for each specific instance on the production system, as well as on the backup system. This allows the production and backup systems to have multiple versions and maintenance levels installed.
- Prior versions of Data Protection for Snapshot Devices should be uninstalled to remove the old files.
  - To uninstall V5.5, see “Uninstalling Data Protection for Snapshot Devices” on page 100.
  - To uninstall V5.3 or V5.4, use InstallShield (`/usr/tivoli/tsm/tdpessr3/<database>/_uninstall` or `/usr/tivoli/tsm/acs/<database>/_uninstall`, respectively).

Related tasks

"Data Protection for Snapshot Devices installation prerequisites" on page 66
Data Protection for Snapshot Devices requires specific applications and settings to exist before it can be successfully installed.

"Uninstalling Data Protection for Snapshot Devices" on page 100
Uninstall Data Protection for Snapshot Devices as described in this procedure.

Related reference

"Key files and directories" on page 194
Certain files and directories are of considerable importance when using Data Protection for Snapshot Devices.

Installation process overview

This section provides an overview of the steps that are required to install Data Protection for Snapshot Devices.

To set up Data Protection for Snapshot Devices you need to perform the following basic steps:

1. Install the Data Protection for Snapshot Devices binaries to a global install directory (/usr/tivoli/tsm/acs_<TSM ACS version>)
2. Activate Data Protection for Snapshot Devices for selected database instances
3. Configure Data Protection for Snapshot Devices for selected systems

If you are performing an upgrade you need to repeat steps 1 and 2.

Data Protection for Snapshot Devices is installed on a production server (PS) and optionally on a backup server (BS) if one is employed. The decision whether TSM for ACS is installed on a PS or BS is made during step 3. Steps 1 and 2 do not distinguish between PS and BS configurations.

For federated DB2 environments (DB2 DPF), the PS installation is required on only one DB2 node. This is because, for DB2, the installation directory is an NFS share that is automatically accessible from all other DB2 nodes.

Installation sequence

This section provides further details about each of the steps that are required to set up Data Protection for Snapshot Devices.

Installation step

During installation of Data Protection for Snapshot Devices all binaries are copied to the global installation directory (/usr/tivoli/tsm/acs_<TSM ACS version>). During de-installation those binaries are removed. Due to the fact that the files in the global installation directory are copied to a product version-based target directory, multiple versions of Data Protection for Snapshot Devices can be installed concurrently and there is no need for an upgrade installation.

The installation needs to be performed as user **root** and can only be executed via InstallAnywhere.

Note: The files in the global installation directory are not used directly. They need to be activated for a particular system before they can be used.

Activation step

During activation all binaries are copied from the global installation directory to the instance specific installation directory (INST_DIR) and the access rights of all executable files are set properly (the s-bit is set for device agents).

If the product has been activated previously, the previous version of Data Protection for Snapshot Devices will be stopped and restarted after the data is copied to the instance specific install directory. The steps of stopping and starting Data Protection for Snapshot Devices are performed on the PS and BS.

Note: Activation on a BS may fail if Data Protection for Snapshot Devices is already running on the PS and the instance specific installation directory is an NFS share between the PS and BS. In such a case Data Protection for Snapshot Devices needs to be stopped on the PS prior to activating Data Protection for Snapshot Devices on the BS.

The activation step needs to be executed as root and can be performed via InstallAnywhere or by invoking:

```
setup_<database>.sh –a install –d <INST_DIR> -u <user> -g <group>
```

Activation on the BS in environments where the INST_DIR is an NFS share between the PS and BS

If both the configuration directory and the instance-specific installation directory are NFS-shared between all PS and BS nodes, TSM for ACS is, after initial configuration, best administered from the *master PS node only*. For the initial configuration, TSM for ACS needs to be installed, activated, and configured on the PS, and afterwards configured on the BS. The installation and activation steps on the BS can be skipped. Upgrades and reconfigurations should only be performed on the master PS node. There is typically no need for invoking the setup script on the BS after initial configuration.

Exceptions to this rule may include:

- The release notes may mention that an upgrade requires you to activate or reconfigure the BS in such a configuration
- The use of alternative storage hardware may require a reconfiguration of TSM for ACS on the BS
- Changes to the scheduling policy for offloaded TSM backups may require you to reconfigure the BS

In these cases, you need to stop TSM for ACS on the PS before reconfiguring the BS. Otherwise you will be prompted to stop TSM for ACS on the PS.

Configuration step

The configuration of Data Protection for Snapshot Devices is required only once after the initial activation of the product. Configuration is required on the PS and BS and is initiated by invoking the setup script without any arguments. During configuration Data Protection for Snapshot Devices creates the following:

- the configuration directory (ACS_DIR, typically <Instance owner’s $HOME directory>/acs)
- the profile <Instance owner’s $HOME directory>/acs/profile
- a link to the profile from the instance specific installation directory (INST_DIR/profile)

In addition to these steps the appropriate (PS and BS specific) /etc/inittab entries are made during this step.

Typically, that is, when INST_DIR is NFS-shared with other nodes, Data Protection for Snapshot Devices needs to be configured on only one PS node (for federated DPF environments only on one node), and on the BS.

Typical configurations

The following table shows typical configurations:

		Production server (one node)				**Backup server**			
Instance installation directory	**Configuration directory (including ACS_DIR)**	**Installation**	**Activation**	**Initial PS configuration**	**Profile sections**	**Installation**	**Activation**	**Initial BS configuration**	**Profile sections**
Not NFS share	NFS share	Yes	Yes	Generate profile	All	Yes	Yes	Skip profile generation	Reused from PS
Not NFS share	No NFS share	Yes	Yes	Generate profile	All except OFFLOAD	Yes	Yes	Generate profile	GLOBAL OFFLOAD
NFS share	NFS share	Yes	Yes	Generate profile	All	No	No	Skip profile generation	Reused from PS
NFS share	Not NFS share	Yes	Yes	Generate profile	All except OFFLOAD	No	No	Generate profile	GLOBAL OFFLOAD

Note: The installation wizard always configures all sections, even if some are not required.

Configuration using the setup script is optimized for environments where the configuration directory is an NFS share among all PS and BS nodes, but the instance-specific installation directory is an NFS share only among PS nodes and is not shared between the PS and BS. In this case the setup script can be invoked on the master PS node and BS node independently.

In such a configuration the profile and password files created on the master PS node are automatically available to all other PS and BS nodes. That is, the profile needs to be created only once and can be centrally administered. In such a configuration, TSM for ACS needs to be configured only once on the BS, and the step to generate a profile on BS can be skipped (see table). Upgrades of TSM for ACS need to be installed and activated on the PS and BS before TSM for ACS is operational again. It is recommended to upgrade the PS first.

If the configuration directory is not NFS-shared between PS and BS

In such a configuration, you have to ensure that all nodes have access to a copy of the profile and to all files residing in ($ACS_DIR)/shared.

It is permssible for different nodes to use different profiles, but some minimum consistency requirements need to be observed. It is also required that at least the following profile sections be available on the various TSM for ACS nodes:

- The global section is required on all nodes
- The CLIENT (and ORACLE) sections are required on PS nodes
- The OFFLOAD section is required only on the BS

The ACSD and device sections are required only for the profile that is loaded from acsd.

Data Protection for Snapshot Devices installation prerequisites

Data Protection for Snapshot Devices requires specific applications and settings to exist before it can be successfully installed.

This prerequisite information must be taken into account in order for Data Protection for Snapshot Devices to install successfully. The **README** files and release notes contain the most current information on hardware and software requirements, including specific release levels. Refer to the Hardware/Software Requirements link in the release notes.

(DB2) The assumption is made that DB2 Advanced Copy Services is already installed, so that the installation process represents an upgrade.

Preparing the disk layout

It is helpful to plan and review the disk configuration layout in your environment before performing any installation tasks.

This planning assists in avoiding reinstallation work, unplanned snapshot backup behavior, and conflicting situations when performing a snapshot restore. The system environment consists of a production system (which contains the database server) and a backup system for offloading the backup to Tivoli Storage Manager. The production system contains a disk setup for the database so that the database files are allocated on source volumes. The corresponding target volumes will be accessible to receive the snapshots of each source volume. For the IBM FlashCopy process, corresponding target volumes have to be configured for each source volume by the user. For the NetApp Snapshot feature, the snapshot function is managed within the storage system, and Data Protection for Snapshot Devices automatically creates target clone volumes when they are required, such as for offloaded tape backup. Multiple sets of target volumes can be used, in order to have different generations of disk copy backups.

To assist in setting up the disk environment properly, an overview of the Data Protection for Snapshot Devices (and DB2 Advanced Copy Services) processing that occurs when a snapshot is requested is provided here. When a snapshot is requested

DB2:

- all tablespace container files
- all files in the local database directory
- the database log directory (if specified by the `'db2 backup'` command)

Oracle:

- all tablespace container files
- all files in the local database directory

must either

- be transferred via the FlashCopy mechanism to the target volumes (FlashCopy devices), or
- reside on volumes that are subject to the snapshot mechanism (N Series).

Because all these database files are involved in the snapshot process, the following rules must be observed:

- The database files (or the underlying logical volumes) must reside on source volumes which are copied to target volumes as a result of a snapshot request.
- Files from other applications should not be allocated on the set of physical volumes used for the database files. This helps prevent complications with these files in the case of a snapshot restore.

Consider mounting shared directories via NFS prior to installing Data Protection for Snapshot Devices.

Related concepts

"Mounting shared directories via NFS" on page 116
The $HOME/acs directories on the production system should be mounted on the backup system.

Subdividing the disk environment for DB2

Subdivide the disk environment for DB2 before installing Data Protection for Snapshot Devices.

For best results when planning to install Data Protection for Snapshot Devices, first subdivide the disk environment (distributed over the two systems) into the following six categories. An illustration is provided in Figure 5 on page 69.

1. Local disks on the production system (p_disk category)

   Besides the operating system disks, the production system also contains the disks where DB2 and SAP executable files (if applicable) will be placed during DB2 and SAP installation.
2. Source volumes (disks) on the production system (db_disk and db_log categories)

   The db_disk category contains files (such as tablespace containers) and the local database directory. The db_log category contains database log files.

   Make sure that these two categories reside on separate source volumes. This allows a snapshot restore to process when the LOGTARGET EXCLUDE parameter is specified (which is the default). Otherwise, LOGTARGET INCLUDE FORCE must be specified for the restore command. This causes the log directory to be included in the restore and overwrites the current log directory. If db_log resides on the same volumes as db_disk, this would require saving the log files in this directory prior to the snapshot operation and copying them back when the restore has completed.

   All the disks that make up the volume groups in which the files reside must be logical volumes. These volumes become the source volumes during the FlashCopy or snapshot operation. For FlashCopy devices, at least the same number of target volumes (constituting one target set) must be planned and made available for the planned FlashCopy operations. These volumes will become available, with the image copies, on the backup system after the FlashCopy has been initiated by DB2 Advanced Copy Services.
3. 'Shared disks' on the production system (NFS_disk category)

   Using the NFS mount, the backup system must have access to the following directory on the production system:

   ```
   $HOME/acs
   ```

   or access to each of these individual subdirectories:

   ```
   $HOME/acs/shared
   $HOME/acs/acsvolumes
   $HOME/acs/acsrepository
   ```

   These shared directories, as part of the local disk setup of the production system, are exported on the production system so that they can be NFS-mounted on the backup system. They can also be used by Tivoli Storage Manager for ERP to share profiles and password files.
4. Supplementary local disks on the production system (p_db_disk category)

   These disks contain the DB2 instance directory and the log archive directories (if used for DB2 log management).
5. Local disks on the backup system (b_disk category)

   Besides the operating system disks, the backup system also contains the disks on which DB2 executable files are placed during the installation.
6. Disks for the Tivoli Storage Manager server (optional, TSM_disk category)

If the Tivoli Storage Manager server will operate on the backup host, you must plan for an additional disk category (TSM_disk category) for the Tivoli Storage Manager database, log, and storage disks.

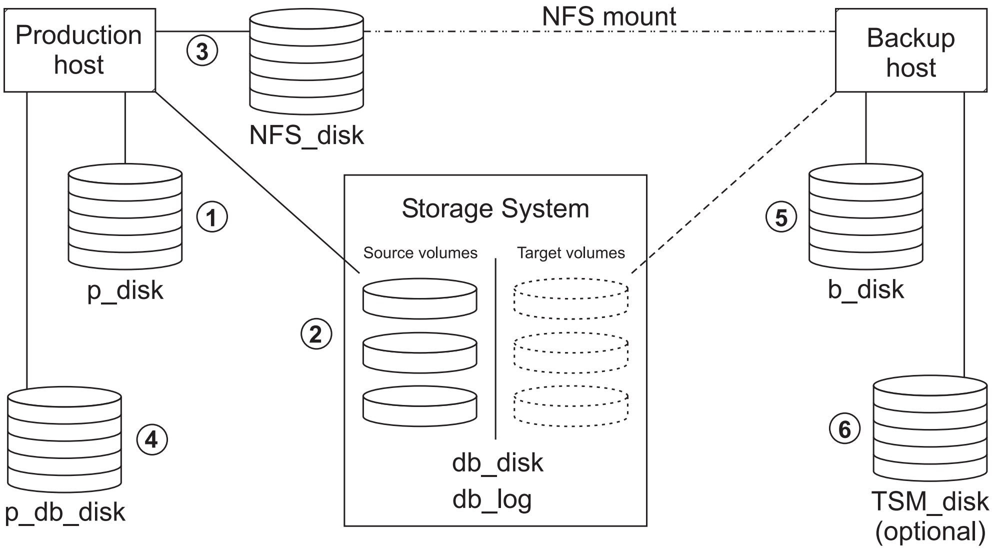


Figure 5. Overview of the Backup Scenario (DB2, Single Target Set)

Compared to Figure 5, Figure 6 depicts an environment with multiple target sets, in which the snapshot backup can be done to different target sets, thus allowing different disk-copy backup levels (see “Overview of multiple backup generations (target sets) on disk” on page 37).

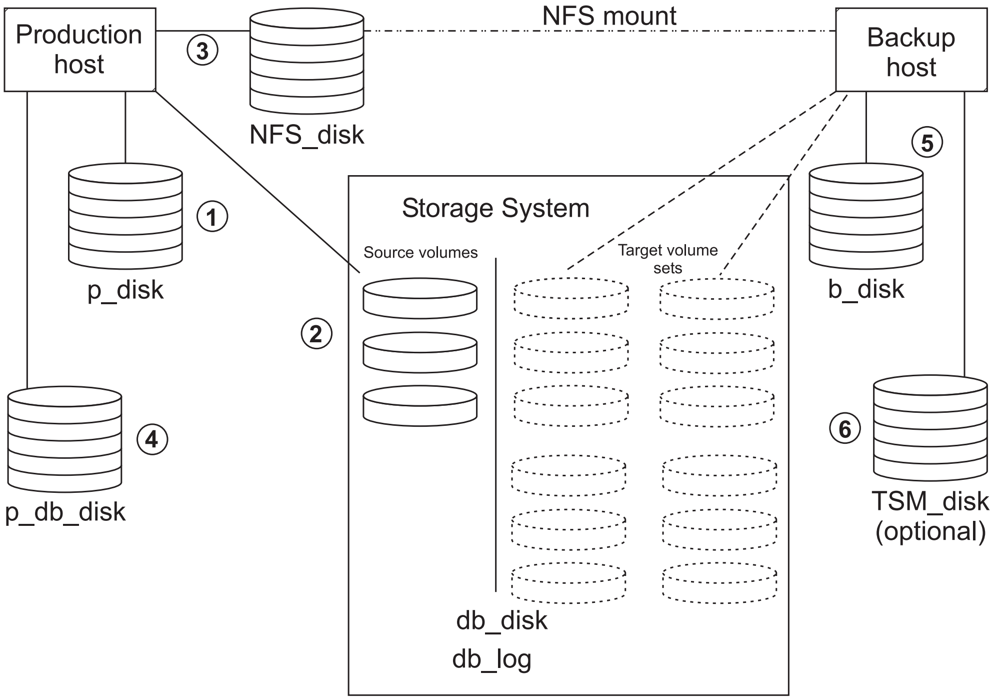


Figure 6. Overview of the Backup Scenario (DB2, Multiple Target Sets)

The above layout does not prevent using disks for categories 1, 3, 4, 5, and 6 in the database storage system as well. It is meant to depict the various categories to be managed and to highlight the role of FlashCopy source volume and target volume pairs, which are used in the snapshot process.

By following the above approach, you ensure that Tivoli Storage Manager for ERP and the Tivoli Storage Manager interface on the backup system (Tivoli Storage Manager for ERP or the DB2 native Tivoli Storage Manager agent) will find all files that must be backed up to Tivoli Storage Manager.

Related concepts

"AIX Journaled File Systems overview" on page 76
Data Protection for Snapshot Devices supports operations on AIX JFS or JFS2 file systems.

"Logical volume name requirements" on page 76
Data Protection for Snapshot Devices uses logical volume names for best results.

"Concurrent I/O setup requirements" on page 77
Data Protection for Snapshot Devices propagates the concurrent I/O in the Enhanced Journaled File System (JFS2).

"Data Protection for Snapshot Devices and copy sets in an AIX logical volume manager mirror environment" on page 50
In a Data Protection for Snapshot Devices FlashCopy configuration that uses AIX logical volume manager (LVM) mirrors, the production and takeover systems access the two sets of source volumes and the backup system accesses the target volumes.

"Overview of Data Protection for Snapshot Devices in an SAP® environment" on page 1
Support for SAP® environments requires installation of the appropriate SAP-capable component of Data Protection for Snapshot Devices.

Related reference

"Environment requirements" on page 89
Data Protection for Snapshot Devices requires specific environment conditions to exist before it can be installed successfully.

"Example overall disk layout for a DB2 environment" on page 199
Refer to this example when configuring the disk layout for a DB2 environment.

Subdividing the disk environment for Oracle

Subdivide the disk environment for Oracle before installing Data Protection for Snapshot Devices.

For best results when planning to install Data Protection for Snapshot Devices, first subdivide the disk environment (distributed over the two systems) into the following categories. An illustration of these categories is provided in Figure 7 on page 71.

1. Local disks on the production system (p_disk category)

   Besides the operating system disks, the production system also contains the disks where Oracle and SAP executable files (if applicable) will be placed during Oracle and SAP installation.

2. Source volumes (disks) on the production system (db_disk and db_log categories)

   The db_disk category contains files (such as tablespace containers) and the local database directory. The db_log category contains database log files.

   All the disks that make up the volume groups in which the files reside must be logical volumes. These volumes become the source volumes during the FlashCopy or snapshot operation. For FlashCopy devices, at least the same number of target volumes (constituting one target set) must be planned and made available for the planned FlashCopy operations. These volumes will become available, with the image copies, on the backup system after the FlashCopy has been initiated by Data Protection for Snapshot Devices for Oracle.

3. 'Shared disks' on the production system (NFS_disk category)

   Using the NFS mount, the backup system must have access to the following directory on the production system:

   ```
   $HOME/acs
   ```

   or access to each of these individual subdirectories:

   ```
   $HOME/acs/shared
   $HOME/acs/acsvolumes
   $HOME/acs/acsrepository
   ```

   These shared directories, as part of the local disk setup of the production system, are exported on the production system so that they can be NFS-mounted on the backup system. They can also be used by Tivoli Storage Manager for ERP to share profiles and password files.
4. Supplementary local disks on the production system (p_db_disk category)

   These disks contain the Oracle instance directory.
5. Local disks on the backup system (b_disk category)

   Besides the operating system disks, the backup system also contains the disks on which Oracle executable files are placed during the installation.
6. Disks for the Tivoli Storage Manager server (optional, TSM_disk category)

   If the Tivoli Storage Manager server will operate on the backup host, you must plan for an additional disk category (TSM_disk category) for the Tivoli Storage Manager database, log, and storage disks.

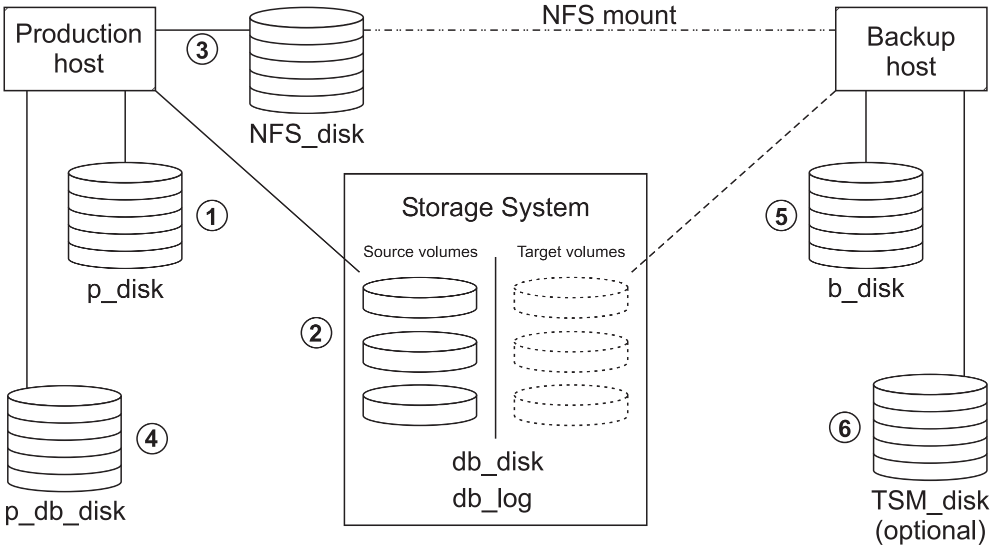


Figure 7. Overview of the Backup Scenario (Oracle, Single Target Set)

The above layout does not prevent using disks for categories 1, 3, 4, 5, and 6 in the database storage system as well. It is meant to depict the various categories to be managed and to highlight the role of FlashCopy source volume and target volume pairs, which are used in the snapshot process.

By following the above approach, you ensure that Tivoli Storage Manager for ERP and the Tivoli Storage Manager interface on the backup system (Tivoli Storage Manager for ERP or the DB2 native Tivoli Storage Manager agent) will find all files which must be backed up to Tivoli Storage Manager.

Related concepts

"AIX Journaled File Systems overview" on page 76
Data Protection for Snapshot Devices supports operations on AIX JFS or JFS2 file systems.

"Logical volume name requirements" on page 76
Data Protection for Snapshot Devices uses logical volume names for best results.

"Concurrent I/O setup requirements" on page 77
Data Protection for Snapshot Devices propagates the concurrent I/O in the Enhanced Journaled File System (JFS2).

"Data Protection for Snapshot Devices and copy sets in an AIX logical volume manager mirror environment" on page 50
In a Data Protection for Snapshot Devices FlashCopy configuration that uses AIX logical volume manager (LVM) mirrors, the production and takeover systems access the two sets of source volumes and the backup system accesses the target volumes.

"Overview of Data Protection for Snapshot Devices in an SAP® environment" on page 1
Support for SAP® environments requires installation of the appropriate SAP-capable component of Data Protection for Snapshot Devices.

Related reference

"Environment requirements" on page 89
Data Protection for Snapshot Devices requires specific environment conditions to exist before it can be installed successfully.

Disaster recovery and business continuity support overview

Data Protection for Snapshot Devices provides support for Metro Mirror, Global Copy, and Global Mirror environments

Data Protection for Snapshot Devices supports the following relationships of FlashCopy volumes in a Metro Mirror, Global Copy, or Global Mirror environment, also known as Peer-to-Peer Remote Copy (PPRC). While other combinations might be supported by the hardware, Data Protection for Snapshot Devices support is limited to the listed cases:

Metro Mirror

- A FlashCopy source volume can become a Metro Mirror primary volume and vice versa. The order of creation is optional.
- A FlashCopy target volume can become a Metro Mirror primary volume and vice versa. If you want to use a FlashCopy target volume as a Metro Mirror primary, be aware of the following considerations:
  - The recommended order is to first establish the Metro Mirror, and then enable a FlashCopy volume for that Metro Mirror primary. The Metro Mirror secondary will not be in a fully consistent state until the Metro Mirror enters the full duplex state.
  - If you create the FlashCopy first and then enable a Metro Mirror of the FlashCopy target, you must monitor the progress of the FlashCopy background copy. In this case the following considerations apply:

    - The Metro Mirror secondary will not be in a fully consistent state until the FlashCopy background copy process is complete.
    - Use the copy option to ensure that the entire FlashCopy source volume data is copied to the Metro Mirror secondary.

Global Copy

- A FlashCopy source volume can become a Global Copy primary volume and vice versa. The order of creation is optional.
- A FlashCopy target volume can become a Global Copy primary volume and vice versa. If you want to use a FlashCopy target volume as a Global Copy primary, be aware of the following considerations:
  - The recommended order is to first establish the Global Copy, and then enable a FlashCopy volume for that Global Copy primary. The Global Copy secondary will not be in a fully consistent state until the Global Copy is forced to the full duplex state.
  - If you create the FlashCopy first and then enable a Global Copy of the FlashCopy target, you must monitor the progress of the FlashCopy background copy.
    - The Global Copy secondary will not be in a fully consistent state until the FlashCopy background copy process is complete and the Global Copy is forced to the full duplex state.
    - Use the copy option to ensure that the entire FlashCopy source volume data is copied to the Global Copy secondary.

At the secondary site of the Global Copy, a FlashCopy source volume can be based on the secondary Global Copy volume.

Global Mirror

FlashCopy in combination with Global Mirror supports only one type of relationship at the primary site: a FlashCopy source volume can become a Global Mirror primary volume and vice versa. The relationships can be established in any sequence. A FlashCopy target volume cannot become a Global Mirror primary volume.

On the Global Mirror secondary site, the Global Mirror target volume cannot be used as a FlashCopy source or target unless the Global Mirror pair is first suspended.

The measures taken by Data Protection for Snapshot Devices to permit this toleration are transparent to the user. Given a common scenario in which a production volume is both a PPRC primary and a FlashCopy source, the support is beneficial when a FlashCopy restore of the production volume is necessary. In previous versions of IBM Tivoli Storage Manager for Advanced Copy Services, the customer had to suspend the PPRC relationship, do the FlashCopy restore, then re-establish the PPRC relationship. This is no longer necessary because Data Protection for Snapshot Devices allows the FlashCopy target to be a PPRC primary.

Note:

1. This support applies only to devices interfaced to Data Protection for Snapshot Devices via a version of the CIM Agent for DS Open API that is 5.2 or higher. Refer to the hardware/software requirements page for specific release information.
2. Maintaining a PPRC relation from a FlashCopy target may have performance impacts on the FlashCopy background copy process in the storage subsystem, but Data Protection for Snapshot Devices performance will not be affected.

3. The SAN Volume Controller does not currently allow a FlashCopy target volume to be a Metro Mirror or Global Mirror primary. This restriction may be lifted in a future release.

Specific customization requirements

Tivoli Storage Manager for ERP requires specific customization tasks to be performed before installing Data Protection for Snapshot Devices.

When running
- Tivoli Storage Manager for ERP for backup and restore to and from Tivoli Storage Manager and for archiving/retrieving log files to/from Tivoli Storage Manager on the production system
- `tsm4acs` to request an offloaded tape backup on the backup system

it is strongly recommended to use
- a common profile directory ($HOME/acs), via NFS mount
- only *one* common Tivoli Storage Manager Client node name for database backups

Further customization requirements to consider are:
- The database software must also be installed on the backup server (same version and fix pack level as on the production system).
- (SAP) In the case of SAP, the home directory structure must correspond to that of the standard SAP installation.
- (DB2) Default directories used by `tsm4acs` will be

  ```
  <DB2 instance directory>/acs
  $HOME/acs
  ```

  $HOME/acs (or its subdirectories individually) must be NFS-exported to the backup system.
- (Oracle) Default directories used by `tsm4acs` will be

  ```
  $HOME/acs
  ```

  $HOME/acs (or its subdirectories individually) must be NFS-exported to the backup system.
- Ensure that within the db_disk category each `jfslog` LV with all its LPs is allocated non-striped on one OS disk (AIX physical volume) only.
- No other files or file systems from applications (other than the SAP application, if applicable) should be allocated on the disks of the `db_disk` category. Such an invalid allocation can create problems during the FlashCopy backup and within restore runs if planned for a disk-to-disk restore/recovery.
- (DB2) Ensure that the local database directory resides on the db_disk category disk volumes.
- (DB2) Ensure that the DB2 log directory resides on the db_log category disk volumes.

(DB2) Running `tsm4acs` on the backup and production systems requires that
- the user ID of the DB2 instance owner, and the user ID number
- the group ID of the DB2 instance owner group, and the group ID number

match on both systems.

(DB2) The following figure shows the relationships of the profiles of Data Protection for Snapshot Devices, Tivoli Storage Manager for ERP (when employed), and the Tivoli Storage Manager API for a two-system environment:

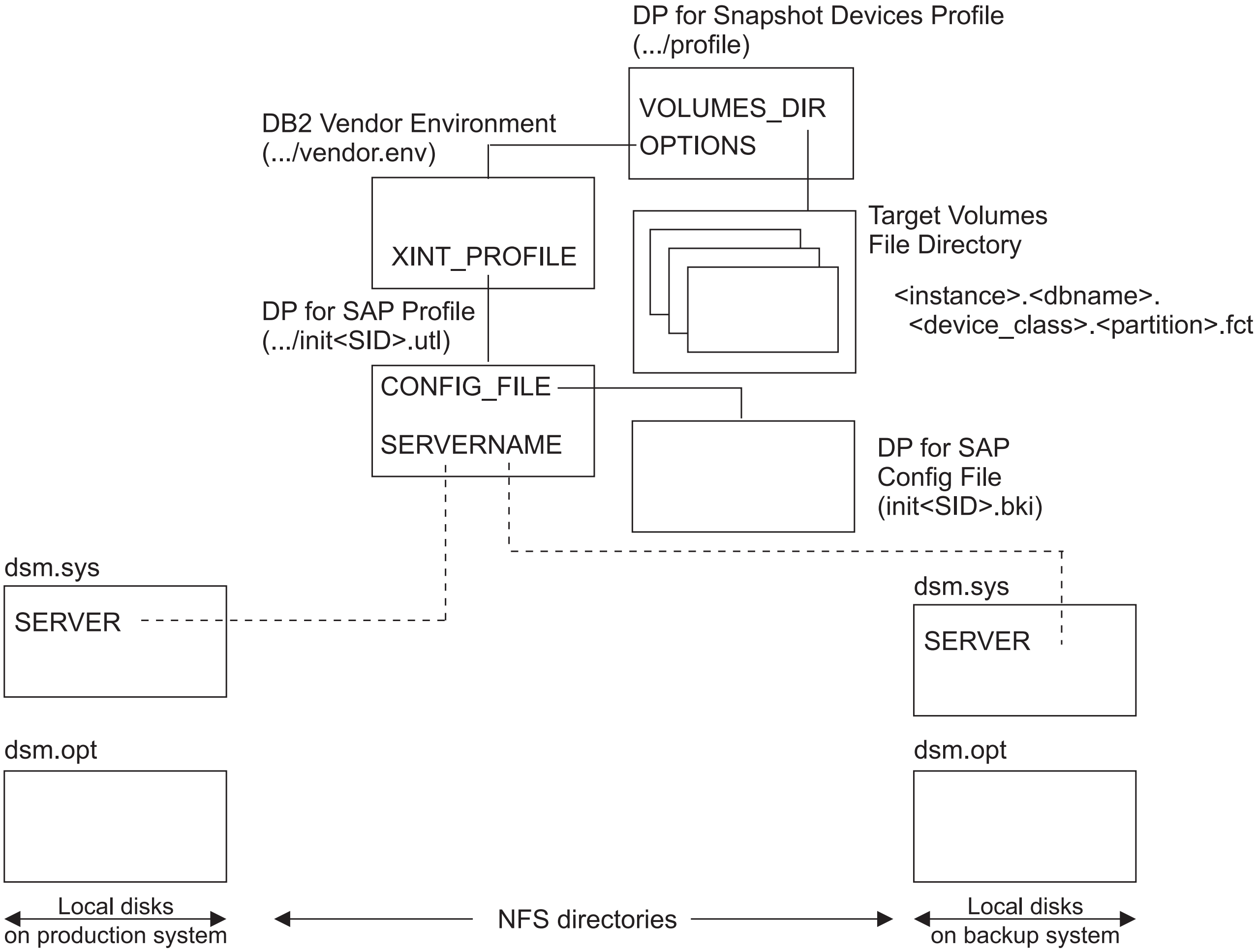


Figure 8. Configuration File Relationships With Data Protection for Snapshot Devices and DP for SAP (DB2)

Utilizing the storage system capabilities, such as FlashCopy for disk copy backups, with succeeding backups to external media (using Tivoli Storage Manager and Data Protection for Snapshot Devices), you involve a two-system environment (see Figure 8), in which the various configuration files and profiles contain information needed by both systems. The ideal setup is to have the Tivoli Storage Manager for ERP and Data Protection for Snapshot Devices profiles and configuration files set up on NFS disks, so that all DP tools (tsm4acs, the management and device agents, and the shared vendor library) use the same configuration files, regardless of the system the tool has been started on.

In addition, Tivoli Storage Manager for ERP and Data Protection for Snapshot Devices each use the same profiles, regardless of whether they were started on the production or backup system.

(SAP) Such a setup will allow the snapshot function of the storage system to be integrated transparently into Data Protection for Snapshot Devices and Tivoli Storage Manager for ERP in such a way that the database administrator can perform all the SAP database administrator tasks he is accustomed to doing, such as:

- administering a DB2 database on the production system

- initiating backups with Copy Services capabilities on the production system using Data Protection for Snapshot Devices and Tivoli Storage Manager for ERP, or backups without Copy Services capabilities on the production system with Data Protection for Snapshot Devices and with Tivoli Storage Manager for ERP.
- running and controlling backups/archiving of the log files on the production system
- restoring/recovering the database on the production system with Copy Services capabilities using Data Protection for Snapshot Devices snapshot restore, or restoring/recovering the database on the production system on the basis of the objects that were backed up to Tivoli Storage Manager

AIX raw logical volumes overview

Data Protection for Snapshot Devices supports operations on AIX raw logical volumes on Oracle.

Data Protection for Snapshot Devices for Oracle backs up and restores Oracle data files and control files that reside on raw logical volumes. This provides flexibility as all Oracle data files can reside on raw logical volumes only, or the Oracle data files can reside on both raw logical volumes and JFS or JFS2 file systems. However, when Oracle control files reside on raw logical volumes on the production server, the same raw logical volumes (with the same characteristics) must be created on the backup server. Use the `smitty` or `mklv` command to create the raw logical volumes, and then use the raw logical volumes to create the Oracle data files. Data Protection for Snapshot Devices does not support an environment that contains Oracle data files that were created using `/dev/hdisk#`. Since Data Protection for Snapshot Devices does not copy Oracle redo log files, these redo log files can reside on any volumes except for the volumes that contain the Oracle database files. When you create symbolic links to raw logical volumes on the production server, you must manually create the same symbolic links on the backup server. Raw logical volume support for Oracle is also available in LVM mirror environments.

AIX Journaled File Systems overview

Data Protection for Snapshot Devices supports operations on AIX JFS or JFS2 file systems.

Basic support for JFS2 requires that at least one JFS2 log logical volume must exist in each volume group that is set up with JFS2 file systems that will participate in a snapshot backup. The JFS2 file system is required for SAN-based N Series devices. In a DB2 environment, it is also required when using DB2 Advanced Copy Services without Data Protection for Snapshot Devices. Data Protection for Snapshot Devices JFS support is only on FlashCopy devices.

Logical volume name requirements

Data Protection for Snapshot Devices uses logical volume names for best results.

Use unique logical volume names (including the ones for the jfslog logical volumes) that reside on the source volumes and target volumes used in snapshot operations on the production system and backup system. Unique logical volume names help prevents having AIX rename the original logical volume name (when using non-concurrent volume groups) and AIX failure on encountering the duplicate logical volume name (when using enhanced concurrent capable volume groups).

Concurrent I/O setup requirements

Data Protection for Snapshot Devices propagates the concurrent I/O in the Enhanced Journaled File System (JFS2).

AIX 5L version 5.2 ML01 introduced the Concurrent I/O (CIO) feature in the Enhanced Journaled File System (JFS2), which allows the inode lock serialization on a file level. Database applications that implement their own data serialization mechanisms, usually at a finer level of granularity than the file, can now achieve performance throughput comparable to that obtained by using raw logical volumes. When properly set up, Data Protection for Snapshot Devices propagates the CIO of the JFS2.

In order to have the data files work properly with Data Protection for Snapshot Devices, make sure these requirements are met:

- AIX 5L version 5.3 and JFS2 file systems for the database
- The JFS2 file systems need the CIO option to be established at the file system or logical volume level. This can be accomplished by issuing this command:

  ```
  mkfs -o cio <fs name>
  ```

  Make sure that the `'cio'` option is defined in `/etc/filesystems` (check with command **lsfs**). Also check the logical volume control block (LVCB) of the file system using the command **getlvcb**:

  ```
  x1::root:/#getlvcb -AT fslv01
  AIX LVCB
  intrapolicy = m
  copies = 1
  interpolicy = m
  lvid = 0059d79a00004c00000000fb53c1c4d1.9
  lvname = fslv01
  label = /db2/C01/sapdata7
  machine id = 9D7AA4C00
  number lps = 13
  relocatable = y
  strict = y
  stripe width = 0
  stripe size in exponent = 0
  type = jfs2
  upperbound = 32
  fs = vfs=jfs2:log=/dev/loglv10:mount=true:options=cio,rw:account=false
  time created  = Wed Mar 10 13:50:33 2004
  time modified = Tue Aug 16 17:11:15 2005
  ```

Caution: Data Protection for Snapshot Devices does not support snapshot operations on a CIO setup if the CIO option is specified using the `mount` command on a file system level or on subdirectories of a file system. If this occurs, the CIO option is lost during a snapshot restore operation. In this situation, after a snapshot restore, you need to manually perform an unmount and issue the `mount` command (with the CIO option).

Network file system requirements for Network-Attached N Series devices

N Series devices must be defined to Data Protection for Snapshot Devices before performing a backup or restore operation on these devices.

Network attachment of N Series storage systems and use of NFS as the access protocol permits the following functions:

- volume-level snapshot backup
- volume-level snapshot restore
- snapshot deletion

Such N Series devices are defined to Data Protection for Snapshot Devices with the `COPYSERVICES_HARDWARE_TYPE NAS_NSERIES` parameter. The filer in this case exports data as files by NFS. NFS clients can mount resources (files, directories, or volumes) that have been exported by the filer.

```
root (/) at host workstation
- bin
- etc
- home
  - users
    - adam
    - joe
    - sally
      - old stuff
      - invoices
      - proposals
        - tranco
        - metasoft
     - zoe
  - users2
    - ming
    - daniela
    - dulcetta
    - tom
 - applications
   - solaris
     - staroffice
     - other
```

- The filer A NFS volume ′home′ is mounted at ′/home/users′ .
- The filer B NFS volume ′home′ is mounted at ′/home/users2′.
- The filer C NFS volume ′appl′ is mounted at ′/applications′.

Files in the directories are accessed by NFS and follow UNIX file semantics. By default, each filer volume contains a directory named ′.snapshot′, through which users can access old versions of files. Snapshot files carry the same read permission as the original file. Since snapshots are read-only, write permissions do not apply. NFS-accessed N Series devices can be managed by Data Protection for Snapshot Devices systems running either AIX or Linux for System x.

FlashCopy backup requirements for a SAN Volume Controller environment

A FlashCopy backup on SAN Volume Controller requires that several conditions be met before attempting a backup or restore operation.

The following characteristics, requirements, and restrictions apply to a FlashCopy with SAN Volume Controller:

- Volumes in the SAN Volume Controller are referred to as *virtual disks* (vDisks) and are addressed by a logical unit number (LUN). The virtual disks are defined by the user in the SAN Volume Controller master console Web GUI.
- FlashCopy occurs between a source virtual disk and a target virtual disk.
- The virtual disks must be the same size.
- A virtual disk is designated by a name which must be unique.
- The minimum granularity that SAN Volume Controller supports for FlashCopy is an entire virtual disk. A FlashCopy of part of a virtual disk is not supported.
- The source and target virtual disks must both be managed by the same SAN Volume Controller cluster.
- The source and target virtual disks are available (almost) immediately after the FlashCopy is initiated.
- After the start of the FlashCopy, the target volume and source volume might be updated independently.
- SAN Volume Controller FlashCopy associates a source virtual disk and a target virtual disk together in a FlashCopy mapping.
- Each virtual disk may be a member of only one FlashCopy mapping relationship, and a FlashCopy mapping relationship always has exactly one source virtual disk and one target virtual disk. Therefore, it is not possible for a virtual disk to simultaneously be the source for one FlashCopy mapping relationship and the target for another FlashCopy relationship.
- The sizes of vDisks that are members of a FlashCopy mapping cannot be changed while the mapping is in effect.
- An SAN Volume Controller supports the creation of enough FlashCopy mapping s to allow each virtual disk to be a member of a FlashCopy mapping relationship.
- Incremental FlashCopy is supported by Data Protection for Snapshot Devices in a SAN Volume Controller configuration starting with SAN Volume Controller version 4.2.1. This support is based on a single incremental relationship between a given pair of source and target volumes within one SVC cluster. In the case of LVM mirroring, the user can specify two sets of target volumes, one for each storage cluster involved.
- The SAN Volume Controller requires that SDD or SDDPCM be installed on all attached hosts.

Consistency groups

A snapshot backup from an SAN Volume Controller employs *consistency groups*. Consistency groups consider the issue of whether the application contains related data that spans multiple virtual disks. The *consistency group* feature reduces the time needed to verify the consistency of participating disks. In order to create a consistent image of the data, a Flash Copy operation on multiple virtual disks is performed as an atomic operation. A FlashCopy mapping is created between a source and target virtual disk. A FlashCopy mapping must be a member of a consistency group. A consistency group can contain an arbitrary number of Flash

Copy mappings, up to the maximum number supported by a SAN Volume Controller cluster. The SAN Volume Controller `'Start'` command causes the point-in-time copy to be directed to a consistency group. In this case, all of the mappings in the consistency group are started at the same time, resulting in a point-in-time copy that is consistent across all mappings in the group.

Hardware requirements

Data Protection for Snapshot Devices requires specific hardware to be available before it can be installed successfully.

The following table lists the basic hardware requirements. Refer to the requirements Web page for specific versions and further information.

Note: The numbers in parentheses refer to the notes following the table.

Table 25. Hardware Requirements Summary

	Database Storage System						**(PS)**	**Backup System (BS)**	**Takeover System (HACMP)**
	ESS 800	**DS6000/ DS8000**	**SVC**	**N Series (SAN)***9*	**N Series (NAS)***9*	**XIV®**			
Processor	IBM System p®				IBM System p or IBM System x	Machine Type 2810, Model A14	x	x	x
Storage system options	FC 1830-1835 (*7*)	2244-PTC (*7*)					x	x	x
Storage system microcode and LIC	(*8*)	(*8*)	(*8*)	Data ONTAP (*10*)		XIV® CLI version 2.3.1 to 2.3.x	x	x	x
Connection of processor to storage system (*1*)	SCSI or Fibre Channel adapters			Fibre Channel	NFS compatible technology	Fibre Channel	x	x	x
Disk space	250 MB (*3*)						x	x	x
Memory	256 MB (*4*)						x	x	x
LAN connection to:	CIM Agent for DS Open API		SVC master console	N Series filer		XIV® system	x	x	x
	NFS (PS to BS)						x	x	x
LAN or SAN connection to:	TSM Server						x (*2*)	x (*2*)	x
LVM mirrors (*6*)	Two mirror sets (if used)						x	x	x
HACMP (*5*)	x						x	x	x

Note:

1. Source volumes accessible to production system, target volumes accessible to backup system. Sources and targets must not be accessible to both systems simultaneously. Source and target volume pairs must have the same size and reside in the same hardware unit.

2. On the production system, to the Tivoli Storage Manager server for restore and backup/restore of log files. On the backup system, to the Tivoli Storage Manager server for backup, if the Tivoli Storage Manager server is not already installed on the backup system.
3. Applies to each Data Protection for Snapshot Devices version level installed. In order to avoid an uncontrolled termination of Data Protection for Snapshot Devices (or the called system commands) due to lack of space, Data Protection for Snapshot Devices issues a warning message (IDS1310W) if an essential file system has less than 50 MB free space. If the available space is less than 5 MB, Data Protection for Snapshot Devices terminates with an error message (IDS1311E); in this case, the affected file system first needs to be increased prior to rerunning Data Protection for Snapshot Devices.
4. (SAP) Check the SAP database server memory requirements, which normally are in the range 1-2 GB, depending on workload objectives.
5. Three IBM System p systems are required when planning for a high availability environment where a primary and takeover system with HACMP will become established with HACMP. Each needs to play the role of the production system depending on which is currently the active system. The takeover system for the production server cannot be the backup system. HACMP on network-attached storage (NAS) is not supported on Linux. Refer to the Release Notes for current information on support provided by AIX in this case. Refer to the Release Notes for current information on HACMP support provided by AIX on network-attached storage (NAS).
6. For details, see “Overview of Data Protection for Snapshot Devices support for AIX Logical Volume Manager mirrored environments” on page 48.
7. The FlashCopy LIC or the equivalent point-in-time copy (PTC) function is required. For the ESS, at least microcode V2 is required.
8. See the Hardware/Software Requirements Web page link in the Release Notes.
9. The N Series models currently available are the N3700, N5000, and N7000 series. Network attached (NAS) devices must be accessed using the NFS protocol. NAS is available only on N Series devices. Target sets do not apply in this case. A snapshot space with up to 100% reserve is required.
10. Operating system required on the N Series filer. FCP, Flexible Volume Clone, SnapRestore features activated.

    Note: There is an dependency between the Data ONTAP version and the ONTAPI software development kit (SDK) version used by Data Protection for Snapshot Devices. Messages referring to an insufficient ONTAPI level can indicate that Data ONTAP needs to be upgraded.

Related reference

“IBM Tivoli Storage Manager for Advanced Copy Services information sources” on page xv

Software requirements

Data Protection for Snapshot Devices requires specific software to be available before it can be installed successfully.

Note:

1. For the supported software levels of each component, up-to-date information, and further details, check the README information or refer to the Hardware/Software Requirements page, which is accessible via the Release Notes .
2. Unless otherwise stated, software required on both the production and backup systems must be installed and configured identically on each system.
3. The numbers in parentheses refer to the notes following the table.

Table 26. Software Requirements Summary

	Database Configuration			Database Storage System						Operating system			
Comp.	**DB2**	**SAP with Oracle**	**Native Oracle**	**ESS 800**	**DS6000 DS8000**	**SVC**	**N Series (SAN)**	**N Series (NAS)**	**XIV®**	**AIX**	**Linux**	**Prod system**	**Backup system**
Operating System													
AIX 5.3 (64-bit)	x	x	x	x						x		x	x
Linux on System x (64-bit)	x							x			x	x	x
Multipath Subsystem Device Driver (SDD) (12 on page 88)	x	x	x	x						x		x	x
Multipath Subsystem Device Driver Path Control Module (SDDPCM) (12 on page 88)	x	x	x	x						x		x	x
MPIO AIX native driver (12 on page 88) (17 on page 89)	x	x	x	x					x	x		x	x

Table 26. Software Requirements Summary (continued)

	Database Configuration			Database Storage System						Operating system			
Comp.	**DB2**	**SAP with Oracle**	**Native Oracle**	**ESS 800**	**DS6000 DS8000**	**SVC**	**N Series (SAN)**	**N Series (NAS)**	**XIV®**	**AIX**	**Linux**	**Prod system**	**Backup system**
FCP Host Attachment Kit	x	x	x				x			x		x	x
Locale	x	x	x	en_US.ISO8859-1 (3 on page 88)						x	x	x	x
JFS	x	x	x	x (13 on page 88)					x	x		x	x
JFS2 with freeze/ thaw function	x	x	x	x (13 on page 88)			x		x	x		x	x
NFS	x	x	x	x						x	x	x	x
libgcc (15 on page 89)	x	x	x				x			x	x	x	x
Open SSL (4 on page 88)	x	x	x										
Tivoli Storage Manager (TSM) (5 on page 88)													
TSM Server	x	x	x	x									x
TSM Backup/ Archive Client	x	x	x	x						x	x	x	x
TSM API	x	x	x	x						x	x	x	x

Table 26. Software Requirements Summary (continued)

	Database Configuration			Database Storage System						Operating system			
Comp.	**DB2**	**SAP with Oracle**	**Native Oracle**	**ESS 800**	**DS6000 DS8000**	**SVC**	**N Series (SAN)**	**N Series (NAS)**	**XIV®**	**AIX**	**Linux**	**Prod system**	**Backup system**
Tivoli Storage Manager for Enterprise Resource Planning (8 on page 88)	x	x		x						x	x	x	x
Data Protection for Snapshot Devices	x	x	x	x						x	x	x	x
Data Protection for Oracle (18)			x	x									
Database Software													
SAP (6 on page 88)	x	x		x						x	x	x	
BR*Tools		x		x						x		x	x
Oracle		x	x	x						x		x	x
DB2 Enterprise (64-bit) (13 on page 88)	x			x						x	x	x	x

Table 26. Software Requirements Summary (continued)

Comp.	Database Configuration			Database Storage System						Operating system		Prod system	Backup system
	DB2	SAP with Oracle	Native Oracle	ESS 800	DS6000 DS8000	SVC	N Series (SAN)	N Series (NAS)	XIV®	AIX	Linux		
DB2 Advanced Copy Services	x			x						x	x	x	x
Storage System Interface													
ESS Copy Services Command-Line Interface (CLI) (7 on page 88)	x	x	x	x									
CIM Agent for DS Open API (10 on page 88)	x	x	x	x						x		(9 on page 88)	(9 on page 88)
CIM Agent for SVC (11 on page 88)	x	x	x			x							
CIM Server Runtime Env. (Pegasus) (1 on page 88)	x	x	x	x						x		x	x

Table 26. Software Requirements Summary (continued)

Comp.	Database Configuration			Database Storage System						Operating system		Prod system	Backup system
	DB2	SAP with Oracle	Native Oracle	ESS 800	DS6000 DS8000	SVC	N Series (SAN)	N Series (NAS)	XIV®	AIX	Linux		
CIM Server Base Providers for AIX (Pegasus)	x	x	x	x						x		x	x

Note:

1. FC 0949 (AIX 5.2), FC 0968 (AIX 5.3). From the AIX Expansion Pack CD (not part of the Data Protection for Snapshot Devices package). Consisting of:
   - sysmgt.pegasus.cimserver.rte
   - sysmgt.pegasus.osbaseproviders

   Only the client libraries are used in a Data Protection for Snapshot Devices environment. Therefore, the term *CIM Client* is used instead of *CIM Server* to refer to the software following installation.
2. See the README information and/or the requirements Web page link in the Release Notes for current maintenance level and PTF information. Virtual I/O is not supported.
3. Verify with `locale –a` .
4. For AIX, Open SSL is available on the ″AIX Toolbox for Linux Applications for POWER® Systems″ CD. For CIM devices, installation is required by the Pegasus package, even if non-SSL mode is to be configured. See "Installing Open SSL" on page 96 for additional information..
5. The Tivoli Storage Manager server, backup/archive client, and API are required for offloaded tape backup (both SAP and non-SAP environments). In addition, in an SAP environment after a snapshot backup, BR*Tools perform two additional runs to save the database control files and other files important for recovery. This is done via TSM for ERP and is a file backup to the TSM Server.
6. (SAP) SAP on production system (with SAP-approved DB2 version). Data Protection for Snapshot Devices is required for the Tivoli Storage Manager interface.
7. **For ESS 800 only**: IBM 2105 ESS Storage Management CLI and Copy Services CLI for AIX. The code level must correspond to that of the microcode installed in the ESS clusters. See "Hardware requirements" on page 80. Installation required only on the machine hosting the CIM Agent for DS Open API. Must be installed prior to installing the CIM Agent.
8. (SAP) Required for interface to Tivoli Storage Manager. Corresponding to OS level and DB2 level (64-bit).
9. Installable on any supported host accessible to both systems[8]. Installation on the PS is not recommended, due to the load imposed by Java™ on the CIMOM component. Production systems normally host only the DBMS and application server. User ID required for Data Protection for Snapshot Devices access.
10. Includes DS Open API, ESS NI Client, CIMOM, SLP. User ID required for Data Protection for Snapshot Devices access. Installable on any host accessible to PS or BS. Installation on the PS is not recommended due to the loading imposed by Java on the CIMOM.
11. Installed as part of SAN Volume Controller. User ID required to allow access by Data Protection for Snapshot Devices.
12. See *Support Matrix for the Subsystem Device Driver, Subsystem Device Driver Path Control Module, and Subsystem Device Driver Device Specific Module*.
13. The database must reside on a Journaled File System (JFS or JFS2), or be accessible via NFS (N Series). JFS is supported for FlashCopy devices only and, in a DB2 environment, only by Data Protection for Snapshot Devices and not DB2 Advanced Copy Services..
14. Only NAS/NFS-attached N Series devices supported. Required by Linux.

---

[8] This has been tested on AIX only.

15. For databases residing on N Series devices, Data Protection for Snapshot Devices requires the GCC Compiler Dynamic Runtime Library (libgcc). Refer to the hardware/software requirements Web page (see the link in the Release Notes) for information on obtaining this package. On Linux systems, this library is preinstalled. It must be installed manually on an AIX system. In this case, a symbolic link (`/usr/lib/libgcc_s.a`) is required that points to the libgcc installation directory:

    ```
    ln -s <full pathname of gcc library> /usr/lib/libgcc_s.a
    ```

16. (DB2) DB2 Advanced Copy Services is part of the DB2 High Availability Feature, which is provided with DB2 9 (starting with V9.5) as a standard component of DB2 Enterprise. It is a functional subset of Data Protection for Snapshot Devices. Data Protection for Snapshot Devices requires that DB2 Advanced Copy Services have been previously installed and enabled, so that installation of Data Protection for Snapshot Devices represents a DB2 Advanced Copy Services upgrade.
17. Required only for SDDPCM.
18. Required on the production and backup systems if offloaded tape backup to Tivoli Storage Manager is needed.

Environment requirements

Data Protection for Snapshot Devices requires specific environment conditions to exist before it can be installed successfully.

Data Protection for Snapshot Devices requires that certain conditions concerning the overall system environment be satisfied before Data Protection for Snapshot Devices can be installed:

- Certain directories on the production system must be made available via NFS to the backup system (see “Mounting shared directories via NFS” on page 116).
- The database files needed for backup reside completely on the storage subsystem and are visible to the production machine.
- (DB2) All DB2 tablespaces must be database-managed tablespaces (DMS). All user/system temporary tablespaces such as PSAPTEMP can be system- managed tablespaces.
- (DB2) The database must be in log-retain mode.
- (DB2) The ulimits of the ’db2<sid>’ user and ’root’ on the production and backup systems should be at least the following (check with **ulimit –a**):

  ```
  data seg size (kbytes)     unlimited
  max memory size (kbytes)   131000
  stack size (kbytes)        131000
  ```

  Depending on the user’s shell and OS level, the output of **ulimit –a** can vary.

Volume group requirements

Data Protection for Snapshot Devices requires specific volume group settings to be available before it can be installed successfully.

Refer to the hardware and software requirements in the Release Notes for current information.

Logical Volume Manager mirroring requirements

Data Protection for Snapshot Devices requires specific Logical Volume Mirroring (LVM) settings to be available before it can be installed successfully.

See "Overview of Data Protection for Snapshot Devices support for AIX Logical Volume Manager mirrored environments" on page 48 and the hardware and software requirements Web page in the Release Notes for current information.

Recommended installation order

Installing Data Protection for Snapshot Devices in a specific order assists in completing all installation tasks successfully.

It is recommended that the products be installed and customized in the following sequence:

1. CIM (DS, ESS, and SAN Volume Controller only)
2. SDD, SDDPCM, and MPIO (as applicable), if multipath I/O is employed. These components should be installed as early as possible.
3. (DB2) DB2 on the production and backup servers. The DB2 Advanced Copy Services files are installed by default but DB2 Advanced Copy Services must be subsequently configured and enabled prior to installing and using Data Protection for Snapshot Devices. For FlashCopy devices, make sure the source volumes to be used for the database on the production system and the target volumes to be used later for a snapshot backup request are identified. (DB2) For N Series devices, DB2 Advanced Copy Services determines the source volumes from DB2 and allocates target volumes accordingly.
4. (Oracle) Oracle Server on the production and backup servers.
5. (SAP) SAP NetWeaver® or another SAP e-business solution on the production system.
6. (TSM Server) Tivoli Storage Manager products (if offload backup to Tivoli Storage Manager is to be employed):
   - Tivoli Storage Manager server on the backup system (might not apply if already available or on a different host)
   - Tivoli Storage Manager Backup-Archive client and the Tivoli Storage Manager API on the production and backup systems. For information regarding installation procedures for these software applications, see *Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients Installation and User's Guide*.
7. Export as NFS

   ```
   $HOME/acs
   ```

   or its three subdirectories individually

   ```
   $HOME/acs/share
   $HOME/acs/acsvolumes
   $HOME/acs/acsrepository
   ```

on the production system for access by the backup system (see "Mounting shared directories via NFS" on page 116).

8. (SAP) Install and customize Tivoli Storage Manager for ERP on the production and backup systems.

   (DB2) When installing Tivoli Storage Manager for ERP, you must define the Tivoli Storage Manager for ERP DB2 vendor options file (vendor.env) in the OPTIONS parameter of the Data Protection for Snapshot Devices profile (OFFLOAD section).

   Tivoli Storage Manager for ERP downward compatibility: In order to allow the restore of data on the production system that was backed up on a different system (in the case of Data Protection for Snapshot Devices, on the backup system), the downward compatibility of Tivoli Storage Manager for ERP must be strictly observed. In general, Tivoli Storage Manager for ERP has downward restore compatibility unless otherwise stated in the product.

   If possible, keep the Tivoli Storage Manager for ERP levels the same on both systems. Never have the backup system running a higher level than on the production system.
9. Install Data Protection for Snapshot Devices and perform additional customization steps, such as creating the target volumes set file (*.fct) if using FlashCopy devices (see "Data Protection for Snapshot Devices Target Volumes File (.fct)" on page 189).

Installing Data Protection for Snapshot Devices

This section provides information about installing Data Protection for Snapshot Devices

(DB2) It is assumed that DB2 Advanced Copy Services is already installed so that the installation process represents an upgrade.

For current information concerning installation of Data Protection for Snapshot Devices, refer to the **README** and Release Notes information shipped with the product installation media or files.

Data Protection for Snapshot Devices installation procedure

Data Protection for Snapshot Devices must be installed as described in this procedure in order to successfully perform backup and restore operations.

Installation and Activation: These phases install the components and transfer them to the respective database instances as specified by the user. No configuration or customization is performed.

1. (DB2) Ensure that DB2 ACS has been installed and enabled on the respective instances. Refer to the DB2 documentation for the High Availability feature.
2. Log in as user ID **root** on the production (or backup) system.
3. The Data Protection for Snapshot Devices installation packages are delivered on an installation disc, or an image thereof downloaded from Passport Advantage, as individual executable files with the following name format:

   ```
   <version>-TIV-TSMACS-<OS-platform>  Data Protection for Snapshot Devices
   ```

   The package files have the appropriate extension and are executable. Refer to the README.1ST file on the installation disc for information on the directory structure.

You can also download an install package for upgrading via the TSM for ACS Web site (Web-based install packages reside on the IBM public FTP server and the package names contain ″FTP″).

To install from the installation disc, ensure that it is inserted in the proper drive.

4. If you want to install in graphic mode, ensure that the environment variable DISPLAY is set to `host:display`, where `host` identifies the host name of the X Server to contact and `display` is the display number.
5. Invoke the executable file and follow the InstallAnywhere instructions.

   All the necessary components of Data Protection for Snapshot Devices software are copied to a global installation directory that allows for concurrent installation of multiple product versions:

   ```
   /usr/tivoli/tsm/acs_<TSM ACS version> (AIX)
   /opt/tivoli/tsm/acs_<TSM ACS version> (Linux)
   ```

   This directory contains the Data Protection for Snapshot Devices executable files, which are accessed by the setup script.

   (DB2) The installer copies tsm4acs and the device agents to the DB2 INST_DIR directory (see the activation step).

   ```
   <DB2 instance directory>/sqllib/acs
   ```

   for each selected instance.

   For the device agent executable files, the installer changes the owner to root:<sysadm> and sets the s-bit (chmod 4750).
6. Check the summary issued by InstallAnywhere for successful installation. If an error occurs during the installation process, check the error messages in the output carefully and correct the problems. After correcting the errors repeat the installation procedure.
7. (Optional) Activate Data Protection for Snapshot Devices for one or more systems (maximum of one system for SAP and Oracle, multiple systems for DB2) by invoking the following;

   ```
   setup_<database>.sh –a install –d <INST_DIR> -u <user> -g <group>
   ```

   This step is implemented such that it upgrades Data Protection for Snapshot Devices for systems that were previously activated. For systems that Data Protection for Snapshot Devices has not yet activated, the activation step simply deploys all binary files for subsequent configuration.

In the activation step, the following functions are performed:

1. Get input parameters acsd-hostname and acsd-port (unless console mode was selected)
2. Check if acsd and one or more device agents already exist on acsd-hostname
3. Create an entry for acsd-port in /etc/services (if an entry does not already exist)
4. Create two entries in /etc/inittab to start acsd and acscim/acsnsan/acsnnas/acsxiv.
5. Check if acsd and the device agent are able to start. These employ only the default profile at this time.

Related tasks

"Installing Data Protection for Snapshot Devices in silent mode"
Describes how to install in console (non-graphic) mode, possibly for a silent or unattended installation.

Chapter 4, "Configuring Data Protection for Snapshot Devices," on page 103
Instructions regarding how to run the setup script manually. For DB2, this procedure must be performed on each applicable DB2 instance.

Installing Data Protection for Snapshot Devices in silent mode

You can perform the installation and distribution phases of the Data Protection for Snapshot Devices installation task in the non-graphic console mode. You can also use a response file for silent (or unattended) installation.

1. To install in silent (unattended) mode, first create the response (properties) file, such as `installer.properties`, containing the following variables:
   a. The installation directory:
      ```
      USER_INSTALL_DIR=<installation directory>
      ```
      where <installation directory> has the value:
      - (Linux) `/opt/tivoli/tsm/acs_<version>`
      - (AIX) `/usr/tivoli/tsm/acs_<version>`

      and `<version>` has the format `6.1.0.0`, for example.
   b. To create a log file during installation, set the variable
      ```
      INSTALL_LOG_DESTINATION=<installation directory>/<log file name>
      ```
   c. `LICENSE_ACCEPTED=TRUE`
   d. To define the product database component that will be installed, set the following variable:
      ```
      CHOSEN_INSTALL_SET=<InstallSet>

      where <InstallSet> is
      TSMACSORA (Oracle component)
      TSMACSSAP (SAP with Oracle component)
      TSMACSDB2 (DB2 component)
      ```
   e. (Oracle and SAP Oracle) To set the home folder of the Oracle <SID>, use the following variable:
      ```
      ORACLE_HOME_FOLDER=/oracle/<SID>
      ```
   f. (DB2) For a DB2 installation: To copy the required files directly to desired IBM DB2 instances after installing in the main installation directory, set the following variable with a comma-separated list of existing IBM DB2 instances:
      ```
      DB2_INSTANCES_SELECTED=db2inst1,db2inst2
      ```
      If you do not want to copy the files, leave this variable blank:
      ```
      DB2_INSTANCES_SELECTED=
      ```
2. Invoke the executable file with the ″-i silent″ option (silent mode) and the ″-f″ option if a properties file was generated:
   ```
   ./<version>-TIV-TSMACS–<OS-platform>.bin -i silent [-f <properties file>]
   ```
   The `<properties file>` specification must contain a full path.

Sample properties file (DB2):

```
# Properties file for Tivoli Storage Manager for Advanced Copy Services Installations
# Created on: Dec 8, 2008 5:53:17 PM
# This file contains the information, the installer needs to perform a successful installation in silent mode.
#
# Properties recorded:

# Has the license been accepted
# -----------------------------
LICENSE_ACCEPTED=TRUE

# The chosen Install Set
# -----------------------------
CHOSEN_INSTALL_SET=TSMACSDB2

# Installation Directory
# ----------------------
USER_INSTALL_DIR=/usr/tivoli/tsm/acs_6.1.0.0

# ORACLE_HOME Directory
# ---------------------
# ORACLE_HOME_FOLDER=/oracle

# Selected IBM DB2 Instances
# --------------------------
# Specify a comma separated list of existing IBM DB2 instances,
# e.g. DB2_INSTANCES_SELECTED=db2inst1,db2inst2
# During the installation all files from install directory will be copied to
# the home directory of IBM DB2 instance(s) (<instance home>/sqllib/acs)
# If you do not want to copy the files, leave it blank.
DB2_INSTANCES_SELECTED=db2inst1,db2inst2
```

Sample properties file (Oracle):

```
# Properties file for Tivoli Storage Manager for Advanced Copy Services Installations
# Created on: Dec 8, 2008 4:47:36 PM
# This file contains the information, the installer needs to perform a successful installation in silent mode.
#
# Properties recorded:

# Has the license been accepted
# -----------------------------
LICENSE_ACCEPTED=TRUE

# The chosen Install Set
# -----------------------------
CHOSEN_INSTALL_SET=TSMACSORA

# Installation Directory
# ----------------------
USER_INSTALL_DIR=/usr/tivoli/tsm/acs_6.1.0.0

# ORACLE_HOME Directory
# ---------------------
ORACLE_HOME_FOLDER=/oracle/SID

# Selected IBM DB2 Instances
# --------------------------
# Specify a comma separated list of existing IBM DB2 instances,
# e.g. DB2_INSTANCES_SELECTED=db2inst1,db2inst2
# During the installation all files from install directory will be copied to
# the home directory of IBM DB2 instance(s) (<instance home>/sqllib/acs)
# If you do not want to copy the files, leave it blank.
DB2_INSTANCES_SELECTED=
```

Sample properties file for SAP with Oracle:

```
# Properties file for Tivoli Storage Manager for Advanced Copy Services Installations
# Created on: Dec 8, 2008 5:47:59 PM
# This file contains the information, the installer needs to perform a successful installation in silent mode.
#
# Properties recorded:

# Has the license been accepted
# -----------------------------
LICENSE_ACCEPTED=TRUE

# The chosen Install Set
# -----------------------------
CHOSEN_INSTALL_SET=TSMACSSAP

# Installation Directory
# ----------------------
USER_INSTALL_DIR=/usr/tivoli/tsm/acs_6.1.0.0

# ORACLE_HOME Directory
# ---------------------
ORACLE_HOME_FOLDER=/oracle/SID

# Selected IBM DB2 Instances
# --------------------------
# Specify a comma separated list of existing IBM DB2 instances,
# e.g. DB2_INSTANCES_SELECTED=db2inst1,db2inst2
# During the installation all files from install directory will be copied to
# the home directory of IBM DB2 instance(s) (<instance home>/sqllib/acs)
# If you do not want to copy the files, leave it blank.
DB2_INSTANCES_SELECTED=
```

Lines starting with "#" are treated as comments.

You can also generate a properties file during installation (in either graphic or console mode) by invoking the executable file as follows:

```
./<version>-TIV-TSMACS–<platform>.bin [-i console]
-DRECORDFILE=/tmp/installer.properties
```

Configuring a new DB2 instance

Use this procedure to configure a DB2 instance when it has been added after initial Data Protection for Snapshot Devices installation.

1. Log on as root.
2. Enter this command:

   ```
   cd /opt/tivoli/tsm/<version>
   setup_db2.sh -a install -d <DB2 instance directory> [-F]
   ```

   The version to be installed must be newer than the currently installed version. The -F option forces any existing version to be overwritten.
3. To set up the new instance, run the setup script from the DB2 instance directory as the DB2 instance owner.

Related tasks

Chapter 4, “Configuring Data Protection for Snapshot Devices,” on page 103
Instructions regarding how to run the setup script manually. For DB2, this procedure must be performed on each applicable instance.

Installing Open SSL

The Open SSL (Secure Sockets Layer) rpm file must be installed in order for the CIM Client to operate successfully.

AIX: In order for the CIM Client to operate successfully (even if Data Protection for Snapshot Devices will run in non-SSL mode), the OpenSSL rpm file must be installed. Issue the following commands to determine if the CIM Client exists on your system:

```
rpm -q -f /opt/freeware/lib/libssl.a
rpm -qa | grep -i openssl
```

If both the libssl.a library and openssl-<version><buildlevel>.rpm are found, OpenSSL is currently installed on your system. If OpenSSL is not installed, the rpm file is available on the AIX Linux ToolBox CD or downloadable from the AIX Toolbox for Linux Applications Web site:

`http://www.ibm.com/servers/aix/products/aixos/linux/download.html`

Select AIX Toolbox Cryptographic Content under the Sorted Download heading on the right of the page. After you have registered and accepted the license, you can download ″openssl - Secure Sockets Layer and cryptography libraries and tools″, such as openssl-0.9.7k-1.aix4.3.ppc.rpm, or a later supported version. Issue the following command to install the OpenSSL rpm file:

```
rpm -ivh openssl-<version><buildlevel>.rpm
```

SUSE Linux Enterprise Server (SLES 10): Install the package

`compat-openssl<version>-32bit`

if it is missing from the operating system installation media.

Red Hat Enterprise Linux 4 and 5 : Install the `openssl<version` package if it is missing from the operating system installation media.

1. Issue the following command as the root user:
   ```
   cd /lib
   ```
2. Check that the `libssl.so.<version>` and `libcrypto.so.<version>` files exist.
3. Create soft links as shown in this example for version 0.9.7::
   ```
   ln -s libssl.so.0.9.7a libssl.so.0.9.7
   ln -s libcrypto.so.0.9.7.a libcrypto.so.0.9.7
   ```

Related concepts

"Installing the Pegasus CIM Server package" on page 98
The Pegasus CIM Server package includes the client libraries that are required by Data Protection for Snapshot Devices.

Installing the Common Information Model (CIM) components and related software

The CIM components must be installed in order for the CIM interface to function properly.

The following applications are not provided with the Data Protection for Snapshot Devices packages and must be obtained separately:

- Open SSL
- Pegasus CIM Server package
- CIM Agent for DS Open API (ESS or DS configuration)

- ESS Copy Services CLI (ESS configuration)

The CIM Agent for SAN Volume Controller is automatically installed and integrated with the SAN Volume Controller master console.

Configuring the CIM environment for SSL communication

The Data Protection for Snapshot Devices COPYSERVICES_COMMPROTOCOL and COPYSERVICES_CERTIFICATEFILE profile parameters must specify correct values for Secure Sockets Layer (SSL) communication.

By default, the CIM Agent for DS8000, which is preinstalled on the HMC, requires communication in secure mode. In this case, clients such as Data Protection for Snapshot Devices need to connect using HTTPS instead of HTTP. This requires that the CIM Client must first obtain the public key used for encryption from the 'truststore' certificate in the CIM Agent and then authenticate using the user name and password.

To enable the HTTPS protocol, the Data Protection for Snapshot Devices profile parameter COPYSERVICES_COMMPROTOCOL must specify HTTPS (default value). In this case, parameter COPYSERVICES_CERTIFICATEFILE can define a certificate file name, and Data Protection for Snapshot Devices exports the certificate using this file.

The CIM Agent also provides another communication mode known as *null trust provider*. In this case, the CIM Agent does not verify that the certificate passed by the client matches a known certificate. Rather, it accepts any certificate from the client, including a null string for the filename. To enable this mode, the value of COPYSERVICES_CERTIFICATEFILE must be NO_CERTIFICATE. This mode is recommended only if the production and backup systems, as well as the storage system, are protected by a firewall. If NO_CERTIFICATE is in effect, the cimom.properties parameter `DigestAuthentication` must be set to 'false'.

Related concepts

"Installing the Pegasus CIM Server package" on page 98
The Pegasus CIM Server package includes the client libraries that are required by Data Protection for Snapshot Devices.

Generating a new CIM certificate

A new CIM certificate can be generated if it is suspected that security is comprised.

Use the procedure that applies to your version of the CIM Agent:

- **CIM Agent Version 5.1:**
  1. Change to the CIM Agent installation directory (typically `/opt/IBM/cimagent`)
  2. Run the **mkcertificate** command. This command creates an X.509 certificate and places it in a certificate store entitled 'truststore'.
- **CIM Agent Version 5.2:**
  1. Change to the CIM Agent installation (typically `/opt/IBM/cimagent`)
  2. The **dscimcii** command is used to view and modify the configuration of the CIM Agent.
  3. The following subcommands for SSL Certificate Management are provided by **dscimcii**:
     - **lscert**: List the current SSL certificate
     - **mkcert**: Create a new SSL certificate
     - **rmcert**: Remove the current SSL certificate

  - **getcert**: Obtain the current SSL certificate from the CIM Agent in ASCII form.
- **SAN Volume Controller (V4.2.1 or higher)**

  The procedure is illustrated for a Windows environment:

  1. Make sure that the CIM Agent Service (IBM System Storage SAN Volume Controller Pegasus Server) is stopped.
  2. From a DOS prompt, go to the svcconsole\cimom\config directory and run

     ```
     envConf.bat
     ```

     to set the environment.
  3. Enter the command

     ```
     mkcertificate ssl
     ```
  4. Run the following commands:

     ```
     cimconfig -s sslCertificateFilePath="%SVCAGENT_HOME%\certificate\ssl.cert" -p
     cimconfig -s sslKeyFilePath="%SVCAGENT_HOME%\certificate\ssl.key" -p
     ```

     This SSL certificate is valid for 365 days by default.
- Start up the CIM Agent Service. If you still cannot start the cimserver, check the `svcconsole\cimom\pegasus\cimserver_planned.conf` file and verify that the SSL parameters are correct.
- Copy the `c:\program files\svcconsole\cimom\certificate\ssl.cert` file to `/oracle/SID/102_64/dbs/ssl.cert` on the appropriate Oracle SAP server system
- Update the COPYSERVICES_CERTIFICATEFILE parameter in the Data Protection for Snapshot Devices profile.

Installing the Pegasus CIM Server package

The Pegasus CIM Server package includes the client libraries that are required by Data Protection for Snapshot Devices.

In addition to a server component that is installed (but not used by Data Protection for Snapshot Devices), the Pegasus CIM Server package includes the client libraries that Data Protection for Snapshot Devices needs to interface to the CIM agent for the respective storage system. The client libraries are referred to in the Data Protection for Snapshot Devices environment as the *CIM Client*. The Pegasus package must be installed on each AIX server on which Data Protection for Snapshot Devices is installed. The CIM Client requires the libssl.a library component of Open SSL ("Installing Open SSL" on page 96.

Related tasks

"Installing Open SSL" on page 96
The Open SSL (Secure Sockets Layer) rpm file must be installed in order for the CIM Client to operate successfully.

Installing the OpenPegasus package:

The AIX Expansion Pack contains the OpenPegasus components that are required by Data Protection for Snapshot Devices.

Refer to the README file for the most current information regarding the Pegasus CIM Server.

The AIX Expansion Pack contains the OpenPegasus components. To obtain the AIX Expansion Pack, place an order on the 5692-A5L SPO in the configurator for feature 0968 (AIX 5.3 Expansion Pack) A valid AIX software maintenance agreement (SWMA) is required. They can also be downloaded from the IBM Director Web page. After registering, follow the link for IBM Director for AIX and Linux on POWER.

The following packages are available for Pegasus:

sysmgt.pegasus.cimserver.rte (Pegasus CIM Server Runtime)
Installs the Pegasus CIM Server filesets in the `/opt/freeware/cimom/pegasus` directory

sysmgt.pegasus.osbaseproviders (Base Providers for AIX OS)
Installs the base providers for AIX filesets in the `/usr/pegasus/provider` directory

These packages can be installed using either the System Management Interface Tool (SMIT) or the installp command.

To verify that the CIM Client fileset was installed correctly, use the `lslpp` command as follows:

```
lslpp -al sysmgt.pegasus.cimserver.rte
```

If the installation completed successfully, a message similar to the following is returned:

```
lslpp -l sysmgt.pegasus.cimserver.rte
Fileset                                              Level   State      Description
----------------------------------------------------------------------------
Path: /usr/lib/objrepos sysmgt.pegasus.cimserver.rte 2.5.1.0 COMMITTED \ Pegasus CIM Server Runtime Environment
```

If the installation was not successful, a message similar to the following is returned:

```
lslpp: Fileset sysmgt.pegasus.cimserver.rte not installed.
```

To verify that the Base Providers for AIX fileset was installed correctly, use the `lslpp` command as follows:

```
lslpp -al sysmgt.pegasus.osbaseproviders
```

If the installation completed successfully, a message similar to the following is returned:

```
lslpp -l sysmgt.pegasus.osbaseproviders
Fileset                                                Level   State      Description
----------------------------------------------------------------------------
Path: /usr/lib/objrepos sysmgt.pegasus.osbaseproviders 1.2.6.0 COMMITTED \ Base Providers for AIX OS
```

If the installation did not complete successfully, a message similar to the following is returned:

```
lslpp: Fileset sysmgt.pegasus.osbaseproviders not installed.
```

Installing the CIM Agent for DS Open API

Install the CIM Agent for DS Open API on a system with access to both the production and backup systems through HTTP or HTTPS when using an ESS or DS storage system.

Refer to the *IBM TotalStorage DS Open Application Programming Interface Reference* for the installation procedure. This publication also contains the procedure for configuring the agent to run in non-SSL mode.

The CIM Agent for DS Open API can be co-located with the CIM Client. In this case, installation on the backup system is recommended. The CD image for the CIM Agent for DS Open API, as well as updates and other information, can be obtained online. The CIM Agent for DS Open API requires the *prior* installation of the ESS Copy Services Command Line Interface (CLI) if an ESS 800 storage system is configured. The functions of this package for a DS storage system are performed by the ESS Network Interface (NI).

Installing the CIM Agent for SAN Volume Controller

The CIM Agent for SAN Volume Controller is installed as part of the SAN Volume Controller master console environment.

Configuring the Common Interface Model Agent for SAN Volume Controller:

The Data Protection for Snapshot Devices COPYSERVICES_CERTIFICATEFILE profile parameter must specify correct values for use with the SAN Volume Controller.

By default, the CIM Agent for SAN Volume Controller runs in secure mode using the HTTPS protocol. To generate an SSL certificate, refer to “Generating a new CIM certificate” on page 97. If NO_CERTIFICATE is used, the parameter `DigestAuthentication` in the cimom.properties file must be set to ’false’.

Related tasks

“Installing Open SSL” on page 96
The Open SSL (Secure Sockets Layer) rpm file must be installed in order for the CIM Client to operate successfully.

Uninstalling Data Protection for Snapshot Devices

Uninstall Data Protection for Snapshot Devices as described in this procedure.

Perform the following steps to uninstall Data Protection for Snapshot Devices version 5.5 (or later):

1. Log in as the root user.
2. The uninstall procedure can be run in graphic or silent mode. Graphic mode requires a graphical X Window installation. Ensure that the environment variable DISPLAY is set to host:display, where ’host’ identifies the host name of the X Server to be contacted and ’display’ is the display number.
3. When in graphic mode, issue this command:

```
<installation path>/_uninst/uninstaller.bin (V5.5)
<installation path>/uninstall/uninstaller.bin (V6.1 or higher)
```

where `<installation path>` is

```
/usr/tivoli/tsm/acs_<version>  (AIX)
/opt/tivoli/tsm/acs_<version>  (Linux)
```

and follow the instructions provided in the dialog.

4. To uninstall in silent mode, issue this command:

```
<installation path>/uninstall/uninstaller.bin -i silent
```

Restoring backups from previous versions of DP for Snapshot Devices

- Backups taken with SVC 4.2.0 can be restored in a TSM for ACS V6.1 environment using SVC 4.2.1. However, it is recommended that a backup be taken immediately after installing TSM for ACS V6.1 in an SVC 4.2.1 environment or upgrading to SVC 4.2.1 after installing TSM for ACS V6.1.
- (Oracle) Any snapshot backup in existence when upgrading to DP for Snapshot Devices V6.1 must be withdrawn prior to the upgrade. This backup can no longer be restored using DP for Snapshot Devices V6.1. It is advisable to generate a new snapshot backup when installation is complete.

Chapter 4. Configuring Data Protection for Snapshot Devices

Configuration comprises setting up the database-independent components of Data Protection for Snapshot Devices, which establishes the basic snapshot backup and restore framework, and then tailoring the specific database environment to Tivoli Storage Manager functions (if applicable).

Configuring Data Protection for Snapshot Devices common components

The setup script must be run before attempting any backup or restore operation.

The setup script allows different levels of Data Protection for Snapshot Devices to be used simultaneously on the backup and production systems. This procedure must be performed for all applicable production systems and the backup system. For DB2, the script must be run for each DB2 instance.

1. (DB2) Log on as the DB2 instance owner.
2. (DB2) Change to the DB2 Advanced Copy Services installation directory `<DB2 instance directory>/acs`. For example:

   ```
   cd /home/db2inst1/sqllib/acs
   ```

3. Start the setup script (without options):

   ```
   setup_<database>.sh
   ```

   See "Installation setup script" on page 134 for details.

   The script in this mode performs the following steps to set up the instance:

   a. Stops the Management Agent (acsd) if it is running.

   b. If a profile already exists, you are prompted to perform one of these tasks:

      1) update the existing profile

      2) create a new profile

      3) use the existing profile without updates

      In the first two steps (or if the profile does not exist as in a first-time setup for the instance), the setup script starts the Management Agent wizard to create or update the profile and password file.

      The wizard asks for all profile parameters and performs syntax and range checking where possible. These profile entries must be defined by the user:

      - APPLICATION_TYPE
      - COPYSERVICES_HARDWARE_TYPE
      - VOLUMES_DIR (required for FlashCopy devices only)
      - ACS_REPOSITORY

      Other parameters have default values. The wizard also prompts for password information and creates the password file.

      Note: On an initial installation, the directory specified by ACS_REPOSITORY must not exist. It will be created by Data Protection for Snapshot Devices.

c. On a production system, restart `acsd` with the new profile (if applicable).
d. On a backup system, install the appropriate device agent and (optionally) the Offload Agent (tsm4acs). You can specify not to have tsm4acs entered in `/etc/inittab` and must then either call it manually or use a scheduler to start it. This is typically done to delay calling tsm4acs until resources are available for the backup.

If applicable, install the GCC Compiler Dynamic Runtime Library (libgcc) and set the links to the SSL libraries. See the sections on software requirements and Open SSL.

Related concepts

"Data Protection for Snapshot Devices profile description" on page 160
Detailed information is provided regarding the profile.

Related tasks

"Installing Open SSL" on page 96
Information about SSL libraries is provided.

Related reference

"Installation setup script" on page 134

Configuring the Oracle environment

The native Oracle environment requires specific configuration tasks before attempting a backup or restore operation.

This section addresses setup activity for backing up a native Oracle database to, or restore it from, a Tivoli Storage Manager server. This interface is not required for snapshot-only backup and restore.

This section provides the following instructions on how to configure Data Protection for Snapshot Devices so you can back up and restore your databases:

1. Register your workstations with the Tivoli Storage Manager server.
2. Specify a Tivoli Storage Manager management class for your backups.
3. Configure your disk storage environment.
4. Configure your Data Protection for Snapshot Devices and Data Protection for Oracle environment. This includes:
   - specifying options in the Data Protection for Oracle options file (tdpo.opt)
   - configuring your client software by specifying options in the client user options file (dsm.opt) and the client system options file (dsm.sys)
   - setting your client environment variables:
     - DSM_DIR
     - DSM_CONFIG
     - DSM_LOG
     - DSMI_DIR
     - DSMI_CONFIG
     - DSMI_LOG

     Note: These environment variables are defined in the Data Protection for Oracle options file (tdpo.opt).
   - create the RMAN backup script

Steps 1 and 4 must be performed on *both* the production system and backup system.

List of files installed by Data Protection for Snapshot Devices for Oracle

Data Protection for Snapshot Devices installs these files on a native Oracle environment.

The following Data Protection for Snapshot Devices files are installed in the installation directory:

- Sample server script (serverscript.smp.oracle)
- Production System User Interface (acsora)
- Offload Agent (tsm4acs)
- License File (tsmacs.lic)

Step 1. Register the workstations with the Tivoli Storage Manager server

Data Protection for Snapshot Devices requires both the backup system and production system to be registered as Tivoli Storage Manager clients.

A node name and a password (if one is required) is required to identify each client. Tivoli Storage Manager maintains a password for each node name. If a Tivoli Storage Manager client already exists on the system, it is recommended that a separate and unique node name for Data Protection for Oracle be used on the same system. This separate and unique Data Protection for Oracle node name must be the same on the production system and the backup system. For example, if the Data Protection for Oracle node name on the production system is *dporc1*, then the Data Protection for Oracle node name on the backup system must also be *dporc1*.

See the *IBM Tivoli Storage Manager for AIX Administrator's Guide* and the *IBM Tivoli Storage Manager for AIX Administrator's Reference* for more information about registering workstations to the Tivoli Storage Manager server.

Related reference

"AIX information sources" on page xvi

Step 2. Specify a Tivoli Storage Manager management class

Data Protection for Snapshot Devices backups in a native Oracle environment should be assigned to their own management class.

When you back up a database, the default management class for the node is used. Rather than binding a different management class for Oracle backups, we recommend that you specify a different domain. Create a new domain to be used for the Oracle backups and register your node to this new domain. The Oracle backups will be bound to the Default Management Class within this new domain.

When defining the backup copy group within this Default Management Class, set the following parameter values so that deleted backups are immediately removed from server storage:

- VERDELETED=0
- RETONLY=0

You can override the default value for the Management Class by specifying a different value with the client ***include*** option. The ***include*** option can be placed directly in the dsm.sys file located in the directory pointed to by $DSMI_DIR or in the include-exclude options file. The name of the include-exclude options file is placed in the client system options file (dsm.sys) located in the directory pointed to by $DSMI_DIR.

For example, to assign the management class name *orcbackup* to all of the Oracle backups with a default file space name of *tsmorc*, the include statement is:

```
include /tsmorc/.../* orcbackup
```

All the files backed up with a default file space name of *tsmorc* are assigned to management class *orcbackup*. Increase the value of the ***commtimeout*** option on the Tivoli Storage Manager server to 600 seconds to prevent a time-out from occurring during large database backups. You must increase the value of the ***maxnummp*** option on the Tivoli Storage Manager server to a value greater than the default value of *1* if you operate with multiple processors.

Step 3. Configure the disk storage environment

Each disk storage system requires its own unique configuration tasks.

Follow the steps in the appropriate procedure for your disk storage environment. Be aware that on your disk storage subsystem, Oracle datafiles must be defined on volume groups that are separate from the volume groups where the Oracle control files and redo logs are defined.

Defining Logical Unit Numbers on IBM TotalStorage snapshot devices storage subsystems

Logical Unit Numbers (LUNs) must be defined for the storage subsystem.

Perform these steps so that the proper LUNs are defined on both the production system and backup system:

1. Use the DS Storage Manager to create two (or more) LUNs on the production system:

   ```
   Real-time manager (or Simulated manager)-> Configure storage -> Open systems ->
   Volumes-open systems
   ```

   Note the following:
   - This example creates two LUNs.
   - These LUNs are the location where your database will reside.
   - The size of the LUNs is dependent upon the size of the database.
   - The size of the LUNs on both the production system and backup system must be the same.
   - Both the Source Volume and Target Volume must be defined on the same storage subsystem. However, the Oracle database itself can span multiple DS6000 storage subsystems or multiple DS8000 storage subsystems. For example, one set of source volumes and target volumes can be on the first storage subsystem while another set of source volumes and target volumes can be on the next storage subsystem. In this case, make sure that the ESSNI Servers for all storage subsystems (over which a database spans) are configured to the same ICAT using the **set device - addessserver** command.
2. Use the DS Storage Manager to create the same number of LUNs on the backup system as were created on the production system in Step 1:

   ```
   Real-time manager (or Simulated manager)-> Configure storage -> Open systems ->
   Volumes-open systems
   ```

These LUNs must also be the same size as the LUNs created on the production system.

3. Identify the serial numbers of the target LUNs using the DS Storage Manager:

   ```
   Real-time manager (or Simulated manager)-> Configure storage -> Open systems ->
   Volumes-open systems
   ```

   Select the target LUNs created on the backup system in Step 2. Identify the serial numbers with the matching size in the source LUNs. For example:

   ```
   1301901
   Nickname      Number Status Type GB
   sandburr_3300 3300   Normal  DS  2.0
   sandburr_3400 3400   Normal  DS  2.0
   ```

   In this example, the serial numbers are `13019013300` and `13019013400`.

4. Define the ***target_volume*** parameter in the profile with the appropriate serial numbers of the target LUNs:

   ```
   target_volume: 13019013300
   target_volume: 13019013400
   ```

   This setting specifies the target volumes to which the database will be backed up.

Creating virtual paths on the SAN Volume Controller

Virtual paths (vpaths) must be defined for the SAN Volume Controller.

This procedure uses the SAN VC Console to complete the tasks. Be aware that the SAN VC command line interface can also be used. For detailed information regarding these SAN VC applications, see *IBM TotalStorage SAN Volume Controller Configuration Guide Version 2.1.0*.

These instructions assume the following conditions exists:

- A functioning storage area network (SAN) is available.
- Storage disks are attached and available in the SAN VC environment.
- SDD is installed and available on the host machines.
- A cluster is available in the SAN VC environment.
- Each host has at least two (or more) paths to the SAN VC storage subsystem.

Perform these steps so that the proper vpaths are created on both the production system and backup system:

1. Create a host in the SAN VC environment:

   ```
   Work with Virtual Disks-> Hosts -> Create Host
   ```

   Repeat this step for each host that will participate in the Data Protection for Snapshot Devices environment.

2. Create and name a Managed Disk Group:

   ```
   Work with Managed Disks -> Managed Disk Groups -> Create MDisk Group
   ```

   You can select any number of disks.

3. Create a Virtual Disk using the Managed Disk Group created in the previous step:

   ```
   Work with Virtual Disks-> Virtual Disks -> Create Virtual Disks
   ```

Map the Virtual Disk to the hosts that were added in Step 1.

4. To view the Virtual Disks, run the following AIX commands on *each* host:
   a. **cfgmgr** This command makes the newly created LUNs recognizable to the host.
   b. **lsvpcfg** This command displays the hdisks and vpaths.

Step 4. Configuring the Data Protection for Oracle environment

Data Protection for Snapshot Devices in a native Oracle environment requires that the Data Protection for Oracle application be configured as directed.

Be aware that the only Data Protection for Oracle option you can specify in Oracle RMAN scripts is the fully qualified path name to the tdpo.opt file. For example:

```
allocate channel ch1 type 'sbt_tape 'parms'
ENV=(TDPO_OPTFILE=/usr/tivoli/tsm/client/oracle/bin/tdpo.opt)';
```

If the fully qualified path name is not specified, RMAN uses the tdpo.opt file located in the default installation directory.

See the *IBM Tivoli Storage Manager for Databases: Data Protection for Oracle for UNIX Installation and User's Guide* for more information regarding the tdpo.opt file.

Perform the following steps to configure Data Protection for Snapshot Devices:

1. Create a user account on both the production system and backup system. These two user accounts must have the same user name and user ID on *both* the production system and backup system.
2. Install Oracle Server on *both* the production system and backup system as the user created in Step 1.
3. Log on to the production system as the account created in Step 1. Create an Oracle database using **dbca** on the production system.
   - **Snapshot devices**: Use the LUNs that were defined in this procedure: "Defining Logical Unit Numbers on IBM TotalStorage snapshot devices storage subsystems" on page 106.
   - **SAN VC**: Use the vpath that was created in this procedure: "Creating virtual paths on the SAN Volume Controller" on page 107.

   Consider the following requirements when creating the target database:
   - Run the **smitty lv** command to verify that the file systems to be used by the database reside on snapshot-capable disks.
   - When creating file systems for your database on volume groups with snapshot volumes, make sure the JFS log is located on a single volume within the volume group. The FlashCopy backup may fail if the JFS log is striped across multiple volumes within the volume group.
   - Make sure all the Oracle control files and redo logs are on a volume group separate from the volume group where the Oracle datafiles reside. For example, run the **smitty lv** command to verify these files are on a separate volume group:

     ```
     Oracle VG1:
     ```

```
|LV NAME TYPE LPs PPs PVs LV STATE MOUNT POINT |

orc_system01 jfs 32 32 1 closed/syncd N/A |
orc_undotbs01 jfs 16 16 1 closed/syncd N/A |
orc_undotbs02 jfs 16 16 1 closed/syncd N/A |
orc_users jfs 8 8 1 closed/syncd N/A |
orc_index jfs 8 8 1 closed/syncd N/A |
orc_temp jfs 8 8 1 closed/syncd N/A |
orc_tools jfs 8 8 1 closed/syncd N/A |
orc_dbf1 jfs 16 16 1 closed/syncd N/A |
```

`Oracle VG2:`

```
LV NAME TYPE LPs PPs PVs LV STATE MOUNT POINT |
orc_redo01 jfs 8 8 1 closed/syncd N/A |
orc_redo02 jfs 8 8 1 closed/syncd N/A |
orc_redo03 jfs 8 8 1 closed/syncd N/A |
orc_redo04 jfs 8 8 1 closed/syncd N/A |
orc_redo05 jfs 8 8 1 closed/syncd N/A |
orc_redo06 jfs 8 8 1 closed/syncd N/A |
orc_control01 jfs 2 2 1 closed/syncd N/A |
orc_control02 jfs 2 2 1 closed/syncd N/A |
orc_control03 jfs 2 2 1 closed/syncd N/A |
orc_spfile jfs 2 2 1 closed/syncd N/A |
```

When Oracle control files reside on raw logical volumes on the production server, the same raw logical volumes (with the same characteristics) must be created on the backup server.

4. Create an Oracle user with **sysdba** authority for the database created in Step 3.
5. Log on to the production system and backup system as **root** user. Configure your client software on each system by performing the following:
   a. Specify appropriate options in the Data Protection for Snapshot Devices options files (dsm.opt and dsm.sys). See Table 27 on page 110.
   b. Specify appropriate options in the Data Protection for Oracle options files (dsm.opt and dsm.sys). See Table 28 on page 112.
   c. Specify appropriate Data Protection for Oracle options in the tdpo.opt file. See *IBM Tivoli Storage Manager for Databases: Data Protection for Oracle for UNIX Installation and User's Guide*.
   d. Set your environment variables for Data Protection for Snapshot Devices.
   e. Set your environment variables for Data Protection for Oracle. See Table 29 on page 114.
6. While logged on to the production system and backup system as user **root**, perform the following:
   a. Use the Data Protection for Oracle **tdpoconf password** command to generate a password file. For example:

      ```
      tdpoconf passw -tdpo_opt=tdpo.opt
      ```

   b. Use the Data Protection for Oracle **tdpoconf showenv** command to verify your Data Protection for Oracle environment. For example:

      ```
      tdpoconf showenv -tdpo_opt=tdpo.opt
      ```

7. Log on to the production system and backup system as the account created in Step 1. Add an entry to the tnsnames files that points to the RMAN catalog

database that will be used for the RMAN backup. Make sure the production system and backup system point to the same RMAN catalog database.

8. Create a generic RMAN backup script on the production system. See "RMAN backup script overview" on page 115 for detailed information.
9. Make sure the Oracle listener is running on the Oracle installation that contains the RMAN catalog database. Verify the RMAN configuration by manually connecting to the RMAN catalog from the production system and backup system. For example:

   ```
   rman target agnttest/agnttest rcvcat rman/rman@rmandb
   ```
10. Run the Tivoli Storage Manager **dsmc q f** command on both the production system and backup system to verify the Tivoli Storage Manager password is generated.

Related reference

"IBM Tivoli Storage Manager for Databases: Data Protection for Oracle information sources" on page xv

Configuring the Tivoli Storage Manager client software

You must specify options for the Tivoli Storage Manager API and backup-archive client software before performing a backup of your databases with Data Protection for Snapshot Devices.

Specify these Tivoli Storage Manager options in the client user options files (dsm.opt) and the client system options files (dsm.sys). Since options must be specified on both the production system and backup system, two sets of user options files and two sets of system options files are required.

Tivoli Storage Manager options files for Data Protection for Snapshot Devices for Oracle:

Data Protection for Snapshot Devices uses the dsm.opt and dsm.sys files located in the Tivoli Storage Manager backup-archive client installation directory (`/usr/tivoli/tsm/client/ba/bin`) or as pointed to by the DSM_DIR and DSM_CONFIG environment variables.

Tivoli Storage Manager options files for Data Protection for Snapshot Devices for Oracle

Specify the following options and values in the Data Protection for Snapshot Devices options files on *both* the production system and backup system:

Table 27. Required Data Protection for Snapshot Devices TSM options and values

File name	Required Option	Required Value
dsm.opt	***servername***	*server name defined in stanza in dsm.sys file pointed to by DSM_DIR*

Table 27. Required Data Protection for Snapshot Devices TSM options and values (continued)

File name	Required Option	Required Value
dsm.sys	***nodename***	*the node name in dsm.sys on the production system must be different from the node name in dsm.sys on*
	schedmode	*the backup system*
	passwordaccess	*prompt*
	tcpserveraddress	*generate*
		same TCP/IP server address as defined in stanza in dsm.sys file
	tcpport	*pointed to by DSMI_DIR*
		TCP/IP port address for server defined by tcpserveraddress
	servername	
		the name of the server you want to use and the stanza that contains options for that server
	errorlogname	
		the fully-qualified path and name of the file in which to store all error information

Data Protection for Snapshot Devices TSM options file considerations:

These options files require certain values and considerations before implementing a backup or restore operation.

- The node name specified in the stanza defined in the dsm.sys file pointed to by DSM_DIR on the production system is the *production node*.
- The node name specified in the stanza defined in the dsm.sys file pointed to by DSM_DIR on the backup system is the *backup node*.
- The names of the *production* and *backup* nodes must be different.
- The *production node* and *backup node* must be registered on the same server.
- The ***passwordaccess*** option must be set to *generate* on both the production system and backup system.
  - Run the **dsmc query session** command as *root* user on the production system to generate the password before running acsora for the first time.
  - Run the **dsmc query session** command as *root* user on the backup system to generate the password before running tsm4cas for the first time.
- You can consolidate all error messages into a single file by specifying the ***errorlogname*** option in the dsm.sys file pointed to by the DSM_DIR environment variable. For example:

  ```
  errorlogname /home/tdphdw/log/tdphwer.log
  ```

Otherwise, Tivoli Storage Manager backup-archive client errors are logged to the dsmerror.log file and Data Protection for Snapshot Devices errors are logged.

Data Protection for Snapshot Devices TSM options file examples:

Refer to these options file examples when setting up Data Protection for Snapshot Devices in a native Oracle environment.

The dsm.opt file in the `/usr/tivoli/tsm/client/ba/bin` directory on the production system and backup system:

```
servername server1
```

The stanza for **server1** in the dsm.sys file in the `/usr/tivoli/tsm/client/ba/bin` directory on the production system:

```
servername server1
tcps       server1.test.rsch.com
tcpp       1500
passworda  generate
schedmode  prompt
nodename   prodnode
errorlogname /home/tdphdw/log/tdphwer.log
```

The stanza for **server1** in the dsm.sys file in the `/usr/tivoli/tsm/client/ba/bin` directory on the backup system:

```
servername server1
tcps       server1.test.rsch.com
tcpp       1500
passworda  generate
schedmode  prompt
nodename   bunode
errorlogname /home/tdphdw/log/tdphwer.log
```

Data Protection for Oracle options files:

Data Protection for Oracle uses the dsm.opt and dsm.sys files located in the Tivoli Storage Manager API installation directory (`/usr/tivoli/tsm/client/api/bin`) or as pointed to by the DSMI_DIR and DSMI_CONFIG environment variables.

Tivoli Storage Manager options files for Data Protection for Oracle

Specify the following options and values in the Data Protection for Oracle options files on *both* the production system and backup system:

Table 28. Required Data Protection for Oracle option values

File name	Required Option	Required Value
dsm.opt	**`servername`**	*`server name defined in stanza in dsm.sys file pointed to by DSMI_DIR`*

Table 28. Required Data Protection for Oracle option values (continued)

File name	Required Option	Required Value
dsm.sys	***nodename***	*the node name in dsm.sys on the production system must be the same as the node name in dsm.sys on the backup system*
	passwordaccess	*prompt*
	tcpserveraddress	*same TCP/IP server address as defined in in stanza in dsm.sys file pointed to by DSM_DIR*
	tcpport	*TCP/IP port address for server defined by tcpserveraddress*
	servername	*the name of the server you want to use and the stanza that contains options for that server*
tdpo.opt	***tdpo_owner***	*the value specified on the production system must be the same as the value specified on the backup system*

Data Protection for Oracle options file considerations:

These options files require certain values and considerations before implementing a backup or restore operation.

- The names of the *production* and *backup* nodes must be the same.
- The ***passwordaccess*** option must be set to *prompt* on both the production system and backup system.

Data Protection for Oracle options file examples:

Refer to these options file examples when setting up Data Protection for Oracle.

The dsm.opt file in the `/usr/tivoli/tsm/client/api/bin` directory on the production system and backup system:

```
servername server2
```

The stanza for **server2** in the dsm.sys file in the `/usr/tivoli/tsm/client/api/bin` directory on the production system:

```
servername server2
tcps       server1.test.rsch.com
tcpp       1500
passworda  prompt
nodename   hdworc1
```

The stanza for **server2** in the dsm.sys file in the `/usr/tivoli/tsm/client/api/bin` directory on the backup system:

```
servername server2
tcps       server1.test.rsch.com
tcpp       1500
passworda  prompt
nodename   hdworc1
```

System options file requirements:

These requirements must be met when setting the system options files (dsm.sys).

The system options file (dsm.sys) must refer to the same Tivoli Storage Manager server.

- See "Configuring system options files to use the same server" on page 221 for instructions and examples.

The system options file (dsm.sys) can be configured with multiple server stanzas or as two separate files.

- To configure the system options files (dsm.sys) as *multiple server stanzas*:
  1. See "Configuring multiple server stanzas" on page 222 for instructions and examples.
  2. Set the option values in the dsm.opt and dsm.sys files as shown in Table 27 on page 110 and Table 28 on page 112.
  3. Make sure the dsm.opt file points to a server stanza defined in the dsm.sys file.
- To configure the system options files (dsm.sys) as *two separate files*:
  1. Set the option values in the dsm.opt and dsm.sys files as shown in Table 27 on page 110 and Table 28 on page 112.
  2. Make sure the dsm.opt file points to a Tivoli Storage Manager server defined in the dsm.sys file.

Environment variable settings

If backups are not solely disk backups, the following environment variables must be set on both the production system and backup system.

Data Protection for Snapshot Devices shares environment variables with the Tivoli Storage Manager backup-archive client:

Data Protection for Oracle shares environment variables with the Tivoli Storage Manager API:

Table 29. Required Data Protection for Oracle environment variable settings

Environment Variable	Value	Default
DSMI_DIR	The fully-qualified path containing dsm.sys	`/usr/tivoli/tsm/client/api/bin`
DSMI_CONFIG	The fully-qualified path including the tdpo.opt file	`/usr/tivoli/tsm/client/api/bin/dsm.opt`
DSMI_LOG	The fully-qualified path containing tdpoerror.log. This directory must have write access.	`/usr/tivoli/tsm/client/api/bin`

Additional information about environment variables is located in the *IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients Installation and User's Guide* and the *IBM Tivoli Storage Manager Using the Application Program Interface*.

Related reference

"Tivoli Storage Manager information sources" on page xiv

RMAN backup script overview

An RMAN backup script is a user-created script that defines Oracle RMAN functions.

Data Protection for Snapshot Devices performs Tivoli Storage Manager database backups using an Oracle RMAN backup script. This RMAN backup script is invoked by Data Protection for Snapshot Devices and must be created by the user. The Data Protection for Snapshot Devices user profile will need to be edited to include the fully qualified path and file name for this RMAN backup script. The RMAN backup script must contain the following:

- **run**, **backup** keywords
- allocate and release at least one channel
- the fully qualified path name to the Data Protection for Oracle options file (tdpo.opt)
- The allocate channel command and the ENV parameter MUST be specified on the same line. For example:

  ```
  allocate channel t1 type 'sbt_tape' parms 'ENV=(TDPO_OPTFILE=(.../tdpo.opt)';
  ```

  The allocate channel commands and ENV parameters are shown on separate lines in the example below due to formatting restrictions.
- The database command MUST be specified on a line separate from the backup command as show in the example below.

Attention: To prevent possible processing failures, do not specify the RMAN *full* parameter in the Oracle RMAN backup script.

RMAN backup script example:

Refer to this example when creating the RMAN backup script.

Below is an example RMAN backup script:

```
run
{
allocate channel t1 type 'sbt_tape' parms
'ENV=(TDPO_OPTFILE=/usr/tivoli/tsm/client/oracle/bin/tdpo.opt)';
allocate channel t2 type 'sbt_tape' parms
'ENV=(TDPO_OPTFILE=/usr/tivoli/tsm/client/oracle/bin/tdpo.opt)';
allocate channel t3 type 'sbt_tape' parms
'ENV=(TDPO_OPTFILE=/usr/tivoli/tsm/client/oracle/bin/tdpo.opt)';
allocate channel t4 type 'sbt_tape' parms
'ENV=(TDPO_OPTFILE=/usr/tivoli/tsm/client/oracle/bin/tdpo.opt)';
backup
(database);

release channel t1;
release channel t2;
release channel t3;
release channel t4;
}
```

Mounting shared directories via NFS

The $HOME/acs directories on the production system should be mounted on the backup system.

It is recommended to do this step prior to installation and customization of Data Protection for Snapshot Devices in order to facilitate the overall installation and customization process.

To simplify the implementation and to facilitate later operations control, the following directories of the production system should be mounted on the backup system:

```
$HOME/acs
```

If additional directories (such as the ones you will specify in the Data Protection for Snapshot Devices profile) will be shared, you have to mount them as well.

NFS is required primarily to share profiles and password files.

Setting up source and target volumes for FlashCopy devices

Explicit definition of target volumes is required only for FlashCopy devices. Snapshot devices such as N Series allocate target volumes automatically on request.

Setting up volumes for FlashCopy operations requires that the volumes that are used as source volumes and target volumes reside on the same hardware unit or SAN Volume Controller cluster. In addition, the size of the source volume must match the size of the target volume. If you plan to use multiple target sets, the target-volume requirements apply for all target volumes in each set. Attach the source volumes to the production system and the target volumes to the backup system. When the FlashCopy completes, Data Protection for Snapshot Devices (tsm4acs) can mount the target volumes on the backup system. Do not attach the source and target volumes to both systems.

Setting up source and target volumes in an ESS or DS configuration

The ESS or DS source volumes and target volumes must be made accessible in AIX.

Use the ESS Specialist or DS Storage Manager interface to make volumes accessible in AIX. The target volumes must be identified by their serial numbers in the target volumes file. A general guideline is to distribute the volumes of one storage system server across as many logical subsystems (LSS) as possible.

Issue this command to check the volumes that have been received:

- Issue this command if SDD or SDDPCM is installed:

```
lsvpcfg >outfile
grep serial outfile
```

- Issue this command if neither SDD nor SDDPCM is installed:

```
lsdev -Cc disk
```

Look for volumes of the storage system by the applicable device type.

Related tasks

"Data Protection for Snapshot Devices Target Volumes File (.fct)" on page 189
The target volumes file identifies the target volumes to be used for a FlashCopy backup.

Related reference

"Target volume parameter settings (ESS or DS configuration)" on page 190
Each target volume planned for use must be specified by its serial number.

Setting up source and target volumes in a SAN Volume Controller configuration

The SAN Volume Controller source volumes and target volumes must be made accessible in AIX.

Use the SAN Volume Controller master console Web interface to make volumes accessible on AIX. In configuration, the target volumes to be used must be identified by the virtual disk name in the target volumes file.

Issue this command to check the volumes that have been received:

- If SDD or SDDPCM is installed, issue this command to view an AIX disk device that belongs to a SAN Volume Controller vdisk name:

  ```
  lsvpcfg > outfile
  grep serial outfile
  ```

  In the SAN Volume Controller Web interface, you can map the virtual disk name to the serial number you see on AIX.
- Issue this command if neither SDD nor SDDPCM is installed:

  ```
      lsdev -Cc disk
  ```

  Look for volumes of the storage system by the applicable device type.

Related reference

"Parameters for an SVC Configuration" on page 191
Each target volume planned for use must be specified by its virtual disk name.

Guidelines for sharing target volumes

Certain requirements must be met when one common set of target volumes is to be used for multiple databases.

Data Protection for Snapshot Devices was designed such that at least one dedicated set of target volumes must be provided for each database instance that is identified by an SID. If one common set of target volumes is to be used for multiple databases, make sure these requirements are met:

- (DB2) The **db2 backup**executions for the various databases (SIDs) must run in sequence and always show a successful completed backup cycle for one database (e.g., SID=TST) before running 'db2 backup' for a different database (e.g., SID=PRD).
- A control mechanism must be in place to ensure that succeeding 'db2 backup' runs will be started only if the preceding run terminated successfully. There are

various possibilities to establish such a mechanism, such as the use of job scheduling products, controlled lock files, etc.

Important: If the customer fails to exercise stringent control over the sequence of ’db2 backup’ runs for the different database instances when using shared target volumes, this can have a decidedly negative impact on all such runs involved. Of course, sharing target set volumes in conjunction with disk copy backups (FLASHCOPY_TYPE COPY or INCR) is counterproductive. Data Protection for Snapshot Devices cannot detect such improper use and would assume that the target set can be used for a snapshot restore if the set was not deleted using the db2acsutil ’delete’ function. If a snapshot restore is attempted using the disk copy backup from another database, corruption of your database is a virtual certainty.

Chapter 5. Protecting data on snapshot devices

Information needed to back up and restore data on snapshot devices is provided.

Review the information carefully before performing a backup or restore operation.

Backing up data on snapshot devices

Data Protection for Snapshot Devices provides two basic backups methods.

Backing up a DB2 database

The following table summarizes the command entries according to the database configuration and type of backup:

Table 30. Summary of Backup Commands for DB2

		Backup to TSM		
Database Configuration	**Snapshot Backup (Disk Only)**	**From Production Database (Tape Only)**	**Integrated with Snapshot**	**From Existing Snapshot**
DB2 (Native)	db2 backup .... use snapshot ...	db2 backup ...use tsm	db2 backup .... use snapshot ... OPTIONS TSM_BACKUP	tsm4acs -f tape_backup
DB2 (SAP)	db2 backup .... use snapshot ...	db2 backup... load <library> or backom	db2 backup .... use snapshot ... OPTIONS TSM_BACKUP	tsm4acs -f tape_backup

Snapshot backup is described in more detail in the DB2 High Availability Feature documentation. The ′db2 backup database′ command with the ′use snapshot′ option is described in the DB2 *Command Reference*.

DB2 backups to a Tivoli Storage Manager server

Data Protection for Snapshot Devices (tsm4acs) accesses DB2 to implement a backup to Tivoli Storage Manager tape from a snapshot backup.

DB2 operates in either of the following environments:

- Tivoli Storage Manager for ERP in an SAP environment
- DB2 native Tivoli Storage Manager agent in a native DB2 environment.

A Tivoli Storage Manager backup is performed by the following:

- The TSM_BACKUP vendor option (specified with the ′db2 backup database′ command or defined as a parameter in the Tivoli Storage Manager for ERP profile) initiates a tape backup from the snapshot target set when the snapshot has completed.
- The ′tape_backup′ function of Data Protection for Snapshot Devices (tsm4acs), backs up a previously generated snapshot. Data Protection for Snapshot Devices accepts snapshot backups generated by IBM Tivoli Storage Manager for Advanced Copy Services version 5.5 (or later) only.

Data Protection for Snapshot Devices and Tivoli Storage Manager for ERP use their own profiles. The Data Protection for Snapshot Devices profile contains a separate section (OFFLOAD) that defines the parameters related for tape backup.

Related concepts

"Specific customization requirements" on page 74
Describes the relationships between the Data Protection for Snapshot Devices and Tivoli Storage Manager for ERP profiles.

"Data Protection for Snapshot Devices profile description" on page 160

Backups without snapshot backup disks:

Partial backups of a database (such as tablespace backups) can be performed on the production system.

The db2 backup command might access Tivoli Storage Manager for ERP (if installed). Data Protection for Snapshot Devices is not accessed for partial backups.

Serial and parallel backup modes for DB2 database partitioning feature partitions:

DB2 backs up database partitioning feature (DPF) partitions in either serial mode or parallel mode.

These modes are determined by DB2 and cannot be configured by the user. In serial mode (used for a native DB2 database), the partitions are processed sequentially: each partition is suspended, the snapshot created, and the partition resumed before the next partition is processed. (SAP) In parallel mode (default mode for an SAP DB2 database), all partitions are suspended before DB2 issues snapshot requests. The requests are then performed in parallel on all partitions. In either mode, Data Protection for Snapshot Devices will return an error at backup time if multiple partitions share a physical volume. A restore operation is always performed on a single partition.

Backing up a native Oracle database

Data Protection for Snapshot Devices integrates with multiple components when backing up an Oracle database.

This table summarizes the command entries according to the type of backup:

Table 31. Summary of Backup Commands for Native Oracle

	Backup to Tivoli Storage Manager		
Snapshot Backup (Disk Only)	**From Production Database (Tape Only)**	**Integrated with Snapshot**	**From Existing Snapshot**
acsora -f backup	RMAN using Data Protection for Oracle	'acsora -f backup' with profile parameter TSM_BACKUP set to YES and running tsm4acs in daemon mode on the backup server	'tsm4acs -f tape_backup' with profile parameter TSM_BACKUP set to YES and tsm4acs not running in daemon mode

(Tivoli Storage Manager Server) Data Protection for Snapshot Devices backs up a metadata file on the production system to the Tivoli Storage Manager server. This file contains information (metadata) required by Data Protection for Snapshot Devices on the production system to perform a snapshot restore. Data Protection for Snapshot Devices also backs up the user profile on the production system to the Tivoli Storage Manager server. This profile is required to perform all Data Protection for Snapshot Devices commands. You can restore this file from the Tivoli Storage Manager server in the event it is lost. If Tivoli Storage Manager is not configured, the metadata is retained in the IBM Tivoli Storage Manager for Advanced Copy Services repository.,

Note: You cannot run multiple concurrent instances of the backup executable component (tsm4acs) on the backup system to back up multiple databases.

Data Protection for Snapshot Devices does not back up the transaction logs of the Oracle database. The database administrator is responsible for periodically backing up the Oracle database transaction logs. It is recommended that the transaction logs be backed up to the Tivoli Storage Manager server after every full database online backup. The backup executable (tsm4acs) cannot be run concurrently on the backup system to back up multiple databases.

FlashCopy relationships and their impact on profile parameters

Specify FLASHCOPY_TYPE: INCR for backup and restore processing to take advantage of improved performance during normal production operations.

The FLASHCOPY_TYPE: *incr* setting reduces the time required to complete background copy processing. Once incremental change recording is enabled and a persistent FlashCopy relationship is established between a source volume and a target volume, the snapshot devices only accepts incremental FlashCopy requests and fails FlashCopy requests for COPY and NOCOPY backup types. It is desirable to maintain these persistent relationships so that incremental backups to the snapshot devices can be used for snapshot restores. It is recommended that an automated backup to the snapshot devices be performed every few hours and an automated backup to the Tivoli Storage Manager server be performed at least once a day. You must use different profiles with the appropriate backup destination for these automated backups. When a database is backed up to the Tivoli Storage Manager server only and FLASHCOPY_TYPE NOCOPY is specified, no background copy of the database is made. However, if the same set of target volumes are used for both backup destinations and a persistent relationship exists due to incremental change recording being enabled, the backup will fail.

To address such conditions, Data Protection for Snapshot Devices proceeds in the following manner:

- If invalid option values or an invalid combination of option values are specified, processing fails and an error message displays.
- If FLASHCOPY_TYPE NOCOPY is specified, the target physical volume identifier (PVID) is cleared and the database cannot be restored through snapshot restore. The database must be manually restored from the Tivoli Storage Manager server. In this case, the target volumes can be used as targets for source volumes from multiple databases.
- If FLASHCOPY_TYPE COPY or INCR is specified, the target PVID remains intact and the database can be restored through snapshot restore.
- If the FlashCopy pairs are found in incremental relations, Data Protection for Snapshot Devices performs an incremental FlashCopy backup and overrides the FLASHCOPY_TYPE value in the profile to keep the persistent relationship intact. The database can be restored using snapshot restore. A message displays stating that an incremental FlashCopy backup was performed and that you must withdraw the persistent relationship to perform a COPY or NOCOPY backup.

Note: Data Protection for Snapshot Devices does not permanently change the profile. It just overrides the value for the current FlashCopy backup.

- Data Protection for Snapshot Devices stores a copy of the database control file in the IBM Tivoli Storage Manager for Advanced Copy Services repository. This allows to restore a snapshot with or without the database control file, even if a Tivoli Storage Manager server is not used in the environment.
- If, during snapshot restore processing from two or more snapshot devicess, the FlashCopy should fail for some unexpected reason, you cannot immediately retry a snapshot restore because a background copy from one of the snapshot devicescould be in progress, . In this situation, perform one of the following tasks:
  - In case of FLASHCOPY_TYPE INCR, wait until the background copy completes for those FlashCopy commands that are already in progress. The persistent FlashCopy relationships will remain intact and the snapshot restore will complete quickly when tried again.
  - Note that when the ’delete force’ option (’ascora -f delete -F ’) is used to withdraw incremental relationships, the corresponding version of the disk backup is considered discarded and is no longer available. Subsequent restores should be performed from Tivoli Storage Manager storage until a valid disk backup is performed.

In the following situations, Data Protection for Snapshot Devices detects that a full volume restore is required and performs a full FlashCopy backup (even when FLASHCOPY_TYPE INCR is specified):

- The very first time a database is backed up during normal production operations.
- Backup or restore processing during normal production when change recording is not enabled or when the database has been lost (restore only).
- Restore processing during normal production when the entire database has been lost and the FlashCopy relationship has been withdrawn.

General backup requirements on native Oracle

These backup strategy requirements must be met in order for Data Protection for Snapshot Devices to function properly when using Tivoli Storage Manager.

- The Oracle user must have **dba** and **sysdba** authority.
- Make sure a file system exists that contains the Oracle archive directory. Mount this file system before performing a backup.
- You must use the same syntax as provided in the sample profile.
- Oracle Server must be available on both the production system and backup system. The target database is created on the production system only.
- The Tivoli Storage Manager client password file must be generated on both the production system and backup system.
- The RMAN backup script created by the user must contain the Data Protection for Oracle TDPO_OPTFILE environment variable. Specify the fully qualified path name to the tdpo.opt options file with the TDPO_OPTFILE environment variable. See “RMAN backup script example” on page 115 for an example of this setting.
- The RMAN backup script created by the user must contain the Data Protection for Oracle TDPO_OPTFILE environment variable. Specify the fully qualified path name to the tdpo.opt options file with the TDPO_OPTFILE environment variable. The allocate channel command and the ENV parameter MUST be specified on the same line. Also, the database command MUST be specified on a line separate from the backup command in the RMAN backup script.

- The physical volume that the database resides on must be associated with the FlashCopy devices on the snapshot devices.
- The FlashCopy storage device must be configured so that the proper Logical Subsystem is available on both the production system and backup system.
- If two databases are backed up (especially at the same time), you must use different profile names.
- The target database being backed up cannot reside on the same volume group as the file system that contains $ORACLE_HOME. Make sure the Oracle Server does not share a volume group with the target database.
- Make sure to increase the size of the following two Oracle options located in the `$ORACLE_HOME/dbs/init(database_name).ora` file:

```
sort_area_size = 10000000
sort_area_retained_size = 10000000
```

Related reference

"RMAN backup script example" on page 115
Refer to this example when creating the RMAN backup script.

Backups to a Tivoli Storage Manager server on native Oracle

A Data Protection for Snapshot Devices backup to Tivoli Storage Manager server storage is an integral part of your overall backup strategy.

Perform regular FlashCopy backups of your databases as a part of your backup strategy. In addition, perform FlashCopy backups when any configuration changes are made to your database. Adding new physical disks, new logical volumes, new file systems, or new database containers are some (but not all) examples of such configuration changes.

Manually backing up a native Oracle database:

A manual backup performs a one-time backup of an Oracle database.

Table 32. Files used during a manual backup

File name	Description	Default Location
acsora	Data Protection for Snapshot Devices production system executable file	`/usr/tivoli/tsm/client/tdphdw/oracle/bin`
tsm4acs	Data Protection for Snapshot Devices backup system executable file	`/usr/tivoli/tsm/client/tdphdw/oracle/bin`
profile	Data Protection for Snapshot Devices profile	`ACS_DIR/profile`

1. Log on to the production system as the database instance owner.
2. Create the profile by running the setup script without parameters.
3. Run the **backup** command:

```
acsora -f backup -p <profile name>
```

Related concepts

"Data Protection for Snapshot Devices profile description" on page 160
Provides descriptions of available profile parameters.

Related tasks

"Restoring hdisks for Subsystem Device Drivers" on page 223
Provides instructions regarding how to bring up the hdisk and vpath devices on a backup system that has SDD installed.

Fully automating a native Oracle database backup:

A fully automated backup uses a server script with the Tivoli Storage Manager scheduler to fully automate online backups of Oracle databases.

The backups on the production system can be run manually or via a scheduler.

A distinction must be made between *synchronous* and *asynchronous* offloaded backups. Synchronous means that the backup on the backup host starts as soon as a FlashCopy has been performed. In this case tsm4acs runs in daemon mode started by the init daemon. Asynchronous means that tsm4acs on the backup server is started manually or by another scheduler. This is useful if the backup should be delayed until required resources are available. During the installation on the backup server the user is asked which way he wants to run tsm4acs.

Related concepts

"Data Protection for Snapshot Devices profile description" on page 160
Provides descriptions of available profile parameters.

Related tasks

"Restoring hdisks for Subsystem Device Drivers" on page 223
Provides instructions regarding how to bring up the hdisk and vpath devices on a backup system that has SDD installed.

Related reference

"Defining settings in the server script" on page 222
A Tivoli Storage Manager server script contains the necessary client steps to coordinate a partially automated backup or a fully automated backup.

Backing up an SAP® with Oracle database

Data Protection for Snapshot Devices integrates with multiple components when backing up an SAP® with Oracle database.

The following table summarizes the command entries for backing up an SAP® database using Oracle:

Table 33. Summary of Backup Commands (SAP with Oracle)

	Backup to Tivoli Storage Manager		
Snapshot Backup (Disk Only)	**From Production Database (Tape Only)**	**Integrated with Snapshot**	**From Existing Snapshot**
brbackup -d util_vol ...	brbackup -d util_file ...	brbackup .... -d util_vol -.O	tsm4acs -f tape_backup

Fully automating an SAP® with Oracle database backup

A scheduled backup starts the backup operation automatically instead of manually.

A Tivoli Storage Manager schedule or crontab (UNIX or Linux) command are examples of those schedules that can be used to automatically run the snapshot disk backups on the production system. Any other suitable scheduler can also be employed.

(SAP®) The SAP® Computing Center Management System (CCMS) scheduler cannot be used to schedule snapshot backups. However, scheduling is available via the DBA Planning Calendar. The scope of control of the Tivoli Storage Manager is at an enterprise level. The crontab approach can only be used to set up schedules on systems on which the backups will be later performed.

Restoring data on snapshot devices

Data Protection for Snapshot Devices provides two basic restore methods.

Restoring from a snapshot on N Series devices with subsequent snapshots in the busy state

Specific guidelines must be understood when a snapshot is in a busy state.

An attempt to restore a snapshot other than the latest snapshot results in the deletion of those snapshots taken after the one to be restored. However, if any of these later snapshots are in the ’busy’ state, they are being used by another application and cannot be deleted until the ’busy’ state has been reset. An error message is issued when the restore from the earlier snapshot is attempted. One specific example would be when the Data Protection for Snapshot Devices offloaded tape backup function is running for a snapshot taken after the one to be restored. The offloaded tape backup function will create a clone volume based on the snapshot and activate it on the backup system. Data Protection for Snapshot Devices will normally free the resource after the function is finished. The user may also use the snapshots for other purposes.

Perform these steps to determine which snapshots are in the ’busy’ state:

1. Log in to the N Series filer using ssh or telnet.
2. Issue this command to determine what snapshots are in use:
   ```
   snap list <volume name>
   ```
3. Issue this command to check the usage of the snapshots of the source volume:
   ```
   vol status <volume name>
   ```
4. Issue this command to check the physical disk on the host in the case of SAN attachment:
   ```
   sanlun lun show
   ```

Example

```
$host>telnet xxxxxxx.location.com
Data ONTAP (xxxxxxx.location.com)
login: username
Password: password
tivoli-na> Mon Jul  9 13:43:15 GMT [telnet_0:info]: username logged in from host: host.location.com

tivoli-na> snap list fvC01data

Volume fvC01data
working...

  %/used       %/total  date          name
----------  ----------  ------------  --------
  0% ( 0%)    0% ( 0%)  Jul 09 13:41  ACS_BOBA10FEC_FVC01DATA (busy,vclone)
  0% ( 0%)    0% ( 0%)  Jul 09 11:03  ACS_BOBA4DB5C_FVC01DATA

tivoli-na> vol status fvC01data
         Volume State      Status            Options
      fvC01data online     raid_dp, flex
                           degraded
                Volume has clones: fvC01data_clone
                Containing aggregate: 'aggr0'

root@morton:/db2/C01/db2c01>sanlun lun show
    filer:         lun-pathname         device filename       adapter     protocol        lun size        lun state
 tivoli-na: /vol/fvC01data_clone/sapdata2       hdisk10        fcs0         FCP        12g (12884901888)    GOOD

 lspv | grep hdisk10
hdisk10         004208976073f72a                    C01tdp1         active
```

Restoring from a snapshot on SVC devices

Specific guidelines must be understood when a snapshot is in a busy state.

The SVC does not support reverse incremental FlashCopy from the target volumes. This means that snapshot restores require the source/target FlashCopy mappings to be discarded and reverse target/source mappings to be created.

Restoring a DB2 database

Specific command entries are used when restoring a DB2 database.

The following table summarizes the command entries according to the database configuration and type of restore:

Table 34. Summary of Restore Commands for DB2

Database Configuration	**Snapshot Restore**	**Restore from Tivoli Storage Manager**
DB2 (Native)	db2 restore .... use snapshot ...	db2 restore ... or db2 recover...
DB2 (SAP)	db2 restore .... use snapshot ...	db2 restore ..., db2 recover... or backom

Depending on the options specified in the `db2 backup database ... use snapshot ...` command when the snapshot was created, both backup types (snapshot and Tivoli Storage Manager) for a particular backup level may be eligible for a restore. A snapshot backup type might not be eligible for restore (even though the snapshot backup request completed successfully) because the background copy has not yet completed. Restore from snapshot backups will handle backup objects residing on the target volumes created in the backup operation with a snapshot process. These objects are referred to as snapshots.

DB2 backup history file overview

DB2 provides its own history file that stores all information about backup, restore, and changes in the database (such as adding containers to a tablespace).

Issue one of these commands to list information from the backup history file:

```
db2 list history backup all for <SID>
```

or

```
db2 list history rollforward all for <SID>
```

For more information about the **db2 list history** command, see *IBM DB2 Command Reference*.

To restore a backup that was performed on the local production system, you can find the timestamp of the backup with the **db2 list history** command.

Restoring an SAP® with Oracle database

Specific command entries are used when restoring an SAP® with Oracle database.

The following table summarizes the command entries according to the type of restore:

Table 35. Summary of Restore Commands for SAP® with Oracle

Snapshot Restore	Restore from Tivoli Storage Manager
brrestore -d util_vol	brrestore -d util_file

Restoring a native Oracle database

Specific command entries are used when restoring a native Oracle database.

The following table summarizes the command entries according to the type of restore:

Table 36. Summary of Restore Commands for Native Oracle

Snapshot Restore	Restore from Tivoli Storage Manager
acsora -f restore [-b backup_ID]	Using Data Protection for Oracle, RMAN.

A Oracle database is restored to one of the following locations:

- Data Protection for Oracle on the production system.
  - The data can be sent directly over a local area network (LAN) to the source volumes on the snapshot devices. This is the recommended restore.
  - Use of LAN-free restore is only supported if the required storage area network (SAN) environment exists.
  - When Oracle data files reside on raw logical volumes, there is no file system to mount on the production server after restore processing completes.
- Data Protection for Oracle on the backup system.
  - Data can be sent to the target volumes (or FlashCopy volumes) on the snapshot devices and copied to the source volumes. This method is not recommended.

Note that Oracle databases backed up with Data Protection for Enterprise Storage Server for Oracle Version 5.2.2 (or earlier) and currently residing on Enterprise Storage Server disks *cannot* be restored directly to a snapshot devices storage subsystem with Data Protection for Snapshot Devices. See “Data Protection for Snapshot Devices for Oracle migration considerations” on page 15 for suggested restore methods for this situation.

This chapter describes how to restore your Oracle database using the snapshot restore feature.

Snapshot restore scenarios for native Oracle databases

These scenarios demonstrate how to perform a snapshot restore of the Oracle database *myDB*.

The following conditions are assumed in all three scenarios described in this section:

- The redo logs for *myDB* reside in a volume group not shared with any datafiles.
- The Oracle control files are created in volume groups not shared by Oracle datafiles.
- The Oracle datafiles are created on the snapshot devices.

Scenario 1: Snapshot restore for native Oracle databases:

This scenario demonstrates how to perform a snapshot restore of the Oracle database myDB when FLASHCOPY_TYPE COPY is specified in the profile and no new file systems or logical volumes have been created on the LUNs that myDB resides on since the database was originally backed up.

Follow these steps to perform a snapshot restore of database *myDB*:

1. Log on to the production system and issue the following command:
   ```
   acsutil -f restore
   ```
   This restores the latest backup. To restore an older backup the backup_ID of this backup needs to be specified as in
   ```
   acsora -f restore -b <backup ID>
   ```
   ’acsutil’ can be used to query for existing backup ID’s.
2. After snapshot restore processing completes, you must recover the database.
   - If DATABASE_CONTROL_FILE_RESTORE YES is specified in the profile, you must perform an incomplete recovery.
   - If DATABASE_CONTROL_FILE_RESTORE NO is specified in the profile, you must perform a complete recovery.

At this point, snapshot restore processing is complete.

If snapshot restore processing completes successfully, you are now able to open the restored database *myDB*. If your snapshot restore was not successful and you receive an error message, see the log file for assistance.

Scenario 2: Snapshot restore for native Oracle databases:

This scenario demonstrates how to perform a snapshot restore of the Oracle database *myDB* when a new file system (*/newFS*) was created on the LUNs that *myDB* resides on since the database was originally backed up.

A snapshot restore process prompts you after determining that the configuration has changed (as a result of the new file system, */newFS*) since the database was originally backed up.

- If you specify *yes*, Data Protection for Snapshot Devices will delete the new file system (*/newFS*) and restore the database to the state it was in when originally backed up.
- If you specify *no*, Data Protection for Snapshot Devices terminates restore processing. You can copy the data in the new file system (*/newFS*) to a temporary location and run the snapshot restore again.

  If the new file system (*/newFS*) contains non-critical data and a copy of */newFS* exists on Tivoli Storage Manager storage, you can perform the following tasks:

  1. Remove */newFS* from the LUNs.
  2. Restore the database using snapshot restore.
  3. Restore */newFS* from Tivoli Storage Manager storage.

  If the new file system (*/newFS*) contains *critical* data and a copy of */newFS* does *not* exist on Tivoli Storage Manager storage, you can manually reconstruct the file system (after a snapshot restore of the database) then recover the database using Oracle SQL commands:

  1. Use the **smitty fs** command to add a file system (*/newFS*):

     ```
     Add File Systems -> Journaled File Systems -> Add a
     Journaled File System -> Add a Standard Journaled File System
     ```

  2. Select the volume group *essvg* and specify the size of the file system and a mount point. Press **Enter** to create the file system.
  3. Change the owner of the file system (*/newFS*) to the appropriate Oracle user (*oracle92* in this example) and group **dba**:

     ```
     chown oracle92:/dba /NewFS
     ```

  4. Run the **smitty vg** command to verify that the file system was created correctly:

     ```
     ->List all File Systems
     ```

  5. Start up the database on the production system with the Oracle **sqlplus** command.
  6. Run the following Oracle SQL command:

     ```
     SQL> select status from v$instance;
     ```

  7. If the database has not started, run the following Oracle SQL command:

     ```
     SQL> startup mount
     ```

  8. Run the following series of Oracle SQL commands to recover the database:

     ```
     SQL> alter database create datafile '/NewFS/dphw_testfile';
     ```

```
SQL> recover datafile '/NewFS/dphw_testfile';
```

```
SQL> recover database
```

```
SQL> alter database open
```

9. Verify that the data was restored correctly with the following Oracle SQL command:

```
SQL> select phone from cust3 where id >10 and id<20;
```

Scenario 3: Snapshot restore for native Oracle databases:

This scenario demonstrates how to perform a snapshot restore of the Oracle database *myDB* when a file system was removed from the LUNs that *myDB* resides on since the database was originally backed up.

After running the `acsora -f restore` command, snapshot restore processing proceeds without interruption after determining that the configuration has changed (as a result of the new file system, */newFS*) since the database was originally backed up

Restoring a native Oracle database from Tivoli Storage Manager

Data Protection for Snapshot Devices backups are restored as an entire database (Restore Method One) or with datafile granularity (Restore Method Two). RMAN must be used to perform restore procedures.

Restore Method One (Entire Database):

Perform these tasks to restore Data Protection for Snapshot Devices backups as an entire database. (Restore Method One) or with datafile granularity (Restore Method Two).

Perform these steps to restore an entire database backup:

1. Shut down the database (if necessary):
   `shutdown;`
2. Mount the database:
   `startup mount;`
3. Start RMAN and connect to the target database and the recovery catalog:
   `rman target username/password rcvcat username/password@connect_string`
4. Perform an RMAN **run** command by specifying the allocation of channels and the restoration of the database:

```
run
{
allocate channel t1 type 'sbt_tape' parms
'ENV=(TDPO_OPTFILE=/usr/tivoli/tsm/client/oracle/bin/tdpo.opt)';
allocate channel t2 type 'sbt_tape' parms
'ENV=(TDPO_OPTFILE=/usr/tivoli/tsm/client/oracle/bin/tdpo.opt)';
allocate channel t3 type 'sbt_tape' parms
'ENV=(TDPO_OPTFILE=/usr/tivoli/tsm/client/oracle/bin/tdpo.opt)';
allocate channel t4 type 'sbt_tape' parms
'ENV=(TDPO_OPTFILE=/usr/tivoli/tsm/client/oracle/bin/tdpo.opt)';
restore database;
}
```

5. Recover the database (as needed) by connecting to the target database:

   ```
   recover database;
   ```

If your restore is not successful and you receive an error message, see the error log file (tdphw.log by default) for assistance.

Restore Method Two (Datafile Only):

Perform these tasks to restore Data Protection for Snapshot Devices backups with datafile granularity.

Perform the following steps to restore a datafile only:

1. Shut down the database (if necessary):

   ```
   shutdown;
   ```

2. Mount the database:

   ```
   startup mount;
   ```

3. Start RMAN and connect to the target database and the recovery catalog:

   ```
   rman target username/password rcvcat username
     /password@connect_string
   ```

   The RMAN command in the above example is divided to accommodate page formatting. The actual RMAN command string is on one line.

4. Perform an RMAN **run** command by specifying the allocation of channels and the restoration of the datafile *n*, where *n* is the number of the datafile:

   ```
   run
   {
   allocate channel t1 type 'sbt_tape' parms
   'ENV=(TDPO_OPTFILE=/usr/tivoli/tsm/client/oracle/bin/tdpo.opt)';
   allocate channel t2 type 'sbt_tape' parms
   'ENV=(TDPO_OPTFILE=/usr/tivoli/tsm/client/oracle/bin/tdpo.opt)';
   allocate channel t3 type 'sbt_tape' parms
   'ENV=(TDPO_OPTFILE=/usr/tivoli/tsm/client/oracle/bin/tdpo.opt)';
   allocate channel t4 type 'sbt_tape' parms
   'ENV=(TDPO_OPTFILE=/usr/tivoli/tsm/client/oracle/bin/tdpo.opt)';
   restore datafile n;
   }
   ```

5. Bring the datafile online with the following SQL command, where *n* is the number of the datafile:

   ```
   alter database datafile n online;
   ```

6. Recover the datafile as needed by connecting to the target database and issuing:

   ```
   recover datafile n;
   ```

If your restore is not successful and you receive an error message, see the error log file for assistance.

Chapter 6. Data Protection for Snapshot Devices commands and scripts

A list of various commands and scripts that are used with Data Protection for Snapshot Devices operations is provided.

Data Protection for Snapshot Devices commands and scripts

This section describes the command entries used to run the various components of Data Protection for Snapshot Devices:

Table 37. Summary of Data Protection for Snapshot Devices commands and scripts

Command	**Description**
Setup script	"Installation setup script" on page 134
Management Agent (acsd)	"Management Agent (acsd)" on page 138
Device Agent for CIM Devices (acscim)	"Device Agent for CIM Devices (acscim)" on page 141
Device Agent for N Series Devices (acsnsan, acsnnas)	"Device Agent for N Series Devices (acsnsan, acsnnas)" on page 143
Device Agent for IBM XIV® Storage System Devices (acsxiv)	"Device Agent for IBM XIV® Storage System Devices (acsxiv)" on page 145
Offload Agent ('tsm4acs')	"Data Protection for Snapshot Devices Offload Agent (tsm4acs)" on page 154
(Oracle) Snapshot Object Manager (acsutil)	"Snapshot Object Manager for Oracle (acsutil)" on page 149
(Oracle) Production system user interface (acsora)	"Production System User Interface for Data Protection for Snapshot Devices for Oracle (acsora)" on page 147
(SAP with Oracle) Data Protection for Snapshot Devices for *SAP® with Oracle* (backint)	"Data Protection for Snapshot Devices for *SAP® with Oracle* ('backint')" on page 151

(DB2) The following commands are provided by DB2 Advanced Copy Services. Refer to the DB2 *Command Reference* for detailed descriptions:

- `db2 backup database ... use snapshot...` (DB2 snapshot backup)
- `db2 restore database ... use snapshot ...` (DB2 snapshot restore)
- `db2acsutil` (DB2 utility for DB2 Advanced Copy Services)
- `db2adutl` (DB2 utility for the native TSM agent)

Unless otherwise stated, file and directory specifications in the following commands must be fully qualified names. As a general rule, relative names are, not supported.

Installation setup script

The setup script for each database variant provides several action options which are usually employed internally by the Data Protection for Snapshot Devices installer. It is also used without options to perform the manual Data Protection for Snapshot Devices setup and basic configuration.

The syntax is:

```
setup_<database>.sh [-a action
                           -d <DB2 instance directory>
                           -u <Instance user ID name>
                           -g <Instance primary group name>]
```

You can use the setup script for the following purposes:

- Activation or upgrade of TSM for ACS for one instance, as root:

  ```
  setup_<database>.sh –a install –d <INST_DIR> -u <user> -g <group>
  ```

- Initial configuration and reconfiguration:

  ```
  setup_<database>.sh
  ```

- Stopping an activated instance:

  ```
  setup_<database>.sh –a stop –d <INST_DIR>
  ```

- Starting an activated instance:

  ```
  setup_<database>.sh –a start –d <INST_DIR>
  ```

- Deinstallation of a stopped instance:

  ```
  setup_<database>.sh –a disable –d <INST_DIR>
  ```

All of these commands can be executed on either the production or backup system. In order to completely stop or disable TSM for ACS, the appropriate command needs to be executed first on the production system and then on the backup system (in that order).

(DB2) The script must be run as the DB2 instance owner from the DB2 Advanced Copy Services installation directory (<DB2 instance directory>/acs). The default action (`'setup'`) is performed and the DB2 instance is configured (see "Data Protection for Snapshot Devices installation procedure" on page 91).

If the script is called without parameters, it can be executed as the root or instance owner. It creates a new profile or modifies an existing one and updates `/etc/inittab` according to the current profile (production system) or user preference (backup system). Updates to inittab require starting and stopping TSM for ACS as intermediate steps. This call cannot stop TSM for ACS on the backup system if it is still running on the production system and the binaries in the instance-specific installation directory are NFS-shared between the production and backup systems. If TSM for ACS cannot be stopped you will need to stop TSM for ACS on the production system before executing the script with the `-a install` option..

Note: Configuration with the setup script is optimized for environments where the configuration directory is an NFS share among all production and backup system nodes, but the instance-specific installation directory is an NFS share only among production system nodes and is not shared among the production and backup systems. In this case the script can be invoked on the master production system and backup system nodes independently.

Possible values of `'database'`are

db2
Configures Data Protection for Snapshot Devices for DB2 Advanced Copy Services.

ora
Configures Data Protection for Snapshot Devices for Oracle.

sapora
Configures Data Protection for Snapshot Devices for *SAP® with Oracle*

Possible values of `'action'` are:

disable

This call can be executed as the root or instance owner. It stops TSM for ACS and removes all entries from /etc/inittab. In order to reactivate TSM for ACS, you need to call the script without paramters.

Note that this call cannot stop TSM for ACS on the backup system if it is still running on the production system and the binaries in the instance-specific installation directory are NFS-shared between the production and backup systems. If TSM for ACS cannot be stopped you need to stop TSM for ACS on the production system before executing `setup_<database>.sh –a install`.

install

This call needs to be executed with the root user ID. It performs the following:

1. Stops TSM for ACS (`setup_<database>.sh –a stop`)
2. Copies all binary files from the global installation directory to the instance-specific installation directory
3. Sets the appropriate access rights for the binary files
4. Restarts TSM for ACS (`setup_<database>.sh –a start`)

The steps to start and stop TSM for ACS are skipped if TSM for ACS has not yet been configured.

This call cannot stop TSM for ACS on the backup system if it is still running on the production system and the binary files in the instance-specific installation directory are NFS-shared between the two systems. If TSM for ACS cannot be stopped you need to stop TSM for ACS on the production system before executing `setup_<database>.sh –a install`.

start

This call can be executed as the root or instance owner. It starts a previously installed and configured version of TSM for ACS. This call creates different entries in /etc/inittab depending on whether the call is executed on the backup or production system.

stop

This call can be executed as the root or instance owner. It stops the version of TSM for ACS that is currently running. This call updates /etc/inittab and checks that TSM for ACS has been stopped successfully (a write lock can be acquired for the .lock file that is located in the instance-specific install directory).

This call will fail on the backup system in environments where the instance-specific installation directory is shared between the production and backup systems, if TSM for ACS is still running on the production system. In order to stop TSM for ACS in those environments successfully, you need to first stop TSM for ACS on the production system.

(DB2) The instance directory name (’-d’ option) is required for all explicit actions. It is not required for the default setup function.

The options ’-u’ and ’-g’ are not currently used.

Options for DB2 Advanced Copy Services and Data Protection for Snapshot Devices commands

Specify these options in the OPTIONS field of commands or in a file specified by the OPTIONS field.

Table 38. Options Available

Device Applicability							**Parameter**		
DS	**SVC**	**ESS**	**N Series (SAN)**	**N Series (NAS)**	**Used by DB2 ACS**	**XIV®**	**Name**	**Value or Action if specified**	**Default value or Action if not specified**
x	x	x	x	x	x	x	PROFILE	Absolute path and file name of profile	$ACS_DIR/profile
x	x	x			x		FLASHCOPY_TYPE	COPY, INCR, NOCOPY See “Data Protection for Snapshot Devices profile parameters” on page 164 for a description of this parameter. INCR and NOCOPY are available only with Data Protection for Snapshot Devices.	COPY
x	x	x	x	x		x	TSM_BACKUP (TSM_BACKUP_ FROM_SNAPSHOT)	Perform a Tivoli Storage Manager backup	Do not perform a Tivoli Storage Manager backup
x	x	x	x	x	x	x	DELETE_FORCE	See note.	FlashCopy relations remain active when backup is deleted.
x	x	x	x	x	x	x	DEVICE_CLASS	*device_section_name* in profile.	STANDARD

Note:

1. (DELETE_FORCE) Applies to db2acsutil only:
   - In conjunction with ’db2acsutil delete’, withdraws any FlashCopy relations currently in effect for the target set represented by the backup (applicable to CIM devices only). A manual withdraw of FlashCopy relations is needed in case of a restore when multiple target sets are in use and at least one target set other than the one to be restored is in a NOCOPY or INCR FlashCopy relation.
   - In conjunction with ’db2acsutil query’, also lists backups deleted without the DELETE_FORCE option.

Related concepts

"Options parameters"
Command line options of the snapshot-related commands allow options to be given in the command line or in an external file.

Options parameters

Command line options of the snapshot-related commands allow options to be given in the command line or in an external file.

(DB2) The OPTIONS parameter has the following components:

options-string
One or more vendor options in the form 'parameter=value' (or simply 'parameter' if the parameter has no value or the value is 'YES'), separated by a space. Multiple options must be enclosed in single or double quotes. The string (without the quotes) is passed to the software that processes the respective command.

file-name
Fully qualified name of a vendor options file (on the DB2 server) that contains the options.

The DB2 VENDOROPT configuration parameter cannot be used to specify vendor options for DB2 ACS snapshot backups and restores.

(SAP for Oracle) Options corresponding to the profile parameters are specified in the BR*Tools commands and passed to the backint interface:

- -O (equivalent to TSM_BACKUP_FROM_SNAPSHOT)
- -C (equivalent to FLASHCOPY_TYPE)
- -S (equivalent to DEVICE_CLASS)

Related reference

"Options for DB2 Advanced Copy Services and Data Protection for Snapshot Devices commands" on page 136

"Data Protection for Snapshot Devices for *SAP® with Oracle* ('backint')" on page 151
Data Protection for Snapshot Devices uses the BR*Tools executable file ('backint') on SAP with Oracle environments.

Management Agent (acsd)

The Management Agent (acsd) coordinates the snapshot backup operation.

The Management Agent (acsd) controls the backup flow and mediates between the other agents. The Management Agent also provides access to the snapshot backup repository, which contains information about the valid snapshot backups and their relationships to snapshot capable storage devices.

(DB2) acsd must be started as the DB2 instance owner.

Syntax for invoking acsd as a daemon process:

```
>>—acsd——┬────────────────────┬──┬─────────────────┬──┬──────────────────────┬──┬─────────────────────┬——————————><
         └─-p—acsd-profile────┘  └─-c—acsd-port────┘  └─-r—acs-repository───┘  └─-d—acs-directory───┘
```

```
►─┬────┬─┬──────────────────┬────────────────────────────────────────────────►
  └─-t─┘ └─-b─password-file─┘

►─┬─────────────────────────────────────────────────────────────────────┬────►◄
  └─-a─administration-assistant-server─┬──────────────────────────────┬─┘
                                       └─:─administration-assistant-port─┘
```

Syntax for obtaining version or help information:

```
►►─acsd─┬────┬─┬────┬────────────────────────────────────────────────────────►◄
        └─-v─┘ └─-h─┘
```

Table 39. Options for Starting the Management Agent (acsd) as a Daemon Process

Option	Description	Default	Overrides Profile Parameter
-p acsd-profile	Full path and name of the profile used by the management agent. The Management Agent uses the 'GLOBAL' and 'acsd' sections of the profile.	<DB2 instance directory>/acs/profile	
-c acsd-port	TCP/IP port number or service name on which the management agent is listening	57328	ACSD (port number or service name)
-r acs-repository	Directory name where the snapshot backup repository is located	None.	ACS_REPOSITORY
-d acs-directory	Name of ACS directory	<ACS_DIR>	
-t	Turn trace on	Trace off	TRACE
-b password-file	File in which the DB2 Advanced Copy Services management agent password is stored (in encrypted form). See notes.	<ACS_DIR>/shared/pwd.acsd	(No corresponding profile parameter.)
-a administration-assistant-server	(SAP) Host name of the server on which the Administration Assistant is running	None.	ADMIN_ASSISTANT (hostname)
administration-assistant-port	(SAP) TCP/IP port on which the Administration Assistant is listening	None.	ADMIN_ASSISTANT (port number)
-v	Display version and help information	None.	N/A
-h	Display help information only	None.	N/A

All parameters override the values specified in the acsd-profile or the corresponding default values. The **shared** and **logs** directories will be automatically created in ACS_DIR. If no parameters are entered, acsd starts with the default profile and using default parameter values where applicable, or it issues an error message if this profile does not exist.

(DB2) When a user installs DB2 and creates a DB2 instance, the Management Agent (acsd) will be copied to <DB2 instance directory>/acs. To activate DB2 ACS (or DP for Snapshot Devices), the user must start the setup script as the DB2 instance owner from this same directory. This script will create two entries in /etc/inittab. The Management Agent (acsd) will thereby be started automatically from /etc/inittab without any command line arguments. In this case the default values will be used for configuring the Management Agent (acsd). The default values can be overridden by providing a profile. By default, this is located in the directory `<DB2 instance directory>/acs`.

Use the following syntax to change the passwords for communication between acsd and the storage devices.

```
►►──acsd── -f password──┬──────────────────────────────────────────────────────────────────────────┬──────────►
                        ├─ -p──acsd-profile──┬───────────────────────────┬─┬──────────────────┬─────┤
                        │                    │  ┌─,───────────────────┐  │ └─master-password──┘     │
                        │                    │  ▼                     │  │                          │
                        │                    └────section──:──password─┴──┘                          │
                        │                      ┌─,──────────────────┐                                │
                        │                      ▼                    │                                │
                        └─ -b──password-file────section──:──password─┴──master-password──────────────┘

►──┬─────────────────┬──┬──────────────────────┬──┬───────────────────────┬──┬──────┬──────────────────────►
   └─ -c──acsd-port──┘  └─ -r──acs-repository──┘  └─ -d──acs-directory──┘  └─ -t──┘

►──┬─────────────────────────────────────────────────────────────────────────────────┬────────────────────►◄
   └─ -a──administration-assistant-server──┬───────────────────────────────────────┬──┘
                                           └─:──administration-assistant-port──┘
```

Table 40. Options for Starting the Management Agent (acsd) (Password Function)

Option	Description	Default	Overrides Profile Parameter
-f password	Set or change passwords		
-p acsd-profile	Full name of the profile used by the management agent. See note.	See “Management Agent (acsd)” on page 138.	See “Management Agent (acsd)” on page 138.
-b password-file	Name of the file the management agent uses to store the encrypted passwords. See note.	See “Management Agent (acsd)” on page 138.	
section:password	Device section name in the profile and password for the device specified in that section.	See note.	
master-password	Master password used to authenticate a library or agent to the management agent	See note	

Table 40. Options for Starting the Management Agent (acsd) (Password Function) (continued)

Option	Description	Default	Overrides Profile Parameter
-c acsd-port	See "Management Agent (acsd)" on page 138..		
-r acs-repository			
-d acs-directory			
-t			
-a administration-assistant-server			
administration-assistant-port			

Notes:

1. Passwords: If either password entry is omitted in conjunction with the '-p' option, acsd will ask interactively for
   - the passwords for all sections in the given profile and/or
   - the master password

   acsd will also ask for all of these passwords interactively if neither '-p' nor '-b' is specified.

When acsd is started for the first time, or with a new ACS_DIR parameter, it will

- create the subdirectories 'shared' and 'logs'
- create a password file pwd.acsd in the 'shared' subdirectory
- generate a master password.

As long as the Snapshot Backup Library uses the same ACS_DIR, it can authenticate itself to acsd with the password provided in the pwd.acsd file. If the Snapshot Backup Library uses a different ACS_DIR, the default password file pwd.acsd must be copied to that directory so that the library can read the master password from that directory.

Related concepts

"Data Protection for Snapshot Devices profile description" on page 160
Data Protection for Snapshot Devices relies on a profile in order to operate properly.

Device Agent for CIM Devices (acscim)

The Device Agent for CIM Devices (acscim) is the snapshot-device-specific component that invokes the snapshot command.

The Device Agent for CIM Devices invokes the snapshot command on a snapshot capable device using the CIM interface (ESS800, DS6000, DS8000 and SAN Volume Controller). Device agents are also used to update progress and usability information about the corresponding snapshot backup that is stored in the (local) snapshot backup repository. The Device Agent for CIM Devices is loaded when the value of COPYSERVICES_HARDWARE_TYPE is DS8000, DS6000, ESS800, or SAN Volume Controller.

```
►►──acscim──┬───────────────┬──┬─────────────────────────────────────┬──┬────────────────────┬──────────►
            └─ -p──profile──┘  └─ -c──acsd-hostname──┬────────────┬──┘  └─ -s──device-class──┘
                                                     └─:──acsd-port─┘
```

```
►─┬──────────────────┬─┬────┬─┬────┬─┬────┬─┬──────────────────┬──────────────────►
  └─-l─acs-directory─┘ └─-D─┘ └─-M─┘ └─-t─┘ └─-d─database-name─┘

►─┬──────────────────────┬─┬──────────────┬─────────────────────────────────────────►◄
  └─-a─filter-arguments──┘ └─-T─timestamp─┘
```

Syntax for obtaining version or help information:

```
►►─acscim─┬────┬─┬────┬──────────────────────────────────────────────────────────►◄
          └─-v─┘ └─-h─┘
```

Table 41. Options for Starting the Device Agent for CIM Devices (acscim)

Option	Description	Default
-p profile	Full profile name. The device agent uses the • GLOBAL • CLIENT • *'device'* • OFFLOAD • ORACLE sections of the profile.	<DB2 instance directory>/acs/profile
-c acsd-hostname	Name of the server where the management agent (acsd) is running	localhost
acsd-port	TCP/IP port number or service name on which the management agent (acsd) is listening	57328
-s device-class	Section in the profile that pertains to the device class	STANDARD
-l acs-directory	Directory where the 'logs' and 'shared' directories can be found.	<ACS_DIR>
-D	Start as daemon The '-a' option defines which usability states the device agent will respond to. Valid only when started from /etc/inittab.	Run and terminate
-t	Turn trace on	<TRACE>
-d database-name	DB2 database name	All database names.
-a filter-arguments	Decimal value representing one or more backup usability states (see "Usability states" on page 35). Only entries with the indicated states are considered. The value of this option is the sum of the numeric values given in table "Usability states" on page 35 for the desired states.	All usability states applicable to context of request.
-T timestamp	A backup ID to which an operation (delete, background monitoring) is to apply.	None.

Table 41. Options for Starting the Device Agent for CIM Devices (acscim) (continued)

Option	Description	Default
-M	Start the device agent as a ″mount agent″. This agent will force the mounting of the target volumes on the backup system in case of database files residing on JFS filesystems or on AIX LVM mirrored volumes. Such a mount verifies the consistency of the associated filesystems.	Start as ″monitoring agent″.
-v	Display version and help information	None.
-h	Display help information only	None.

The return code of the device agent will be 0 if it finishes the request without errors or if there were no candidates for the request. Return code 1 indicates that an error occurred during the process.

Device Agent for N Series Devices (acsnsan, acsnnas)

The Device Agent for N Series Devices (acsnsan or acsnnas) is the snapshot-device-specific component that invokes the snapshot command.

The Device Agent for N Series Devices (acsnsan or acsnnas) invokes the snapshot command on a snapshot capable device using the ONTAPI interface (for example, NetApp or IBM N Series). Device agents are also used to update usability information about the corresponding snapshot backup that is stored in the (local) snapshot backup repository. The appropriate Device Agent for N Series Devices (acsnsan or acsnnas) is loaded when the value of COPYSERVICES_HARDWARE_TYPE is SAN_NSERIES or NAS_NSERIES, respectively.

```
►►──┬─acsnsan─┬──┬──────────────┬──┬────────────────────────────────────┬──┬──────────────────┬──────►
    └─acsnnas─┘  └─ -p──profile─┘  └─ -c──acsd-hostname──┬──────────────┬─┘  └─ -s──device-class─┘
                                                          └─:──acsd-port─┘

►──┬─────────────────────┬──┬────┬──┬────┬──┬────┬──┬──────────────────┬─────────────────────────────►
   └─ -l──acs-directory─┘  └─ -D─┘  └─ -M─┘  └─ -t─┘  └─ -d──database-name─┘

►──┬─────────────────────────┬──┬──────────────────┬──────────────────────────────────────────────►◄
   └─ -a──filter-arguments─┘  └─ -T──timestamp─┘
```

Syntax for obtaining version or help information:

```
►►──┬─acsnsan─┬──┬────┬──┬────┬───────────────────────────────────────────────────────────────────►◄
    └─acsnnas─┘  └─ -v─┘  └─ -h─┘
```

Table 42. Options for the Device Agent for N Series Devices (acsnsan/acsnnas) Command

Option	**Description**	**Default**
-p profile	Full profile name. The device agent uses the • GLOBAL • CLIENT • *′device′* • OFFLOAD • ORACLE sections of the profile.	See “Device Agent for CIM Devices (acscim)” on page 141.
-c acsd-hostname	Name of the server where the management agent (acsd) is running	
acsd-port	TCP/IP port number or service name on which the management agent (acsd) is listening	
-s device-class	Section in the profile that pertains to the device	
-l acs-directory	Directory where the executable files, logs, and shared directories can be found.	
-D	Start as daemon. The ′-a′ option defines which usability states the device agent will respond to. Valid only when started from /etc/inittab.	
-t	Start with trace on	
-d database-name	DB2 database name	
-a filter-arguments	Decimal value representing one or more backup usability states (see “Usability states” on page 35). Only entries with the indicated states are considered. The value of this option is the sum of the numeric values given in “Usability states” on page 35 for the desired states.	
-T timestamp	A backup ID to which an operation (delete, background monitoring) is to apply.	
-M	Start the device agent as a ″mount agent″. This agent will force the mounting of the target volumes on the backup system in case of database files residing on JFS filesystems or on AIX LVM mirrored volumes. Such a mount verifies the consistency of the associated filesystems.	Start as ″monitoring agent″.
-v	Display version and help information	See “Device Agent for CIM Devices (acscim)” on page 141.
-h	Display help information only	See “Device Agent for CIM Devices (acscim)” on page 141.

The return code of the device agent will be 0 if it finishes the request without errors or if there were no candidates for the request. Return code 1 indicates that an error occurred during the process.

Device Agent for IBM XIV® Storage System Devices (acsxiv)

The Device Agent for IBM XIV® Storage System Devices (acsxiv) is the component that invokes a snapshot command on a snapshot capable device using XivAdapter.jar.

This agent is also used to update usability information about the corresponding snapshot backup that is stored in the (local) snapshot backup repository. The XIV Adapter is used in conjunction with the Device Agent for IBM XIV® Storage System Devices (acsxiv). It communicates with acsxiv and issues commands to the XIV® command line interface (xcli). The appropriate Device Agent for IBM XIV® Storage System Devices (acsxiv) is loaded when the value of COPYSERVICES_HARDWARE_TYPE is XIV.

```
►►──acsxiv──┬────────────┬──┬──────────────────────────────────┬──┬──────────────────┬─────────►
            └─-p──profile─┘  └─-c──acsd-hostname──┬──────────────┬─┘  └─-s──device-class─┘
                                                  └─:──acsd-port─┘

►──┬───────────────────┬──┬────┬──┬────┬──┬────┬──┬──────────────────┬──────────────────────────►
   └─-l──acs-directory─┘  └─-D─┘  └─-M─┘  └─-t─┘  └─-d──database-name─┘

►──┬──────────────────────┬──┬──────────────┬──────────────────────────────────────────────────►◄
   └─-a──filter-arguments─┘  └─-T──timestamp─┘
```

Syntax for obtaining version or help information:

```
►►──acsxiv──┬────┬──┬────┬─────────────────────────────────────────────────────────────────────►◄
            └─-v─┘  └─-h─┘
```

Table 43. Options for the Device Agent for IBM XIV® Storage System Devices (acsxiv) Command

Option	Description	Default
-p profile	Full profile name. The device agent uses the • GLOBAL • CLIENT • *’device’* • OFFLOAD • ORACLE sections of the profile.	<DB2 instance directory>/acs/profile
-c acsd-hostname	Name of the server where the management agent (acsd) is running	
acsd-port	TCP/IP port number or service name on which the management agent (acsd) is listening	
-s device-class	Section in the profile that pertains to the device	
-l acs-directory	Directory where the executable files, logs, and shared directories can be found.	
-D	Start as daemon. The ’-a’ option defines which usability states the device agent will respond to. Valid only when started from /etc/inittab.	
-t	Start with trace on	
-d database-name	DB2 database name	
-a filter-arguments	Decimal value representing one or more backup usability states (see “Usability states” on page 35). Only entries with the indicated states are considered. The value of this option is the sum of the numeric values given in “Usability states” on page 35 for the desired states.	
-T timestamp	A backup ID to which an operation (delete, background monitoring) is to apply.	
-M	Start the device agent as a ″mount agent″. This agent will force the mounting of the target volumes on the backup system in case of database files residing on JFS filesystems or on AIX LVM mirrored volumes. Such a mount verifies the consistency of the associated filesystems.	Start as ″monitoring agent″.
-v	Display version and help information	
-h	Display help information only	

The return code of the device agent will be 0 if it finishes the request without errors or if there were no candidates for the request. Return code 1 indicates that an error occurred during the process.

Disk Mapper Script (acsdm.sh)

The Disk Mapper script provides mapping information.

The Disk Mapper (acsdm.sh) is a shell script that provides information such as a mapping of DS storage system volume serial numbers to AIX vpaths and hdisks. This script is called by the DB2 Advanced Copy Services device agent for the snapshot backup and restore cases.

Volume Group Takeover Script (acsvg.sh)

The Volume Group Takeover Script (acsvg.sh) is used in high-availability situations only.

The Volume Group Takeover script (acsvg.sh) applies only to SAN configurations on AIX systems. It is used only in special high-availability scenarios in which customers use enhanced concurrent capable volume groups on their production systems. In these cases, this script will export volume groups and import them again on an HACMP takeover system after a snapshot restore has been performed. This is necessary to synchronize the AIX ODM on the production and HACMP takeover systems.

XIV Adapter Java Archive (XivAdapter.jar)

The XIV Adapter is used in conjunction with the Device Agent for IBM XIV® Storage System Devices (acsxiv).

XivAdapter.jar communicates with acsxiv and issues commands to the XIV® command line interface (xcli).

Production System User Interface for Data Protection for Snapshot Devices for Oracle (acsora)

The production system user interface (acsora) performs commands on a native Oracle environment.

The acsora syntax is as follows:

```
acsora [-p profile]-f <function> [-b backupID] [-F]

where <function> is one of:
        backup
        restore
        delete
        inquire
```

Option	Description	Default	Overrides Profile Parameter
-p acsd-profile	Full path and name of the profile used by the Management Agent The Management Agent uses the 'GLOBAL' and 'ACSD' sections of the profile.	<ACS_DIR>/profile	

Option	Description	Default	Overrides Profile Parameter
-b backupID	Backup ID for restore, delete, inquire functions		
-f backup	Backup database		
-f restore	Restore database		
-f delete	Delete snapshot backup		
-f inquire	List snapshot backups		
-F	In conjunction with ’-f delete’: withdraw source/target relations		

-f backup

This command backs up the Oracle database according to the profile settings:

1. On the production system, you must specify the profile name.
2. On the backup system, you must specify the production host name.

Example (backup database):

```
acsora -f backup
```

-f restore

This command restores the Oracle database from the backup specified by the backup ID, or the latest backup.

The Oracle database is available for immediate use after performing a snapshot restore and a roll forward recovery. However, background copy processing from the target volumes to the source volumes may require additional time to complete, especially if FLASHCOPY_TYPE COPY is specified. Although the database is available, you cannot perform a Data Protection for Snapshot Devices backup until background copy processing completes.

Note that restore processing fails when Data Protection for Snapshot Devices determines that new FlashCopy storage device volumes have been added to the database (and corresponding target volumes have been added to the target volumes file) when volumes are already in an existing incremental relationship.

Example (restore specified backup):

```
acsora -f restore -b B01
```

See “Restoring a native Oracle database from Tivoli Storage Manager” on page 130 and “Restoring a native Oracle database” on page 127 for detailed instructions on how to restore your Oracle database.

-f inquire

This command lists the details for the snapshot backup denoted by the backup ID (if entered), or all backups.

Example (list all backups):

```
acsora -f inquire
```

-f delete

This command deletes the snapshot backup denoted by the entered backup ID.

Example (deleted specified backup):

```
acsora -f delete -b B01
```

Snapshot Object Manager for Oracle (acsutil)

The Snapshot Object Manager for Oracle (acsutil) provides a snapshot backup query and restore interface for native Oracle environments..

Functions of the ’acsutil’ command

The Snapshot Object Manager for Oracle (acsutil) provides a front-end for acsora to show available backups, perform restores, and delete unwanted backups. It communicates with acsora via input and output files.

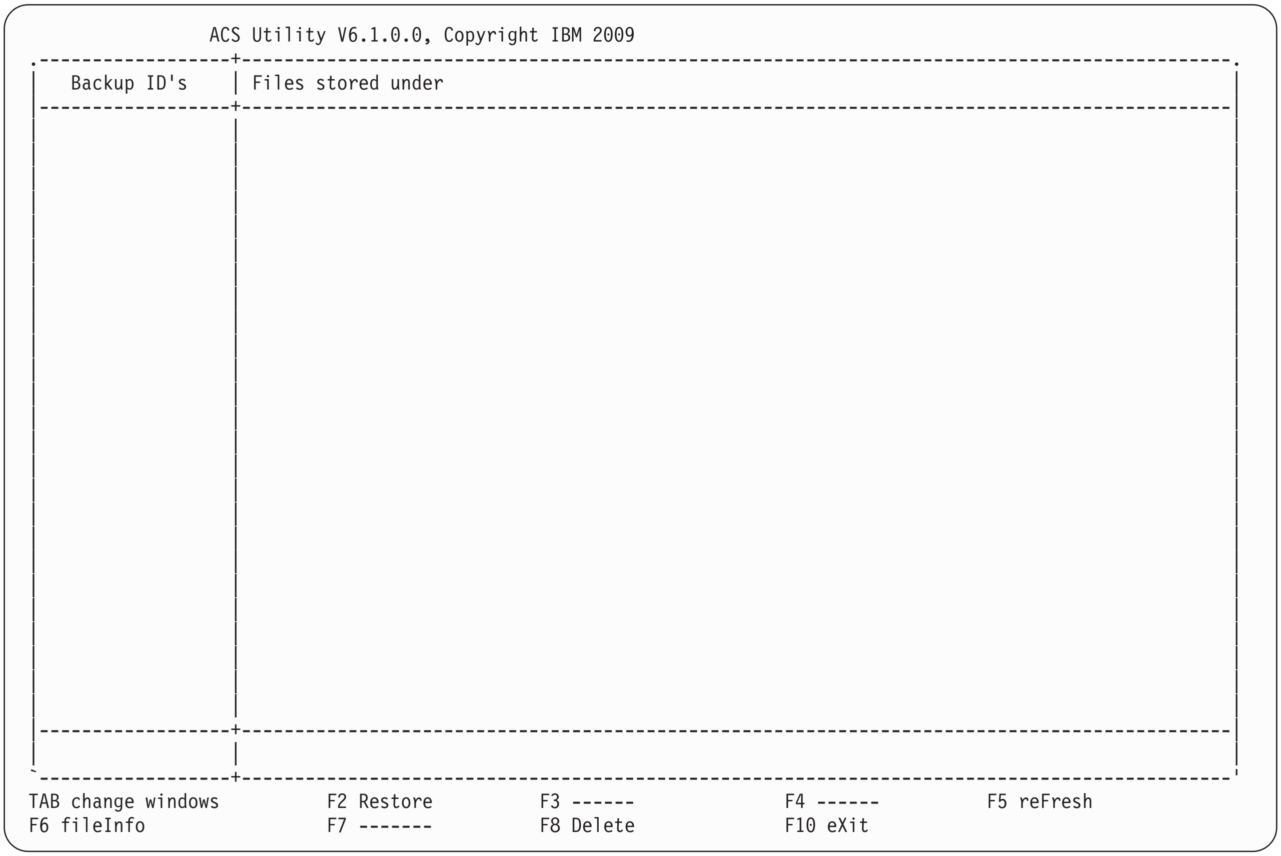
Syntax of the ’acsutil’ command

```
acsutil [-p <profile>]
```

Parameter	Description	Default
-p profile	Data Protection for Snapshot Devices profile	Standard profile

The Snapshot Object Manager user interface consists of a split window, which is character based.

The first step is an automatic inquire operation for all backup IDs. The following figure shows the screen layout for the list of backup IDs found by the Snapshot Object Manager when the inquiry is complete.



```
                 ACS Utility V6.1.0.0, Copyright IBM 2009
.------------------+---------------------------------------------------------------------------------------------.
|   Backup ID's    | Files stored under                                                                          |
|------------------+---------------------------------------------------------------------------------------------|
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|                  |                                                                                             |
|------------------+---------------------------------------------------------------------------------------------|
|                  |                                                                                             |
`------------------+---------------------------------------------------------------------------------------------'
TAB change windows          F2 Restore          F3 ------              F4 ------          F5 reFresh
F6 fileInfo                 F7 -------          F8 Delete              F10 eXit
```

All backup IDs found in the ACS repository are shown on the left. To the right of each backup ID, all the files belonging to that backup ID are displayed. You can select individual backup IDs

If you mark the backup ID you are interested in and then press the Tab key to move the cursor to the right-hand panel, all file names belonging to the marked backup ID will be displayed.

Up, Down, Left, Right - Move cursor
Move the highlighted cursor in the direction indicated on the key.

Tab - Switch window side
Move the cursor between the left and right sides of the window.

F2 - Restore
Restore the marked backup ID.

F5 - Refresh
Refresh the list of backup IDs and file names.

F6 - Fileinfo
Opens a separate window to display file information.

For backup IDs, the sequence number (backup version count) is shown.

F8 - Delete
Delete the selected backup ID and all corresponding files.

F10 - Exit
Exit from Snapshot Object Manager

ENTER - Mark/unmark backup ID
Mark or unmark the backup ID below the cursor.

The Snapshot Object Manager can delete backup IDs with all included files. It is not possible to delete single files within a backup ID. To delete a backup ID it must be highlighted. After pressing F8 you have to confirm the deletion operation. The backup ID and all included files are deleted.

For each restore, a log file will be created.

Data Protection for Snapshot Devices for *SAP® with Oracle* ('backint')

Data Protection for Snapshot Devices uses the BR*Tools executable file ('backint') on SAP with Oracle environments.

In the normal case, Data Protection for Snapshot Devices is invoked by the BR*Tools utilities as the executable file 'backint' (in this implementation, a soft link) with a set of appropriate parameters.

For troubleshooting purposes, however, it is possible to call Data Protection for Snapshot Devices directly from the command line in order to perform data protection operations manually and thus be able to correct errors.

The command:

```
backint -?
```

displays a list of all possible command line options.

Note: For the C shell, enclose the option string in quotes (`backint '-?'`).

The syntax of the backint command is as follows:

```
backint  [-p profile]
         -f <function>
         -t <backup_type>
[        -n <negative_list> or '-n no_check'
        [-O] [-C] [-S]
```

Table 44. Parameters for Data Protection for Snapshot Devices Invocation as 'backint'

Option	Meaning	Default
-p	SAP® Backint profile (see "SAP® backint profile overview" on page 192)	
-f backup	Backup function	
-f restore	Restore function	
-f inquire	Inquire function	
-f delete	Delete function	
-t volume	Type of backup is volume (snapshot)	
-t volume_online	Type of backup is volume (snapshot) with a minimized backup window for Oracle.	
-t file	Type of backup is file	

Table 44. Parameters for Data Protection for Snapshot Devices Invocation as 'backint' (continued)

Option	Meaning	Default
-t file_online	Type of backup is file online with locking	
-n <negative_list>	Name of exception file (*negative list*) providing directories and files to be included in the backup	
-n no_check	Disable validation of files to include in backup	
-O	Offload tape backup. Overrides the TSM_BACKUP_FROM_SNAPSHOT parameter.	Parameter value in profile, or default.
-C	Overrides the FLASHCOPY_TYPE parameter	Parameter value in profile, or default.
-S	Overrides the DEVICE_CLASS parameter	Parameter value in profile, or default.

-f backup

The **backup** function will normally be invoked by the SAP database utilities brbackup and brarchive. These programs give Data Protection for Snapshot Devices an input file (in the case of **backup** and **inquire**) containing the names and paths of the database files to be handled. For troubleshooting, however, it might be necessary to call this function of Data Protection for Snapshot Devices directly to restore individual files. See the following example.

```
backint -p /oracle/SID/dbs/init<SID>.utl -f backup -t volume
```

The backint profile `init<SID>.utl` has to be specified with the path and file name statement as shown above.

The program prompts you to enter one or more file names. Each successful backup run (collection of one or more files) is allocated its own backup ID within Tivoli Storage Manager

Remember to press CTRL + D after you enter the name of the file to be backed up.

-f restore

The **restore** function will be normally started by the SAP database utility brrestore. For troubleshooting, however, it might be necessary to call this function of Data Protection for Snapshot Devices directly to restore individual files. This function can be invoked from the command line as follows.

```
backint -p /oracle/SID/dbs/init<SID>.utl -f restore -t volume
```

You will be prompted to enter the backup ID and the full names of the files to be restored. If the files are to be restored to another directory, it is necessary to specify the path to the input files.

Caution: If a file is restored directly, any existing file with the same name will be overwritten without warning. Thus, it is recommended that you restore database files directly only in a very controlled manner, when it is absolutely necessary in order to remove an error. In normal operation you should never restore a database directly, because this could corrupt the SAP database.

-f inquire

The **inquire** function, normally invoked by BR*Tools and brrestore, will be used to query the Tivoli Storage Manager server for backup IDs or files which belong to a particular backup ID. For troubleshooting, however, it might be necessary to invoke this function manually from the command line as follows.

```
backint -p /oracle/SID/dbs/init<SID>.utl -f inquire -t volume
```

Data Protection for Snapshot Devices prompts you to enter the inquiry in one of four formats. These are:

1. **#NULL** - to display all backup IDs saved so far. A typical line of the response could be:

   ```
   #BACKUP JE0___A0DNE9Z74C
   ```

   The backup ID in this case is `JE0___A0DNE9Z74C` (`#BACKUP` is not part of the backup ID). The first six characters are the user defined prefix. The next 10 characters represent a unique ID of the backup.
2. **BackupID** - to display all of the files which belong to this backup ID. A typical result could be:

   ```
   ##BACKUP JE0___A0DNE9Z74C  /oracle/C21/dbs/initC21.utl.
   ```

3. **#NULL `filename`** - to display all of the backup IDs corresponding to this file. *Filename* requires an input consisting of path and name of the file.
4. **BackupID `filename`** - to verify whether a particular file has been saved under a certain backup ID. *Filename* requires an input consisting of path and name of the file.

-f delete

The **delete** function is used as part of the version control mechanism of Tivoli Storage Manager for ERP and can only be called by Data Protection for Snapshot Devices itself or by a user. The delete function allows you to delete full backups only.

This function can be invoked from the command line as follows:

```
backint -p /oracle/SID/dbs/init<SID>.utl -f delete -t volume
```

You will be prompted to enter the backup ID

Data Protection for Snapshot Devices Offload Agent (tsm4acs)

The Offload Agent provides a single user interface for all functionality associated with the IBM Tivoli Storage Manager for Advanced Copy Services package.

(DB2) In a DB2 environment, the Offload Agent is available with IBM Tivoli Storage Manager for Advanced Copy Services only.The purpose of the Offload Agent is to provide a single user interface for all added functionality associated with the IBM Tivoli Storage Manager for Advanced Copy Services package. This includes backup to Tivoli Storage Manager and additional functions for managing Tivoli Storage Manager backups.

(Oracle) The purpose of the Offload Agent is to provide a user interface for backup to Tivoli Storage Manager and additional functions for managing Tivoli Storage Manager backups.

```
►►──tsm4acs──┬───────────────┬──┬─────────────────────────────────────┬──┬──────────────────────┬──────►
             └─-p──profile───┘  └─-c──acsd_hostname──┬──────────────┬─┘  └─-l──acs-directory───┘
                                                     └─:──acsd_port─┘

►──┬────┬──┬────┬──┬─-f tape_backup────────┬──┬─────────────────────┬──┬─────────────────────┬──────►
   └─-D─┘  └─-t─┘  ├─-f mount──────────────┤  └─-i──instance-name───┘  └─-d──database-name───┘
                   └─-f unmount──┬────┬────┘
                                 └─-F─┘

►──┬────────────────────┬──────────────────────────────────────────────────────────────────────────►◄
   └─-T──snapshot-id────┘


►►──tsm4acs──┬────┬──┬────┬────────────────────────────────────────────────────────────────────────►◄
             └─-v─┘  └─-h─┘
```

Table 45. Options for the Data Protection for Snapshot Devices 'tsm4acs' Command

Option	Description	Default
-p profile	See "Device Agent for CIM Devices (acscim)" on page 141.	
-c acsd-hostname		
acsd-port		
-l acs-directory		
-f tape_backup	Back up a snapshot target set to Tivoli Storage Manager.	
-f mount	Mount snapshot target set	
-f unmount	Unmount snapshot target set	
-d database-name	(DB2) DB2 database name. Required for '-F' option.	No limitation
-T snapshot-id	Timestamp identifying a particular snapshot to which the operation is to apply. Required for '-F' option. Do not use in conjunction with '-f tape_backup'.	No limitation.
-i instance-name	Instance name to apply to the command. Required for '-F' option.	No limitation.

Table 45. Options for the Data Protection for Snapshot Devices 'tsm4acs' Command (continued)

Option	Description	Default
-D	Run as daemon process. Valid only when started from /etc/inittab.	Run and terminate.
-F	Force a reset of usability states for the specified snapshot backup. This parameter also requires the • -d database-name • -i instance-name • -T snapshot-id parameters.	None.
-t	Start with trace on.	Trace off
-v	Display version.	
-h	Display help text.	

The tsm4acs process connects to the Management Agent (acsd) process and performs the function specified with the '-f' option. After executing the appropriate operation, tsm4acs notifies acsd, which then updates the snapshot backup repository accordingly. When started as a daemon (-D option), as is the case for the standard /etc/inittab entry, tsm4acs will perform offloaded tape backup operations. This will result in a synchronous tape backup of all snapshot backups. As soon as a new snapshot is started with TSM_BACKUP, the offload agent will start to back it up to tape when it becomes available for mounting on a backup system (REMOTELY_MOUNTABLE).

(DB2) The snapshot backups for all participating partitions must have completed before the tape backup process is started.

The return code of the Offload Agent will be 0 if it finishes the request without an error or if there were no candidates for the request. Further, the return code will be 1 if one or more minor issues occurred which are not critical but should be checked to prevent major issues later. Return code 2 indicates that an error occurred during the command execution.

The following sections describe the details of the various functions specified with the '-f' option of the Data Protection for Snapshot Devices command **tsm4acs**.

-f tape_backup

This Offload Agent command backs up data to tape storage.

Note: Tivoli Storage Manager for ERP in the case of SAP with Oracle or SAP with DB2 or TSM for Databases (Data Protection for Oracle) for native Oracle must have been installed on the backup server.

To create a snapshot backup with a subsequent tape backup, TSM_BACKUP (or TAPE_BACKUP_FROM_SNAPSHOT) must be specified either as part of the backup command or as a profile parameter, thus applying to all backups. The management agent will update the usability state with TAPE_BACKUP_PENDING. The IBM Tivoli Storage Manager for Advanced Copy Services offload agent will then pick up all data containers in the state TAPE_BACKUP_PENDING and back them up to tape.

Note: (DB2) Only snapshot backups generated by Data Protection for Snapshot Devices V5.5 or above can be processed.

Note: (Oracle) Only snapshot backups generated by Data Protection for Snapshot Devices V6.1 or above can be processed.

To start the Offload Agent with the tape backup task, enter the command

```
tsm4acs -f tape_backup
```

By specifying additional options (filter arguments) such as

```
-i instance-name
-d database-name
```

the appropriate backup for the given instance and or database can be selected for off-loading to tape. The ″-T snapshot-id″ option should not be specified in conjunction with ″-f tape_backup″. The backups should be processed in chronological order. tsm4acs will always back up the oldest snapshot eligible for transfer to Tivoli Storage Manager.

(DB2) Off-loaded tape backups will not be registered in the DB2 history on the production system. They will be reflected in the DB2 history on the offload system as long as the assigned volumes have not been overwritten. See also “DB2 backup history file overview” on page 127.

By specifying the -D option for the IBM Tivoli Storage Manager for Advanced Copy Services offload agent, it will act as a daemon process that periodically checks for outstanding tape backup requests. Furthermore, the IBM Tivoli Storage Manager for Advanced Copy Services offload agent, running as a daemon, tries to offload a snapshot backup to tape only once. If the first attempt fails for some reason, the snapshot backup is marked accordingly and will not be picked a second time by the tsm4acs daemon for offloading to tape. Such a backup must be offloaded to tape manually by issuing

```
tsm4acs -f tape_backup <filter arguments>
```

If multiple snapshot backups of a database are candidates for off-loading to tape, the IBM Tivoli Storage Manager for Advanced Copy Services offload agent (whether as a daemon or with the -f tape_backup function) always selects the one with the oldest snapshot backup ID.

The tsm4acs function ’tape_backup’ will internally do the following steps:

1. Mount the filesystems on the offload system, if they were not previously mounted using tsm4acs or the mount agent. If all necessary filesystems were already mounted using the ″-f mount″ function, this step will be skipped (see “-f mount” on page 157).

   Note: For snapshots of a database located on AIX JFS filesystems or LVM mirrors, the mount of the filesystems on a backup system is required to verify the consistency of the snapshot.
2. Update the usability state to TAPE_BACKUP_IN_PROGRESS for all partitions having the usability state TAPE_BACKUP_PENDING set.
3. Back up these partitions to tape.

4. Update usability states: For those partitions for which the backup succeeded, reset the usability state TAPE_BACKUP_PENDING. For all participating partitions, reset the usability state TAPE_BACKUP_IN_PROGRESS.
5. Unmount the filesystems from the offload system (see “-f unmount” on page 158).

As long as the usability state for a partition is TAPE_BACKUP_IN_PROGRESS, any request to restart the offload of that partition to tape will be refused.

(DB2) The ’tape_backup’ function can also be used to restart a failed tape backup for one or more DPF partitions. If a tsm4acs tape backup fails for one ore more DPF partitions, the TAPE_BACKUP_PENDING usability state will not be changed for these partitions. On the next start of the tape_backup function, tsm4acs will then retry the failed tape backup only for those partitions.

(DB2) In DPF environments, offloaded backups can be performed only if the snapshot was created on all partitions. If a backup to Tivoli Storage Manager fails, the Offload Agent can retry the backup operation. In this case the Offload Agent will only backup those partitions that have not been backed up successfully already. In order to avoid excessive retries the Offload Agent will not perform retries in daemon mode, i.e. when started with –D option. If multiple snapshot backups are required to be backed up to Tivoli Storage Manager, the Offload Agent will always start with the oldest snapshot for which a Tivoli Storage Manager backup was requested. This ensures that the Tivoli Storage Manager backups are created in the appropriate chronological order.

The ’tape_backup’ function can also be used to restart a failed tape backup for one or more DPF partitions. If a tsm4acs tape backup fails for a DPF partition, the TAPE_BACKUP_PENDING usability state will not be changed, but the retry counter will be incremented. On the next start of the tape_backup function, tsm4acs will then retry this failed tape backup.

-f mount

This Offload Agent command mounts a snapshot backup on an offload system.

Mounting a backup means the following occurs:

1. Configure the target volume(s), which must have been assigned to the offload system
2. Import the volume group(s) from the target volume(s)
3. Mount all filesystems within the volume group(s).

The mount itself, if not already done by the mount agent, is done by a device agent started by tsm4acs. By specifying additional options (filter arguments) such as

```
-i instance-name
-d database-name
-T snapshot-id
```

a specific snapshot backup can be selected for mounting on the offload system.

(DB2) In a DPF environment with multiple partitions, the IBM Tivoli Storage Manager for Advanced Copy ServicesS offload agent always mounts all partitions associated with a snapshot backup operation.

To reflect whether a partition of a snapshot backup is currently being mounted or is already mounted, the usability states MOUNTING and MOUNTED, respectively, will be set for those partitions in the snapshot backup repository (see "Usability states" on page 35). These two state values prevent a duplicate mount request for a partition that is currently being mounted, or is already mounted, on the offload system. If multiple snapshot backups of a database are candidates to be mounted, the IBM Tivoli Storage Manager for Advanced Copy Services offload agent always picks the one with the most recent snapshot backup ID.

-f unmount

This Offload Agent command releases all resources on the offload server that were used by the mount command.

Normal mode: The unmount itself will be done by an appropriate device agent started by tsm4acs. The following steps will be done internally:

1. Unmount the filesystems belonging to the target volumes
2. Export the assigned volume group
3. Remove the devices (vpath/hdisk) from the offload system

By specifying additional options (filter arguments) such as

```
-i instance-name
-d database-name
-T snapshot-id
```

a specific snapshot backup can be selected for unmounting from the offload system.

(DB2) In a DPF environment with multiple partitions, the IBM Tivoli Storage Manager for Advanced Copy Services offload agent always unmounts all partitions associated with a snapshot backup.

If the unmount does not succeed due to problems on the device agent side, the usability state of the participating partitions will remain MOUNTED in the snapshot backup repository. Thus, after resolving the problems on the offload system (in some cases the only way might be a manual intervention), the tsm4acs 'unmount' has to be issued again to finalize the unmount of the filesystems and update the usability state of the participating partitions in the snapshot backup repository accordingly. If an off-loaded tape backup is currently running (usability state TAPE_BACKUP_IN_PROGRESS is set), those partitions will not be picked by the IBM Tivoli Storage Manager for Advanced Copy Services offload agent for unmounting.

Force mode: Unexpected system failures in combination with off-loaded tape backups can potentially lead to an incorrect state of the participating partitions reflected in the snapshot backup repository (TAPE_BACKUP_IN_PROGRESS still set). Therefore, a special built-in 'force' option (-F) for the tsm4acs 'unmount' function is provided to return the system to a usable state. Besides the normal unmount function, 'unmount force' is able to pick partitions currently in the TAPE_BACKUP_IN_PROGRESS state as candidates to be unmounted and to reset the TAPE_BACKUP_IN_PROGRESS usability state for those partitions of a snapshot backup. The '-d', '-i', and '-T' options must be specified to uniquely identify the backup involved.

Chapter 7. Configuration files overview

Configuration files are defined by the user with all the information Data Protection for Snapshot Devices (or DB2 Advanced Copy Services) needs to successfully perform its functions.

Data Protection for Snapshot Devices uses the following configuration files:

- Profile
- (SAP with Oracle) SAP Backint configuration file
- Password file
- Target volumes file(s)
- (SAP with Oracle) BR*Tools configuration file
- (Native Oracle) Tivoli Storage Manager options files
- Oracle database control file

(DB2) Data Protection for Snapshot Devices and DB2 Advanced Copy Services use the same set of configuration files (although certain options and parameters are restricted for DB2 Advanced Copy Services). When Data Protection for Snapshot Devices is installed, the existing profile for DB2 Advanced Copy Services is updated.

Related concepts

"SAP® backint profile overview" on page 192
The SAP® backint profile is considered an extension of the Data Protection for Snapshot Devices profile in an SAP® with Oracle configuration.

"Tivoli Storage Manager option files for native Oracle" on page 194
Tivoli Storage Manager provides these options to assist with setting up the native Oracle environment.

Related tasks

"Data Protection for Snapshot Devices password file" on page 188
Data Protection for Snapshot Devices requires a password file in order to access the storage subsystem where the database volumes are stored.

"Data Protection for Snapshot Devices Target Volumes File (.fct)" on page 189
The target volumes file identifies the target volumes to be used for a FlashCopy backup.

Related reference

"BR*Tools configuration profile (.sap)" on page 193
This configuration profile is located in the $ORACLE_HOME/dbs directory on AIX or Linux systems.

Data Protection for Snapshot Devices profile description

Data Protection for Snapshot Devices relies on a profile in order to operate properly.

The profile needs to be available on all database nodes, on the machine where the Management Agent (acsd) is running, and on a backup server when saving snapshot backups to Tivoli Storage Manager.

The Data Protection for Snapshot Devices profile (which in a DB2 environment is also the *DB2 Advanced Copy Services profile* prior to installation of Data Protection for Snapshot Devices) is created or updated using the setup script. The standard profile is named 'profile' and is recommended to be defined as follows:

`HOME/acs/profile`

The location where the profile is defined must meet these requirements:

- The profile directory must not be part of any snapshot operation.
- (DB2) The profile directory can be NFS exported and NFS shared on all DB2 DPF partitions and on the backup system for an offloaded Tivoli Storage Manager backup.

The Data Protection for Snapshot Devices profile is typically used with only one database name. The profile is identified by the value of the option -p of the Data Protection for Snapshot Devices program `tsm4acs` and by the PROFILE vendor option for DB2 Advanced Copy Services and Data Protection for Snapshot Devices. The elements of the profile are not case sensitive. By convention, section and parameter names are shown in uppercase.

Data Protection for Snapshot Devices profile sections

Each section of the Data Protection for Snapshot Devices profile file contains information unique to that section.

The profile is structured into these named sections:

- GLOBAL
- ACSD
- CLIENT
- *device*
- OFFLOAD
- ORACLE

The *device* section can occur multiple times. The names are changeable and determined by using the DEVICE_CLASS profile parameter or vendor option. Each section has a unique set of specific parameters.

GLOBAL section

The GLOBAL section contains information that is required and used by all Data Protection for Snapshot Devices components and is therefore required on all database nodes as well as by the management, device, and offload agents. Any component of Data Protection for Snapshot Devices evaluates this section only once (during startup). Therefore, changes within this section require Data Protection for Snapshot Devices to be restarted before they become effective. Depending on the environment, it might be necessary to install Data Protection for Snapshot Devices on multiple machines. Such an environment might be when the database is distributed across multiple application hosts or when using a backup server to transfer snapshot backups to Tivoli Storage Manager. Even in those environments there is always only one active Management Agent, whose location is specified using the ACSD parameter in this section. The GLOBAL section is also used to specify the location for logging, tracing, and password files.

ACSD section

The ACSD section contains information that is used exclusively by the Management Agent (acsd). This section includes the ACS_REPOSITORY parameter, which specifies the directory where the Management Agent stores its backup repository. This repository is the most important collection of Data Protection for Snapshot Devices data. If the repository is lost, any previously created backup will not be able to be restored.

CLIENT section

The CLIENT section contains all parameters relating to backup operations, such as SAP or native database applications, the number of backup versions, whether a Tivoli Storage Manager backup is to be created from the snapshot, how many snapshot backup generations to retain, and which device section is used during snapshot creation. The CLIENT section is used by the Snapshot Backup Library that is loaded to start backup or restore processing. Most of the parameters in the CLIENT section can be overridden by options.

Note: (SAP with Oracle) The CLIENT section does not apply to this configuration. The parameters described for the CLIENT section are present in a modified form in a separate profile, which is normally the Tivoli Storage Manager for ERP profile. For more information, see "SAP® backint profile overview" on page 192.

device **section**

The *device* section contains parameters related to the storage system. At least one device section is required for the configuration of the Management Agent. A device section describes the characteristics of a storage device that can be used to create a snapshot backup and as such depends heavily on the specific storage subsystem. You can specify multiple device sections within one profile and assign names of your choosing to these sections. By specifying the DEVICE_CLASS parameter or option setting during a backup, the corresponding device section will be activated for use during this particular operation. The value of DEVICE_CLASS is recorded in the IBM Tivoli Storage Manager for Advanced Copy Services repository in order to identify the appropriate device section that is used during restore. For each of the device sections, a password is required and can be set using the Management Agent command `acsd –f password`. These passwords are used by Data Protection for Snapshot Devices to authenticate to the disk subsystem represented by the associated device section. See also "Management Agent (acsd)" on page 138.

OFFLOAD section

The OFFLOAD section contains information on how a snapshot is transferred to Tivoli Storage Manager. It is used by the Offload Agent (tsm4acs) running on the backup server and in a DB2 environment, it requires the Data Protection for Snapshot Devices license. See "Data Protection for Snapshot Devices Offload Agent (tsm4acs)" on page 154 and "Backup methods overview" on page 33.

When the Offload Agent is started, it connects to the Management Agent and queries for snapshot backups that have been backed up with profile parameter) TSM_BACKUP (for SAP with Oracle TSM_BACKUP_FROM_SNAPSHOT) set to YES. If such a backup is found, the Offload Agent will mount this snapshot and initiate a Tivoli Storage Manager backup using the following application:

- (Native DB2) the DB2 built-in Tivoli Storage Manager agent
- (SAP with Oracle or DB2) IBM Tivoli Storage Manager for Enterprise Resource Planning (Tivoli Storage Manager for ERP)
- (Native Oracle) Oracle RMAN and Data Protection for Oracle.

(DB2) The OFFLOAD section is optional unless one of these conditions exists:

- Tivoli Storage Manager for ERP is used for offload tape backup (at least the OPTIONS parameter must be present).
- One or more of the default values must be overridden.

(DB2) In DB2 DPF environments, offloaded backups can be performed only when the snapshot was created on all partitions. If a backup to Tivoli Storage Manager fails, the Offload Agent can retry the backup operation. In this case, the Offload Agent only backs up those partitions that have not already been backed up successfully. In order to avoid an excessive number of retries, the Offload Agent does not perform retries in daemon mode, (for example, when started with the -D option). If multiple snapshot backups are required to be backed up to Tivoli Storage Manager, the Offload Agent always starts with the snapshot for which a Tivoli Storage Manager backup was first requested. This ensures that the Tivoli Storage Manager backups are created in the appropriate order in sequence. In addition to generating backups, the Offload Agent can be used to mount and unmount a snapshot backup on the backup server.

(Oracle) The OFFLOAD *(system ID)* section is optional unless one or more of the default values must be overridden.

Warning: For DS8000, DS6000, SAN Volume Controller, and ESS devices, modifications of a mounted snapshot backup are not undone during unmount and remain persistent, i.e. if a modified backup is restored, all modifications are also persistent on the restored image.

Restriction: You can use only one backup server per database.

ORACLE section

(Oracle) The ORACLE section contains the parameters describing the native Oracle database designated by the DATABASE parameter in the CLIENT section. The ORACLE section is not needed for SAP with Oracle configurations.

Example

All parameters belonging to a section are enclosed by a section-begin statement (>>> *sectionname*) and a section-end statement (<<< *sectionname*). The name is optional on the section-end statement. Comments can be used at any place within the profile; they are introduced by '#' and apply to the remainder of the line. Tab characters are permitted. The basic structure for the file sections is as follows:

```
# Global section
>>> GLOBAL
parameter_line 1
  ....
parameter_line n
<<<
# ACSD section
>>> ACSD
parameter_line 1
  ....
parameter_line n
<<<
# CLIENT section
>>> CLIENT
parameter_line 1
  ....
parameter_line n
<<<
# device section
>>> device
parameter_line 1
  ....
parameter_line n
<<<
# device2 section
>>> device2
parameter_line 1
  ....
parameter_line n
<<<
# OFFLOAD section
>>> OFFLOAD
parameter_line 1
  ....
parameter_line n
<<<
# ORACLE section
>>> ORACLE
parameter_line 1
  ....
parameter_line n
<<<
```

Overriding Data Protection for Snapshot Devices profile parameters

DB2 vendor options can override Data Protection for Snapshot Devices profile parameters.

Several profile parameters can be overridden temporarily using DB2 vendor options, by using the tsm4acs command line, or the BR*Tools utilities. In these situations, the parameters specified during command invocation always supersedes the corresponding value within the profile.

Related reference

“Options for DB2 Advanced Copy Services and Data Protection for Snapshot Devices commands” on page 136

“Data Protection for Snapshot Devices commands and scripts” on page 133

Modifying the GLOBAL or ACSD sections of the Data Protection for Snapshot Devices profile

Changes to the profile take effect immediately and do not require restarting Data Protection for Snapshot Devices except when the GLOBAL or ACSD sections are modified.

Changes to the profile take effect immediately and do not require restarting Data Protection for Snapshot Devices. However, changes to the GLOBAL or ACSD sections do not take effect immediately and require the following procedure:

1. Issue this command to stop Data Protection for Snapshot Devices on all machines where it is currently installed:
   ```
   setup_<database>.sh –a stop
   ```
2. Update the parameters in the GLOBAL or ACSD sections.
3. Issue this command to start Data Protection for Snapshot Devices on all machines that were previously stopped:
   ```
   setup_<database>.sh –a start
   ```

Data Protection for Snapshot Devices profile parameters

Refer to this chart for assistance when setting the Data Protection for Snapshot Devices profile parameters.

The following table summarizes the profile parameters.

Note: Parameters designated as ″+″ under ″SAP with Oracle″ are physically defined (with any alternate name indicated in parentheses) in the separate SAP Backint profile. See “SAP® backint profile overview” on page 192.

Table 46. Data Protection for Snapshot Devices Profile Parameters

	Database Environment			Device Applicability							Parameter		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV®**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
GLOBAL	x	x	x	x	x	x	x	x	x	x	ACS_DIR	Path of the IBM Tivoli Storage Manager for Advanced Copy Services directory. See note 1.	Required
GLOBAL	x	x	x	x	x	x	x	x	x	x	ACSD	*hostname port* Hostname and port (separated by space) of the system on which the Management Agent is running. This parameter must be identical on all systems where Data Protection for Snapshot Devices is installed.	localhost 57328
GLOBAL	x	x	+	x	x	x	x	x	x	x	TRACE (TRACE)	**YES** Enable tracing **NO** Disable tracing For more information, see "Log and trace files summary" on page 228. TRACE can also be specified in the backint profile.	NO
ACSD	x	x	x	x	x	x	x	x	x	x	ACS_REPOSITORY	Path to the ACS repository directory. See Note 2.	This parameter must be specified by the user.

Table 46. Data Protection for Snapshot Devices Profile Parameters (continued)

	Database Environment			Device Applicability							Parameter		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV$^{®}$**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
ACSD	x		x	x	x	x	x	x	x		ADMIN_ASSISTANT	*<server> <port>* Server and port on which the Tivoli Storage Manager for ERP Administration Assistant server component is listening. **NO** Do not send data to the Administration Assistant. See note 3.	NO
ACSD	x	x	x	x	x	x	x	x	x		REPOSITORY_LABEL	A prefix added to each volume name on the storage device. A maximum of three characters is allowed in one of these ranges:`[a-z][A-Z][0-9]`	TSM
CLIENT	x	x		x	x	x	x	x	x		APPLICATION_TYPE	Environment (native or SAP application) **DB2** Treat as a generic (native) DB2 system. **ORACLE** Treat as a generic (native) Oracle system. **SAP** An SAP$^{®}$ application uses the underlying database.	This parameter is set depending on the setup script variant used.

Table 46. Data Protection for Snapshot Devices Profile Parameters (continued)

	Database Environment			Device Applicability							Parameter		
Section	DB2	Native Oracle	SAP with Oracle	DS	SVC	ESS	N Series SAN	N Series NAS	XIV®	Used by DB2 Advanced Copy Services	Name	Value	Default value
CLIENT		x									DATABASE	Oracle database designation	None.
CLIENT	x	x	+	x	x	x	x	x	x		TSM_BACKUP (TSM_BACKUP_ FROM_SNAPSHOT)	YES, NO, TSM_ONLY See note 20.	NO
CLIENT	x	x	+	x	x	x	x	x	x	x	MAX_VERSIONS (MAX_SNAPSHOT_ VERSIONS)	See note 13.	DB2 Advanced Copy Services: 2 Data Protection for Snapshot Devices: ADAPTIVE
CLIENT	x	x	+	x	x	x	x		x	x	LVM_FREEZE_THAW	See note 12.	AUTO
CLIENT	x	x	+	x	x	x	x	x	x	x	DEVICE_CLASS	Name of the device section to use during a backup. See note 10.	STANDARD
CLIENT	x	x		x	x	x	x	x	x	x	NEGATIVE_LIST	**NO_CHECK** Does not check for additional files. **WARN** Issues a warning (processing continues) **ERROR** Issues an error (processing ends) *filename* Contains fully qualified names of files and directories. See note 14.	This parameter must be specified by the user.

Table 46. Data Protection for Snapshot Devices Profile Parameters *(continued)*

	Database Environment			Device Applicability							Parameter		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV®**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
CLIENT		x	+	x	x	x	x	x	x		TARGET_DATABASE_ SUSPEND	YES, NO This value specifies whether to suspend activity on the target database until the FlashCopy operation completes. Enter one of the following values: *yes*, *no*, or *n*. A *yes* value is recommended when transaction processing activity is high. The default value is *no*.	NO

Table 46. Data Protection for Snapshot Devices Profile Parameters (continued)

	Database Environment			**Device Applicability**							**Parameter**		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV$^{®}$**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
device	x	x	x	x	x	x	x	x	x	x	COPYSERVICES_ HARDWARE_TYPE	Storage system on which the database resides: **DS8000** IBM DS8100IBM DS8300 **DS6000** IBM DS6800 **ESS800** IBM ESS Model 800 **SVC** IBM SAN Volume Controller **SAN_NSERIES** IBM N Series (connected via SAN) **NAS_NSERIES** IBM N Series (network attached, accessed via NFS) **XIV** IBM XIV$^{®}$ Storage System See note 5. Only one system can be specified.	This parameter is required.

Table 46. Data Protection for Snapshot Devices Profile Parameters (continued)

	Database Environment			**Device Applicability**							**Parameter**		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV®**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
device	x	x	x	x	x	x	x	x		x	COPYSERVICES_ PRIMARY_ SERVERNAME	*server name or address* Defines the TCP/IP address of the host running the CIM Agent for DS Open API (which can manage the primary and secondary Copy Services servers of the ESS or DS cluster), or of the SVC master console, or of the filer for N Series (Net App).	localhost
device	x	x	x	x	x	x					COPYSERVICES_ SECONDARY_ SERVERNAME	Specify the name of the backup Copy Services server located within an snapshot devices cluster. You can specify either the numeric IP address or the DNS name of the server. The default value is *none*.	'none'

Table 46. Data Protection for Snapshot Devices Profile Parameters (continued)

	Database Environment			Device Applicability							Parameter		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV®**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
device	x	x	x	x	x	x	x	x	x	x	COPYSERVICES_ USERNAME	User name for: *nseries user* Net App user name for accessing the API *cim user* CIM Agent for DS Open API (which can manage the primary and secondary Copy Services servers of the ESS or DS cluster) *svc user* SVC master console	superuser
device	x	x	x	x	x	x				x	COPYSERVICES_ SERVERPORT	*server port* Defines the port number on the host running the CIM Agent for DS Open API (which can manage the primary and secondary Copy Services servers of the ESS or DS cluster), or the SVC master console,	See Note 7.

Table 46. Data Protection for Snapshot Devices Profile Parameters (continued)

	Database Environment			**Device Applicability**							**Parameter**		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV®**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
device	x	x	x	x	x	x				x	COPYSERVICES_ TIMEOUT	*timeout* Maximum length of time (in minutes) the CIM Client will wait for the response to a call issued to the CIMOM (CIM Agent) If the CIM Client does not receive a response within this time, an error message is issued.	6
device	x	x	x	x	x	x				x	COPYSERVICES_ COMMPROTOCOL	Protocol to be used for communication with the CIM Agent. **HTTP** Communication in non-secure mode **HTTPS** Communication in secure mode	HTTPS
device	x	x	x	x	x	x				x	COPYSERVICES_ CERTIFICATEFILE	See note 6.	NO_CERTIFICATE

Table 46. Data Protection for Snapshot Devices Profile Parameters (continued)

	Database Environment			**Device Applicability**							**Parameter**		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV®**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
device	x	x	x	x	x	x	x	x		x	FLASHCOPY_TYPE (See note 11.)	Specifies whether the storage subsystem performs a bitwise copy of data from one logical volume to another. **COPY** Directs the storage system to perform a bit-level copy of the data from one physical volume to another. This value is recommended under the following conditions: • You intend to perform a fast (snapshot) restore backed-up database • A copy of the database data on the target volume is desired.	COPY
device	x	x	x	x	x	x					FLASHCOPY_TYPE (cont'd)	**INCR** Similar to COPY. It differs from COPY by the fact that it only copies those tracks that were modified since the previous incremental FlashCopy was created.	COPY

Table 46. Data Protection for Snapshot Devices Profile Parameters (continued)

	Database Environment			**Device Applicability**							**Parameter**		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV®**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
device	x	x	x	x	x	x					FLASHCOPY_TYPE (cont'd)	**NOCOPY** Directs the storage system to perform a bit-level copy of a track when and if data is modified after the FlashCopy request. This technique is typically referred as copy-on- write	COPY
device	x	x	x	x	x	x				x	VOLUMES_DIR	Fully qualified path of the volumes directory, in which the FlashCopy target volumes file(s) must reside. See the Note 21 and "Data Protection for Snapshot Devices Target Volumes File (.fct)" on page 189.	This parameter must be specified by the user.
device	x	x	x		x						SVC_COPY_RATE	*priority* Specifies the priority that the SVC will give to the FlashCopy background process for the current backup or restore. See note 18.	80

Table 46. Data Protection for Snapshot Devices Profile Parameters (continued)

	Database Environment			**Device Applicability**							**Parameter**		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV®**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
device	x	x	x				x			x	PROD_INITIATOR_ GROUP	*groupname* See note 16.	Production system hostname passed for the application to the device agent (for DB2, this is the takeover-independent hostname).
device	x	x	x				x			x	BACK_INITIATOR_ GROUP	*groupname* See also PROD_INITIATOR_ GROUP	Name of the host on which the mount is executed.
device	x	x	x	x	x	x				x	RESTORE_FORCE	YES, NO (See note 17.)	NO
OFFLOAD	x	x	x	x	x	x	x	x	x		BACKUP_METHOD	DB2, ORACLE, BACKINT	Required
OFFLOAD	x			x	x	x	x	x	x		OPTIONS	**<options string>** Specifies options to be used for this Tivoli Storage Manager backup operation. The string is passed directly to the backup utility. **@filename** Specifies that the options to be used for the Tivoli Storage Manager backup operation are contained in a file located on the backup server. The string will be passed directly to the backup utility. See note 15.	Empty string.

Table 46. Data Protection for Snapshot Devices Profile Parameters (continued)

	Database Environment			Device Applicability							Parameter		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV®**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
OFFLOAD		x		x	x	x	x	x	x		OVERWRITE_ DATABASE_ PARAMETER_ FILE	**YES** Replace the database configuration file on the backup system with the version defined on the production system, to ensure they are identical. **NO** Do not copy the production-system database configuration file to the backup system.	NO
OFFLOAD		x		x	x	x	x	x	x		DATABASE_ BACKUP_ INCREMENTAL_ LEVEL	n Level of backup to be performed. You can enter any numerical value. See note 8.	0
OFFLOAD	x			x	x	x	x	x	x		PARALLELISM	**n** Number of table spaces that can be read in parallel by the backup utility. **AUTO** DB2 calculates an optimum value.	AUTO
OFFLOAD	x			x	x	x	x	x	x		NUM_SESSIONS	**n** Number of I/O sessions to be created between DB2 and Tivoli Storage Manager.	1

Table 46. Data Protection for Snapshot Devices Profile Parameters (continued)

	Database Environment			Device Applicability							Parameter		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV®**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
OFFLOAD	x			x	x	x	x	x	x		NUM_BUFFERS	**n** Number of buffers to be used by DB2. **AUTO** DB2 will calculate the optimum value for this parameter.	AUTO
OFFLOAD	x			x	x	x	x	x	x		BUFFER_SIZE	**n** The value of this parameter specifies the size, in 4 KB pages, of the buffer used by DB2 when building the backup image. The minimum value is 8 pages. **AUTO** DB2 calculates the optimum value if backup was started automatically.	AUTO

Table 46. Data Protection for Snapshot Devices Profile Parameters (continued)

	Database Environment			**Device Applicability**							**Parameter**		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV®**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
OFFLOAD	x			x	x	x	x	x	x		PARALLEL_BACKUP	**YES** The Tivoli Storage Manager backup of all participating partitions will run in parallel. **NO** The Tivoli Storage Manager backups of all participating partitions will run sequentially. Before setting this parameter to YES, check the release notes for the requirements to be observed.	NO
OFFLOAD			x								PROFILE	Name of the external SAP Backint profile	
ORACLE		x		x	x	x	x	x	x		CATALOG_DATABASE_ CONNECT_STRING	Recovery catalog connect string This value specifies the connect string of the Recovery Catalog database to be used to catalog backup information. This value must correspond to the value defined in the $ORACLE_HOME/ network/admin/ tnsnames.ora file.	

Table 46. Data Protection for Snapshot Devices Profile Parameters (continued)

	Database Environment			Device Applicability							Parameter		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV®**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
ORACLE		x		x	x	x	x	x	x		CATALOG_DATABASE_ USERNAME	User name This value specifies a user name that has Oracle system database administrator privileges on the Recovery Catalog database.	
ORACLE		x		x	x	x	x	x	x		TARGET_DATABASE_ PARAMETER_FILE	Target database parameter file This value specifies the fully resolved path and file name of the Oracle parameter file (init<SID>.ora by default) for the target database. Note that this file must be a text-based Oracle parameter file (PFILE) and not an Oracle server file.	
ORACLE		x		x	x	x	x	x	x		DATABASE_BACKUP_ SCRIPT_FILE	Name of the RMAN backup script that contains the Data Protection for Oracle environment variables. See note 9.	

Table 46. Data Protection for Snapshot Devices Profile Parameters (continued)

	Database Environment			Device Applicability							Parameter		
Section	**DB2**	**Native Oracle**	**SAP with Oracle**	**DS**	**SVC**	**ESS**	**N Series SAN**	**N Series NAS**	**XIV®**	**Used by DB2 Advanced Copy Services**	**Name**	**Value**	**Default value**
ORACLE		x		x	x	x	x	x	x		DATABASE_CONTROL_ FILE_RESTORE	YES, NO Specify whether to restore Oracle control files after snapshot restore processing completes. A *no* value will not restore Oracle control files and the user will do the full recovery up to the current image of the Oracle database using existing control files residing in the system. A *yes* value restores Oracle control files and the user will do the incomplete recovery up to the point when the control files were backed up.	NO

Profile parameter notes

1. ACS_DIR

The IBM Tivoli Storage Manager for Advanced Copy Services directory contains the following subdirectories:

- Subdirectory `logs` contains all log and trace information that IBM Tivoli Storage Manager for Advanced Copy Services generates. If you want all of your client nodes to store log and trace information within a single directory, you can use an NFS share for this volume.
- Subdirectory `shared` is used for information that needs to be shared among all Data Protection for Snapshot Devices components. You can either use an NFS filesystem to share this information across multiple servers or transfer a copy of this subdirectory to all systems on which Data Protection for Snapshot Devices is installed.

  The `shared` subdirectory currently contains only the password file (pwd.acsd). This file maintains passwords for all devices specified within the profile (see the device section) and a *master password*, which is used from all components in order to authenticate when connecting to the Management Agent. See "Data Protection for Snapshot Devices password file" on page 188.

  Note: By mapping ACS_DIR (or either of the subdirectories `logs` and `shared`) on an NFS share that is accessible to all Data Protection for Snapshot Devices components, you gain centralized access to all logs and eliminate the need to distribute the password file.

2. ACS_REPOSITORY

Specifies the directory in which the IBM Tivoli Storage Manager for Advanced Copy Services repository resides. The IBM Tivoli Storage Manager for Advanced Copy Services repository is critical for restore. It must be placed in a secure location. If the repository is lost, all backups are effectively deleted. The directory referenced by ACS_REPOSITORY cannot be in a filesystem that is participating in the snapshot backup. Otherwise, Data Protection for Snapshot Devices might fail. It is recommended that the IBM Tivoli Storage Manager for Advanced Copy Services repository not be in the main IBM Tivoli Storage Manager for Advanced Copy Services directory (ACS_DIR). A preferred location is a subdirectory of <ACS_DIR>:

```
<ACS_DIR>/acsrepository
```

ACS_REPOSITORY must be located on an NFS-mounted filesystem that is shared among all servers where Data Protection for Snapshot Devices is installed.

Note: The path to ACS_REPOSITORY must exist prior to the initial configuration, but the directory itself must not exist. The setup wizard will indicate an error if this directory already exists but does not contain a valid repository.

3. ADMIN_ASSISTANT

If this parameter is defined, Data Protection for Snapshot Devices will send backup and restore information to the Administration Assistant if Tivoli Storage Manager for ERP and the Administration Assistant component are installed. <server> and <port> are separated by a space. This parameter is ignored in non-SAP environments.

4. **REPOSITORY_LABEL**

Specify a prefix that will be added to each volume name on the storage device. A maximum of three characters is allowed and must be specified in one of these ranges:

```
[a-z]
[A-Z]
[0-9]
```

This optional parameter is only used with IBM XIV® Storage Systems. The default value is `TSM`.

Note: If the repository label is changed, backups created with the prior repository label are excluded from reconciliation.

5. **COPYSERVICES_HARDWARE_TYPE**

When this parameter specifies `XIV`, the following settings are required and must be specified in the device section of the profile:

COPYSERVICES_SERVERNAME

The hostname of the IBM XIV® Storage System. There is no default value.

PATH_TO_XCLI

The path where the XIV® command line interface (XCLI) is installed. There is no default value.

When the COPYSERVICES_HARDWARE_TYPE parameter specifies `XIV`, the following settings are optional:

BACKUP_HOST_NAME

The name of the backup host that is used during offloaded tape backups only. The default value is the `hostname` of the current machine.

COPYSERVICES_USERNAME

The username for the IBM XIV® Storage System. The default value is `superuser`.

GRACE_PERIOD

The period of time (specified in hours) to retain snapshots after they have been created that are not contained in the snapshot repository or not contained on the IBM XIV® Storage System. The default value is `24` hours. A `0` value reconciles all snapshots.

RECON_INTERVAL

The interval (specified in hours) to perform reconciliation for the IBM XIV® Storage System. The default value is `12` hours.

6. **COPYSERVICES_CERTIFICATEFILE**

If COPYSERVICES_ COMMPROTOCOL is set (or defaults) to `HTTPS`:

certificate file name

Name of a certificate file created for secure communication between the CIM Client and the CIM Agent.

NO_CERTIFICATE

Select null trust provider mode.

Use of NO_CERTIFICATE is required for SAN Volume Controller devices. Otherwise, it is recommended only when both the production and storage systems are protected by a firewall. The cimom.properties parameter `DigestAuthentication` must be set to ’false’.

7. COPYSERVICES_SERVERPORT

The default port number depends on the settings of COPYSERVICES_HARDWARE_TYPE and COPYSERVICES_COMMPROTOCOL:

COPYSERVICES_HARDWARE_TYPE	COPYSERVICES_COMMPROTOCOL	Default Port
DS8000,DS6000,ESS800	HTTPS	5989
SVC (before 4.2.1)	HTTPS	5999
	HTTP	5998
SVC (as of 4.2.1)	HTTPS	5989
	HTTP	5988
Other	HTTP	5988

8. DATABASE_BACKUP_INCREMENTAL_LEVEL

The following conditions apply:

- A *0* value performs a full backup. This is the default.
  - A full backup must be performed before an incremental backup can be performed.
- A numerical value greater than *0* performs an incremental backup.
  - Incremental backups are progressive. For example, a level *0* backup must be performed before a level *1* backup can occur. A level *1* backup must be performed before a level *2* backup can occur and so on.

9. DATABASE_BACKUP_SCRIPT_FILE

The script must:

1. contain commands that are valid for the backup system database (applicable on a database with datafile copies),
2. contain the Data Protection for Oracle environment variable TDPO_OPTFILE.

   Specify the fully qualified path name to the tdpo.opt options file with the TDPO_OPTFILE environment variable. See “RMAN backup script example” on page 115 for an example of this setting.
3. have the allocate channel command and the ENV parameter on the same line. For example:

   ```
   allocate channel t1 type 'sbt_tape' parms 'ENV=(TDPO_OPTFILE=..)';
   ```
4. have the database command specified on a line separate from the backup command. For example:

   ```
   backup
   (database);
   ```

10. DEVICE_CLASS

Multiple sections representing different devices are possible. Any such section can be selected using the DEVICE_CLASS profile parameter or vendor option. At restore time, Data Protection for Snapshot Devices always uses the same DEVICE_CLASS value that was used during the backup.

11. FLASHCOPY_TYPE

- This parameter applies generically to any snapshot device. The values INCR and NOCOPY apply only to FlashCopy devices.
- Only COPY is supported for an N Series configuration or for DB2 Advanced Copy Services without Data Protection for Snapshot Devices installed.
- COPY or INCR is required if the customer plans to run a snapshot restore.

- INCR is recommended if Tivoli Storage Manager backups are desired from disk copies, which are created with less burden on the storage system than for the COPY option. This value is also recommended under the following conditions:
  - You intend to perform a snapshot restore of the backed-up database.
  - You intend to schedule more frequent backups for your database.
- NOCOPY is recommended under the following conditions:
  - A complete copy of the source volumes on which the database files reside to the target volumes is not desired.
  - Backup time constraints are a concern

A successful backup of the database to the Tivoli Storage Manager server is possible even if the parameter is set to NOCOPY. The Tivoli Storage Manager server will contain a valid database backup, but the target volumes cannot be used for a snapshot restore.

For SVC only:

- If FLASHCOPY_TYPE is specified as NOCOPY or INCR, SVC_COPY_RATE is forced to 0.
- As of DP for Snapshot Devices V6.1, the value INCR is supported if the SVC is at level 4.2.1 or higher.

12. LVM_FREEZE_THAW

YES
Enable freeze prior to snapshot and thaw afterwards. For AIX, the value YES is valid only if all filesystems involved in the backup are JFS2 filesystems. The timeout value is set to 12 seconds. This parameter is ignored when Oracle data files reside on raw logical volumes.

NO
Do not perform a freeze. In order to set this parameter to NO, a licensed version of Data Protection for Snapshot Devices is needed and a backup server is required for mounting the snapshot to ensure filesystem consistency.

The value NO is required if at least one JFS filesystem is involved.

AUTO
If TARGET_DATABASE_SUSPEND is YES, treat as LVM_FREEZE_THAW YES.

timeout
Enable freeze/thaw with *timeout* value (seconds).

See also “Interdependency of LVM_FREEZE_THAW and TARGET_DATABASE_SUSPEND” on page 187.

13. MAX_VERSIONS

ADAPTIVE
The maximum number varies depending on the available space. In the case of DS8000, DS6000, SVC, or ESS, Data Protection for Snapshot Devices re-uses the oldest target set as the target for the current backup. For N Series devices, Data Protection for Snapshot Devices relies on the filer to delete snapshot backups.

n Maximum number of snapshot versions to be maintained. When this limit is reached, the oldest version is deleted.

(DB2) DB2 Advanced Copy Services (without a licensed version of Data Protection for Snapshot Devices) accepts only the values ’1’ and ’2’ for this parameter.

14. NEGATIVE_LIST

Depending on the storage device, Data Protection for Snapshot Devices performs backup and restore operations with file-system (NAS attached devices) or volume-group (SAN attached devices) granularity. The parameter NEGATIVE_LIST is used to control processing when non-database files are stored within the same file systems involved in the backup or restore operation. This parameter is required.

NO_CHECK

Does not check for additional files and the operation ignores any additional files that are discovered. Be aware that during restore processing, this setting will result in all files that reside in one of the file systems or volume groups (that are the subject of the restore) being overwritten.

WARN

Issues a warning for each file discovered on the volume that is not part of the FlashCopy operation (processing continues). In case of a restore, the additional files found on the file systems to restore will be overwritten by the restore operation.

ERROR

Issues an error for each file discovered on the volume that is not part of the FlashCopy operation (processing ends).

filename

When files exist that are not part of the database tablespace files but are to be included in the FlashCopy operation, specify the fully qualified names of these files and directories (one entry per line) in this negative-list file (`filename`). Processing continues even when these files are discovered. When other files are discovered that are not contained in this negative-list file, processing ends. Note that any directory listed in the negative-list file is processed recursively; for example, it allows all files within the directory (and any subdirectory) to be processed during a backup or restore request.

This parameter is not available for SAP® with Oracle because a similar mechanism is provided directly by the SAP® BR*Tools. Refer to the SAP® documentation for this purpose.

15. OPTIONS

(DB2) A file specification must be a fully qualified file name. If IBM Tivoli Storage Manager for Enterprise Resource Planning is being used, the IBM Tivoli Storage Manager for Enterprise Resource Planning DB2 vendor options file (vendor.env) must be specified.

(DB2) To be able to set up individual partitions in a DPF environment in a different manner, the placeholder string `%DB2NODE` can be embedded in the options string. At runtime, it will be replaced with the appropriate partition number for which the backup was issued. This placeholder can be part of the vendor options file entry, thus allowing different configuration files depending on the partition. For example, if there are two partitions

```
OPTIONS @/db2/T01/tdpr3/vendor_%DB2NODE.env
```

refers to the two files

```
/db2/T01/tdpr3/vendor_0.env
/db2/T01/tdpr3/vendor_1.env
```

The first file will be used for partition 0, the second for partition 1.Specifying this parameter overrides the value specified by the VENDOROPT database configuration parameter.

16. **PROD_INITIATOR_GROUP**
    In an N Series SAN environment, UNIX hosts serve as initiators and N Series storage systems serve as providers of the storage LUNs. In order to make LUNs accessible to a host server, you must map them to an initiator group that is associated with a Fibre Channel adapter installed on the host. In the mount process, IBM Tivoli Storage Manager for Advanced Copy Services automatically unmaps the LUNs of the clone volumes from the production host and maps them to the backup host. For this process, the initiator groups associated with both the production and backup hosts are needed. See also BACK_INITIATOR_GROUP.
17. **RESTORE_FORCE**
    In the case of a re-run of a snapshot restore, message IDS1089E is issued if the background copy process in the storage device of the previous snapshot restore is still running and RESTORE_FORCE is not set to YES. There are two options:
    - wait until the background copy process terminates
    - specify RESTORE_FORCE YES in the profile and re-run the snapshot restore. This will withdraw all existing source/target relations and create new ones, resulting in a full copy.

      Note: If you set RESTORE_FORCE to YES in a specific situation, but do not want it to apply to all restores, you should consider doing so in a temporary profile.
18. **SVC_COPY_RATE**
    The value represents a priority that can range between 0 and 100. A value of 100 is the highest but has the greatest impact on the responsiveness of the storage system. A value of 0 suppresses the background copy process and forces FLASHCOPY_TYPE to NOCOPY.
19. **TARGET_DATABASE_SUSPEND**
    This value specifies whether to suspend activity on the target database until the FlashCopy operation completes. Enter one of the following values:

    YES
    Suspend the target database until the FlashCopy operation completes. This value is recommended when the level of transaction processing is high.

    NO
    Do not suspend the target database.

    OFFLINE
    All backups must be offline. If SAP requests an offline backup, this parameter is ignored.

    The values YES and NO imply an ’online’ backup type. When performing a backup with OFFLINE specified, the target database on the production system must be in a ″startup mount″ state at the time that acsora or acsutil is issued. Otherwise recovery must be performed to restore the database.

See also "Interdependency of LVM_FREEZE_THAW and TARGET_DATABASE_SUSPEND."

20. TSM_BACKUP

In order to create a TSM backup from a snapshot, it is necessary to install DP for Snapshot Devices on a backup server. On this machine, an Offload Agent can be run to trigger a TSM backup from any snapshot created with TSM_BACKUP set to YES.

YES

Create a TSM backup from this snapshot.

NO

Keep the snapshot backup and do not use it as a source for a subsequent tape backup operation.

TSM_ONLY

If a snapshot/FlashCopy backup is performed with option TSM_ONLY, the backup will automatically be marked for deletion during the unmount operation once the TSM backup has completed, regardless of whether the backup was successful or not. This option was introduced for SVC and DS backups that are done with the option FLASHCOPYTYPE NOCOPY. In this case the FlashCopy is used only to offload the TSM backup workload to a secondary machine. This option is also valid for other values of FLASHCOPY_TYPE and other hardware, although it is not immediately applicable in these cases.

Note: (DB2) The ability to create a Tivoli Storage Manager backup from a snapshot requires a Data Protection for Snapshot Devices license.

21. VOLUMES_DIR

This parameter is required for FlashCopy devices only. Other devices define the target volumes automatically when a snapshot is requested. VOLUMES_DIR must be located on an NFS-mounted filesystem that is shared among all servers where Data Protection for Snapshot Devices is installed. A preferred location is

```
<ACS_DIR>/acsvolumes
```

Related tasks

"Data Protection for Snapshot Devices Target Volumes File (.fct)" on page 189
The target volumes file identifies the target volumes to be used for a FlashCopy backup.

Related reference

"Key files and directories" on page 194
Certain files and directories are of considerable importance when using Data Protection for Snapshot Devices.

Interdependency of LVM_FREEZE_THAW and TARGET_DATABASE_SUSPEND

The LVM_FREEZE_THAW and TARGET_DATABASE_SUSPEND profile parameters are interdependent.

These two Data Protection for Snapshot Devices profile parameters are interdependent in the following manner:

- If LVM_FREEZE_THAW is set to YES, the database must be suspended. Otherwise, write operations to the database might time out and leave the database in an inconsistent state. A specified value of NO for TARGET_DATABASE_ SUSPEND prevents this situation.

- If LVM_FREEZE_THAW is set to NO, the user might want to suspend the database without freezing the file system. Also, if JFS is used, freeze and thaw are not supported.

This parameter is ignored when Oracle data files reside on raw logical volumes.

The following table summarizes the actions taken depending on the values of the two parameters:

Table 47. Actions Taken Depending on Values of LVM_FREEZE_THAW and TARGET_DATABASE_ SUSPEND

Value of LVM_FREEZE_THAW	**Value of TARGET_DATABASE_SUSPEND**		
	YES	**NO**	**Not specified**
YES	Suspend and freeze	Terminate with an appropriate error message. Conflicting parameters.	Suspend and freeze (since suspend required)
NO	Suspend, no freeze	No suspend, no freeze	No suspend, no freeze
AUTO	Treat as LVM_FREEZE_THAW YES	Treat as LVM_FREEZE_THAW NO	Treat as LVM_FREEZE_THAW NO
Not specified	Suspend, no freeze	No suspend, no freeze	No suspend, no freeze

Data Protection for Snapshot Devices password file

Data Protection for Snapshot Devices requires a password file in order to access the storage subsystem where the database volumes are stored.

This password file also contains a *master password*, which is required by the Management Agent to authenticate the database nodes and the Offload Agent. It is possible to share a single password file between all systems by placing it into an NFS mounted file system that is available to all servers on which Data Protection for Snapshot Devices is installed. Separate password file instances can also be used for different database nodes, for the Management Agent, and for the (optional) Offload Agent. Separate password file instances for the Management Agent requires access to the password for the storage subsystem. For the Offload Agent, the master password is required on all systems.

A password file can be created during the initial setup of Data Protection for Snapshot Devices using the setup script, which also updates /etc/inittab appropriately. The following command can be used to update an existing profile and password file:

```
acsd -f password
```

The password file is stored as

`<ACS_DIR>/shared/pwd.acsd`

where <ACS_DIR> is the value of the ACS_DIR parameter in the profile.

Data Protection for Snapshot Devices Target Volumes File (.fct)

The target volumes file identifies the target volumes to be used for a FlashCopy backup.

This file pertains to FlashCopy configurations in both DB2 Advanced Copy Services and Data Protection for Snapshot Devices. The N Series subsystem defines the target files internally as part of the snapshot process and does not require a target volumes file. In an AIX LVM mirroring environment, there is an additional parameter (HARDWARE_ID_LVM_MIRROR).

The file conforms to the following naming convention:

```
<dbm-instance>.<database-name>.<device-class>.<partition-num>.fct

where
<dbm-instance>  = DB2 instance name
<database-name> = DB2 database alias
<device-class>  = device class specified in the DP for Snapshot Devices profile or
                  as a vendor option
<partition-num> = 'NODEnnnn', where nnnn = partition number (leading zeroes)
```

This file resides in the directory specified by the VOLUMES_DIR parameter in the DB2 Advanced Copy Services or Data Protection for Snapshot Devices profile. Multiple files are possible. The name is not case sensitive. For example:

```
keon14.A01.STANDARD.NODE0000.fct
```

Within one FlashCopy backup, a set of target volumes (a target set) will be needed for a FlashCopy operation with a set of source volumes making up the database. More than one target set can be defined for use in different FlashCopy backups.

The volumes in each target set used in one backup need to be specified in a similar way in a separate target set topic. A target set topic is delimited by a topic begin string (>>>) and a topic end string (<<<), each followed by the target set topic name. The target set topic names start with the prefix ’volumes_set_’ and are appended with a target set ID ’x’ (also referenced in some documentation as a *data container ID*) to differentiate the various target set topics. The target set ID can be any alphanumeric value.

In each topic, use one TARGET_VOLUME parameter for each target volume to be used in this target set. A target set topic appears as follows:

```
>>> volumes_set_1
TARGET_VOLUME ...
    .
    .
    .
TARGET_VOLUME ...
<<< volumes_set_1
```

If you plan to use a second target set (multiple target sets), you just add the next target set topic in the file:

```
>>> volumes_set_2
TARGET_VOLUME ...
    .
    .
    ,
TARGET_VOLUME ...
<<< volumes_set_2
```

Comments can be used only before the first target set topic; they are indicated by a ″#″ character in the first column of a line. Tab characters are not permitted.

Related concepts

"Overview of Data Protection for Snapshot Devices support for AIX Logical Volume Manager mirrored environments" on page 48

"Overview of multiple backup generations (target sets) on disk" on page 37
Support for multiple backup generations is inherent on N Series devices and is frequently referred to as frequent snapshots.

Related reference

"Target volume parameter settings (ESS or DS configuration)"
Each target volume planned for use must be specified by its serial number.

Target volume parameter settings (ESS or DS configuration)

Each target volume planned for use must be specified by its serial number.

A snapshot backup operation looks for either a source volume and target volume correlation, or a target-volume-only specification.

Table 48. Parameters of the 'volumes_set_x' Topic (ESS or DS)

Parameter Name	Value

TARGET_VOLUME
<target volume serial number>
<source volume serial number>
<source volume size>
	This parameter specifies the serial number of at least the target volume of one volume pair involved in the FlashCopy. Each target volume planned for use for a FlashCopy operation must be specified by its serial number in the volumes_set_1 topic. The source volume serial number and size are optional. If they are given, they must correctly reflect the current storage-system configuration and have the following format:
	`TARGET_VOLUME 401FCA90 40EFCA90 Size=2.0_GB`
	If they are omitted, dashes must be entered in both fields as placeholders, as shown in the following example:
	`TARGET_VOLUME 401FCA909 - -`
	The dashes will be replaced with the information obtained from the storage system configuration. When all source volumes have been found, the software tries to find an appropriate target volume specified in the volumes_set_1 topic. Note the target volume requirements for a FlashCopy:
	• The size must be the same as that of the source volume
	• The source volumes can be in different hardware units.
	• The target volume in each case must be in the same hardware unit as the respective source volume.
	Note: Do not change the order of the parameters (target volume serial number, source volume serial number, size of source volume).

Although you can specify all three fields within the TARGET_VOLUME parameter, it is recommended to specify only the first field (target volume serial number) and a dash ('-') for the other two fields. Once a FlashCopy has been done, Data Protection for Snapshot Devices will replace the two dashes with the actual values (source volume serial number, source volume size), and these values will continue to be used in future runs. If the storage-system configuration is subsequently altered, the source volume serial numbers and sizes should be reset to dashes to allow the new values to be determined. Any comments placed within or between the target set topics will be overwritten when Data Protection for Snapshot Devices rewrites the target set topic(s).

In case you plan to remove a target set volume, you must first run a db2acsutil delete with the DELETE_FORCE vendor option to ensure that, based on the usage of this target set:

- any existing source/target relationships (such as INCR or NOCOPY) are withdrawn, the FlashCopy backup is no longer valid, and no potential problems remain for succeeding snapshot restores.
- any mounted file systems using this target volume on the backup system must be released (unmount fs, ..., exportvg) prior to running db2acsutil delete. This can be done with the 'tsm4acs -f unmount' command.

Related reference

"Example target volumes file (ESS or DS configuration)" on page 205
Refer to this example when editing the target volumes file for an ESS or DS storage subsystem configuration.

Parameters for an SVC Configuration

Each target volume planned for use must be specified by its virtual disk name.

A snapshot backup operation looks for either a source volume and target volume correlation, or a target-volume-only specification.

Table 49. Parameters of the 'volumes_set_x' Topic (SVC)

Parameter Name	Value

TARGET_VOLUME
<target volume virtual disk name>
<source volume virtual disk name>
<source volume size>
	This parameter specifies the virtual disk name of at least the target disk of one pair of virtual disks involved in the FlashCopy. Each target planned for use for a FlashCopy operation must be specified by its name (also known as the *caption*) in the volumes_set_1 topic. The source name and size are optional. If they are given, they must correctly reflect the current storage-system configuration and have the following format:
	`TARGET_VOLUME svdftgt4 svdfsrc4 Size=2.0_GB`
	If they are omitted, dashes must be entered in both fields as placeholders, as shown in the following example:
	`TARGET_VOLUME svdftgt4 - -`
	The dashes will be replaced with the information obtained from the storage system configuration. When all source volumes that make up the backup request have been found, the software tries to find an appropriate target volume specified in the volumes_set_1 topic. Note the target volume requirements for a FlashCopy:
	• the size must be the same as that of the source volume
	• the source and target volumes must be in the same SVC cluster.
	Note: Do not change the order of the parameters (target volume name, source volume name, size of source volume).

Although you can specify all three fields within the TARGET_VOLUME parameter, it is recommended to specify only the first field (target volume name) and a dash ('-') for the other two fields. Once a FlashCopy has been done, Data Protection for Snapshot Devices will replace the two dashes with the actual values (source volume name, source volume size), and these values will continue to be used in future runs. If the storage-system configuration is subsequently altered, the source volume names and sizes should be reset to dashes to allow the new values to be determined. Any comments placed within or between the target set topics will be overwritten when Data Protection for Snapshot Devices rewrites the target set topic(s).

In case you plan to remove a target set volume, you must first run a 'db2acsutil delete' with the DELETE_FORCE vendor option to ensure that, based on the usage of this target set:

- any existing source/target relationships (such as INCR or NOCOPY) are withdrawn, the FlashCopy backup is no longer valid, and no potential problems remain for succeeding snapshot restores.
- any mounted file systems using this target volume on the backup system must be released (unmount fs, ..., exportvg) prior to running db2acsutil delete. This can be done with the 'tsm4acs -f unmount' command.

Related reference

"Example target volumes file (SAN Volume Controller configuration)" on page 207
Refer to this example when editing the target volumes file for an SAN Volume Controller storage subsystem configuration.

SAP® backint profile overview

The SAP® backint profile is considered an extension of the Data Protection for Snapshot Devices profile in an SAP® with Oracle configuration.

The SAP® backint profile is typically the same profile used by Tivoli Storage Manager for ERP. The linkage between the two reflects the fact that requests made using the SAP® BR*Tools utilities can specify either snapshot- or file-based processing, and the parameters for either case are accommodated in the Tivoli Storage Manager for ERP profile when Tivoli Storage Manager for ERP is also installed.

SAP® Backint profile keyword definitions

These profile keywords are directly applicable to the implementation of Data Protection for Snapshot Devices in accordance with the SAP® backint interface.

This implementation pertains to an SAP® with Oracle database configuration. The parameters listed are typically part of the Tivoli Storage Manager for ERP profile, and the formatting requirements for this profile apply. Other parameters in the Tivoli Storage Manager for ERP profile are ignored when the backint interface relates to snapshot operations (backup type 'volume'). Conversely, the snapshot-only parameters are ignored when operating in the non-snapshot (backup type 'file') mode employed by Tivoli Storage Manager for ERP.

The following parameters are described in "Data Protection for Snapshot Devices profile parameters" on page 164.:

- ACSD

- DEVICE_CLASS
- LVM_FREEZE_THAW
- MAX_SNAPSHOT_VERSIONS
- TARGET_DATABASE_SUSPEND
- TSM_BACKUP_FROM_SNAPSHOT

The following parameters are described in the documentation for Tivoli Storage Manager for Enterprise Resource Planning:

- TRACE
- TRACEFILE

BR*Tools configuration profile (.sap)

This configuration profile is located in the $ORACLE_HOME/dbs directory on AIX or Linux systems.

This configuration refers to the following keywords within that profile:

`backup_type`
Identifies the default type of the database backup. This parameter is only used by brbackup (default is `offline`).

`backup_dev_type`
Determines the backup medium that will be used (default is tape). In order to use the backint interface this parameter must be set to one of the values listed below. For RMAN, this parameter is set to 'rman_util'.

`util_par_file`
This parameter specifies where the parameter file, which is required for a backup with an external backup program, is located.

`util_vol_access`
Specifies the accessibility of snapshot backup volumes

- none (required on the production system)
- copy
- mount (required on the backup system if BR*Tools installed on the backup system)
- both

`util_vol_nlist = (<nfile_name1>, <nfile_name2>, ...) | no_check`
This parameter defines a list of non-database files or directories that are located on the database disk volumes but do not need to appear in the list of files to back up in the input file. These files are automatically included in the backup, but are never reported in the BACKINT interface messages, especially not in the #ERRFILE message. During a restore, these files (and possibly fixed files) might be overwritten without prior warning.

no_check deactivates the BACKINT check of the backup volumes. This check makes sure that the backup volumes do not contain either non-database files or database files that belong to a database other than the database to be backed up. When no_check is set, the user takes responsibility for making sure that the database volumes (directories sapdata, origlog, and mirrlog) only contain database files of the database to be backed up. Or, if the database volumes contain either non- database files or database files from a database other than the database to be backed up, the user accepts that such files can be overwritten without warning.

`rman_parms`
When `backup_dev_type` is set to "rman_util", this parameter defines various parameters required for RMAN operation.

Data Protection for Snapshot Devices and Tivoli Storage Manager for ERP support the combinations of the keywords `backup_dev_type` and `backup_type` shown in the table below. To carry out online backups with individual tablespace locking with the external backup program Tivoli Storage Manager for ERP, the SAP® Backup profile parameter must be set or changed as shown below:

```
backup_type      = online
backup_dev_type  = util_volume_online
util_par_file    = <ORACLE_HOME>/dbs/init<SID>.utl
```

Tivoli Storage Manager option files for native Oracle

Tivoli Storage Manager provides these options to assist with setting up the native Oracle environment.

Tivoli Storage Manager option files used by Data Protection for Oracle

Be aware of the names and locations of these Tivoli Storage Manager option files when using Data Protection for Oracle.

- Client system options (dsm.sys)
- Client user options (dsm.opt)
- Data Protection for Oracle options (tdpo.opt)
- RMAN backup script

Files for Data Protection for Snapshot Devices

Be aware of the names and locations of these Data Protection for Snapshot Devices option files.

- Client system options (dsm.sys)
- Client user options (dsm.opt)
- Data Protection for Oracle options (tdpo.opt)
- RMAN backup script

Key files and directories

Certain files and directories are of considerable importance when using Data Protection for Snapshot Devices.

The following tables show the major files and directories involved when using Data Protection for Snapshot Devices in the various database configurations:

Table 50. Key Files and Directories (DB2)

Directory or File	Environment Variable, Vendor Option, Profile Parameter or Option	Default or Recommended Location	Examples and Remarks
DB2 installation directory	DB2DIR	/opt/IBM/db2/<version> or /opt/ibm/db2/<version>	/opt/IBM/db2/V9.5 Applies to a ’root’ installation.
Home directory of DB2 database manager instance owner	HOME, INSTHOME	/home/<DB2 instance owner> or /db2/<DB2 instance owner>	/home/db2inst1
DB2 instance directory		$HOME/sqllib	/home/db2inst1/sqllib
Data Protection for Snapshot Devices installation directory		**AIX**: /usr/tivoli/tsm/acs_<version> **Linux**: /opt/tivoli/tsm/acs_<version>	
DB2 ACS installation directory		<DB2 instance directory>/acs	/home/db2inst1/sqllib/acs Updated by Data Protection for Snapshot Devices installation
Data Protection for Snapshot Devices working directory	ACS_DIR	Default: <DB2 instance directory>/acs Recommended by installer: $HOME/acs	/home/db2inst1/acs
Log/trace directory		<ACS_DIR>/logs	/home/db2inst1/acs/logs See “Log and trace files summary” on page 228.
ACS shared directory		<ACS_DIR>/shared	/home/db2inst1/acs/shared
Password file		<ACS_DIR/shared/pwd.acsd	See “Data Protection for Snapshot Devices password file” on page 188.
Snapshot backup library		libacsdb2.a (AIX) libacsdb2.so (Linux)	
Data Protection for Snapshot Devices license file		<DB2 instance directory>/acs/tsmacs.lic	
Profile	PROFILE -p profile	Default: <DB2 instance directory>/acs/profile Recommended by installer: $HOME/acs/profile with link to this file from <DB2 instance directory>/acs/profile	**Profile:** /home/db2inst1/acs/profile **Link:** /home/db2inst1/sqllib/acs/profile –> /home/db2inst1/acs/profile See “Options for DB2 Advanced Copy Services and Data Protection for Snapshot Devices commands” on page 136 and “Data Protection for Snapshot Devices commands and scripts” on page 133.

Table 50. Key Files and Directories (DB2) (continued)

Directory or File	**Environment Variable, Vendor Option, Profile Parameter or Option**	**Default or Recommended Location**	**Examples and Remarks**
Target volumes file directory	VOLUMES_ DIR	Default: None. Recommended by installer: $HOME/acs/acsvolumes	/home/db2inst1/acs/acsvolumes Recommended not to reside in <DB2 instance directory> See notes.
ACS repository directory	ACS_ REPOSITORY	Default: None. Recommended by installer: $HOME/acs/acsrepository	/home/db2inst1/acs/acsrepository Recommended not to reside in <DB2 instance directory> See notes.
Target volumes file(s)		<VOLUMES_DIR>/<filename>	See notes and "Data Protection for Snapshot Devices Target Volumes File (.fct)" on page 189.

Note:

1. By convention, the DB2 instance will be created in $HOME of the DB2 instance owner.
2. For SAN environments, VOLUMES_DIR and ACS_REPOSITORY must be accessible via NFS from all production DB2 nodes and the backup server(s). VOLUMES_DIR is required only for hardware types DS8000, DS6000, ESS800, and SVC.
3. The directory specified by ACS_REPOSITORY will be created by Data Protection for Snapshot Devices and must not exist at the time of initial configuration. The path to this directory must exist, however.

Table 51. Key Files and Directories (Native Oracle)

Directory or File	**Environment Variable, Vendor Option, Profile Parameter or Option**	**Default or Recommended Location**	**Examples and Remarks**
Data Protection for Snapshot Devices installation directory		**AIX:**: /usr/tivoli/tsm/acs_<version>/oracle/bin	
Data Protection for Snapshot Devices working directory	ACS_DIR	Recommended by installer: $HOME/acs, where $HOME is the home directory of the Oracle instance owner ora<SID>, where <SID> is the value of ORACLE_SID.	/oracle/C21/acs
Log/trace directory		<ACS_DIR>/logs	/oracle/C21/acs/acs/logs See "Log and trace files summary" on page 228.
ACS shared directory		<ACS_DIR>/shared	/oracle/C21//acs/acs/shared
Password file		<ACS_DIR/shared/pwd.acsd	See "Data Protection for Snapshot Devices password file" on page 188.

Table 51. Key Files and Directories (Native Oracle) (continued)

Directory or File	Environment Variable, Vendor Option, Profile Parameter or Option	Default or Recommended Location	Examples and Remarks
Data Protection for Snapshot Devices license file		<ACS_DIR>/tsmacs.lic	/oracle/C21/acs/tsmacs.lic
Profile	PROFILE -p profile	Recommended by installer: $HOME/acs/profile with link to this file from <Oracle instance directory>/acs/profile	Profile: /oracle/C21/acs/profile
Target volumes file directory	VOLUMES_ DIR	Default: None. Recommended by installer: $HOME/acs/acsvolumes	/oracle/C21/acs/acsvolumes See notes.
ACS repository directory	ACS_ REPOSITORY	Default: None. Recommended by installer: $HOME/acs/acsrepository	/oracle/C21/acs/repository See notes.
Target volumes file(s)		<VOLUMES_DIR>/<filename>	See notes and “Data Protection for Snapshot Devices Target Volumes File (.fct)” on page 189.
Data Protection for Oracle options file		tdpo.opt	
TSM client system options file		dsm.sys	
TSM client user options files		dsm.opt	

Note:

1. For SAN environments, VOLUMES_DIR and ACS_REPOSITORY must be accessible via NFS from all production nodes and the backup server(s). VOLUMES_DIR is required only for hardware types DS8000, DS6000, ESS800, and SVC.
2. The directory specified by ACS_REPOSITORY will be created by Data Protection for Snapshot Devices and must not exist at the time of initial configuration. The path to this directory must exist, however.

Appendix A. Data Protection for Snapshot Devices examples

Refer to these Data Protection for Snapshot Devices examples when configuring, updating, or performing product tasks.

Examples (DB2)

Example overall disk layout for a DB2 environment

Refer to this example when configuring the disk layout for a DB2 environment.

The following figure shows file systems involved in an example disk layout.

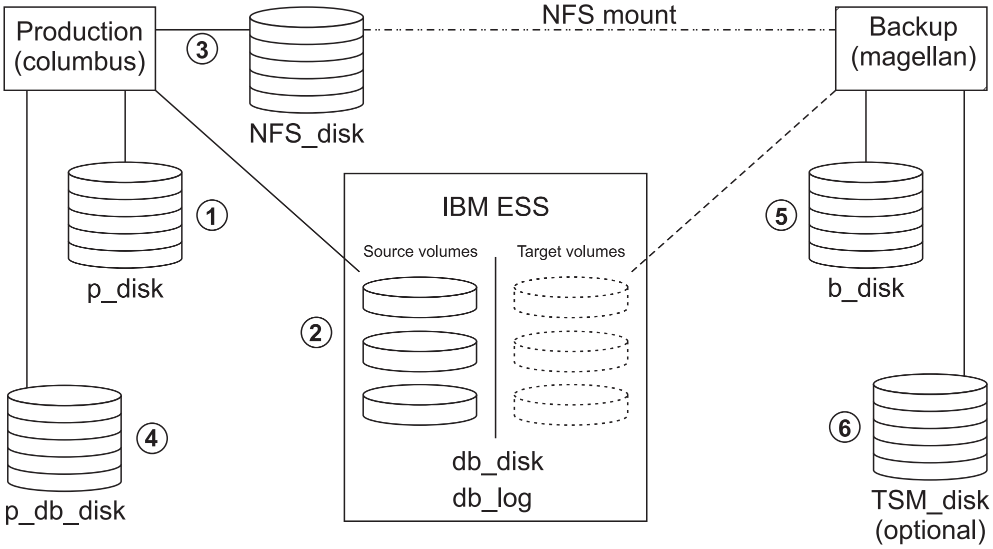


Figure 9. Example Overall Disk Layout

The respective disk categories contain the following disk types that are used for the various file systems:

1. Local disks on the production system (p_disk category) for the file systems

```
/db2/D01
/db2/D01/db2dump
/db2/D01/db2event
/db2/D01/sqllib
/sapmnt/D01
/usr/sap/D01
/usr/sap/trans
/opt/IBM/db2/V9.5
```

2. Source volume disks on the production system (db_disk category) for the file systems

```
/db2/D01/sapdata1
/db2/D01/sapdata2
/db2/D01/sapdata3
/db2/D01/sapdata4
/db2/D01/sapdata5
/db2/D01/sapdata6
/db2/D01/sapdatat
/db2/D01/db2d01
```

Source volume disks on the production system (db_log category) for the file system

```
/db2/D01/log_dir
```

3. 'Shared disks' on the production system (NFS_disk category) for the directory/file system

   ```
   /db2/D01/acs
   ```

4. Local disks on the production system (p_db_disk category) for the file systems

   ```
   /db2/D01/log_archive
   /db2/D01/log_retrieve
   ```

5. Local disks on the backup system (b_disk category) for the file systems

   ```
   /db2/D01
   /opt/IBM/db2/V9.5
   ```

6. Disks for the Tivoli Storage Manager server (TSM_disk category) for the file systems

   ```
   /tsmdb
   ```

Example profile for Data Protection for Snapshot Devices for DB2 Advanced Copy Services

Refer to this example when editing the Data Protection for Snapshot Devices profile.

The following depicts a sample profile:

```
>>> GLOBAL
ACS_DIR <DB2 instance directory>/acs                        # directory for logs, password file, etc.
ACSD <hostname> 57328                                       # <server> <port>
# TRACE NO                                                  # YES | NO
<<<
>>> CLIENT
# BACKUPIDPREFIX DB2___
APPLICATION_TYPE DB2                                        # DB2 | SAP
# TSM_BACKUP NO                                             # YES | NO
# MAX_VERSIONS ADAPTIVE                                     # ADAPTIVE | num
# LVM_FREEZE_THAW AUTO                                      # AUTO | YES | NO
# NEGATIVE_LIST NO_CHECK                                    # NO_CHECK | WARN | ERROR | <path to
#                                           negative list file>
# DEVICE_CLASS STANDARD                                     #
<<<
>>> OFFLOAD
BACKUP_METHOD DB2                                           #
# OPTIONS                                                   # <options string>
# PARALLELISM AUTO                                          # num | AUTO
# NUM_SESSIONS 1                                            # num
# NUM_BUFFERS AUTO                                          # num | AUTO
# BUFFER_SIZE AUTO                                          # num | AUTO
<<<
>>> ACSD
ACS_REPOSITORY <DB2 instance directory>/acs/acsrepository   # *mandatory parameter*
# ADMIN_ASSISTANT NO                                        # NO | <server> <port>
<<<
>>> STANDARD
COPYSERVICES_HARDWARE_TYPE SVC                              #*mandatory parameter* SVC|DS|SAN_NSERIES|NAS_NSERIES
COPYSERVICES_PRIMARY_SERVERNAME <hostname>                  #
VOLUMES_DIR <DB2 instance directory>/acs/acsvolumes         # *mandatory parameter*
# COPYSERVICES_SECONDARY_SERVERNAME                         #
# COPYSERVICES_USERNAME superuser                           #
# SVC_COPY_RATE 80                                          # num
# COPYSERVICES_COMMPROTOCOL HTTPS                           # HTTP | HTTPS
# COPYSERVICES_CERTIFICATEFILE NO_CERTIFICATE               # NO_CERTIFICATE | <certificate file>
COPYSERVICES_SERVERPORT 5999                                # *mandatory parameter*
# FLASHCOPY_TYPE COPY                                       # COPY | INCR | NOCOPY
# COPYSERVICES_TIMEOUT 6                                    # num
# RESTORE_FORCE NO                                          # YES | NO
<<<
```

Examples (native Oracle)

Example overall disk layout for a native Oracle environment

Refer to this example when configuring the disk layout in a native Oracle environment.

The following figure shows file systems involved in a sample disk layout.

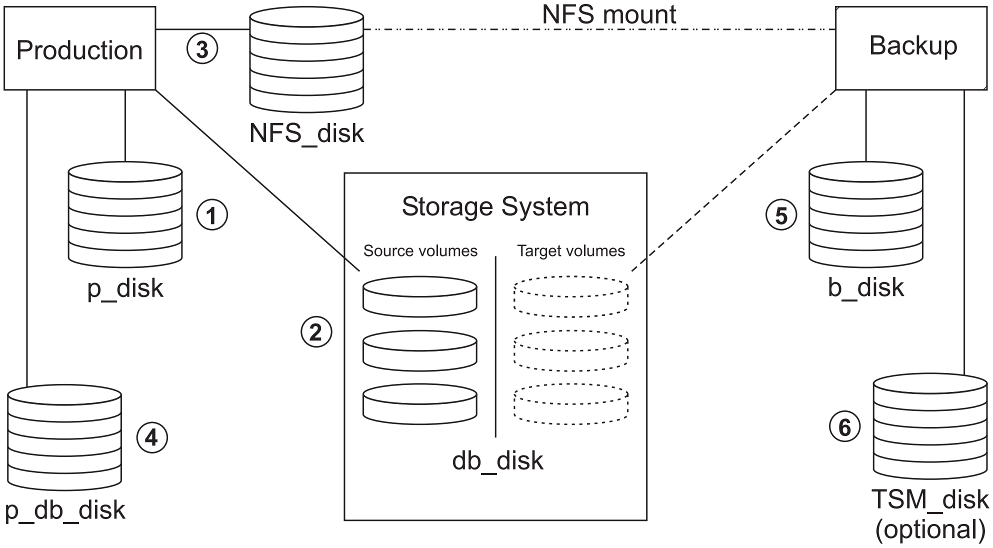


Figure 10. Example Overall Disk Layout

The respective disk categories contain the following disk types that are used for the various file systems:

1. Local disks on the production system (p_disk category) for the file systems

   ```
   /oracle/A01     part of VG ora_main
   ```

2. Source volume disks on the production system (db_disk category) for the file systems

   ```
   /oracle/A01/oradata/system    part of VG ora_d1
   /oracle/A01/oradata/temp      part of VG ora_d2
   /oracle/A01/oradata/custom     part of VG ora_d3

   /oracle/A01/origlogA          part of VG ora_l1
   /oracle/A01/origlogB          part of VG ora_l1

   /oracle/A01/mirrlogA          part of VG ora_l2
   /oracle/A01/mirrlogB          part of VG ora_l2
   ```

   The file systems for the control files must not reside on volume groups that are part of the FlashCopy backup.

   ```
   /oracle/A01/cntrl/cntrlA01.dbf  part of VG ora_main
   /oracle/A01/misc/cntrlA01.dbf  part of VG ora_misc
   /oracle/A01/arch/cntrlA01.dbf   part of VG ora_arch
   ```

3. ’Shared disks’ on the production system (NFS_disk category) for the directories and file systems

   ```
   /oracle/A01/acs
   ```

4. Local disks on the backup system (b_disk category) for the file system

   ```
   /oracle/A01
   ```

There is no need to create separate volume groups for logs and control files.

Example profile for Data Protection for Snapshot Devices for native Oracle

Refer to this example when editing the Data Protection for Snapshot Devices profile.

The following depicts a sample profile:

```
>>> GLOBAL
ACS_DIR /oracle/A10/acs                                         # directory for logs, password file, etc.
ACSD prodsrv 57328                                              # <server> <port>
# TRACE NO                                                      # YES | NO
<<<
>>> CLIENT
APPLICATION_TYPE ORACLE                                         #
TARGET_DATABASE_SUSPEND YES                                     # YES | NO | OFFLINE
# TSM_BACKUP NO                                                 # YES | NO
# MAX_VERSIONS ADAPTIVE                                         # num | ADAPTIVE
# LVM_FREEZE_THAW AUTO                                          # AUTO | YES | NO
# NEGATIVE_LIST NO_CHECK                                        # NO_CHECK | WARN | ERROR | <path to negative list file>
# DEVICE_CLASS STANDARD                                         #
<<<
>>> OFFLOAD
BACKUP_METHOD ORACLE                                            #
# OVERWRITE_DATABASE_PARAMETER_FILE YES                         # YES | NO
# DATABASE_BACKUP_INCREMENTAL_LEVEL 0                           #
<<<
>>> ORACLE
CATALOG_DATABASE_CONNECT_STRING cat_db                          # *mandatory parameter*
CATALOG_DATABASE_USERNAME rman                                  # *mandatory parameter*
DATABASE_BACKUP_SCRIPT_FILE /oracle/A10/acs/tsm_backup.scr      # *mandatory parameter*
TARGET_DATABASE_PARAMETER_FILE /oracle/A10/10gr2/dbs/initA10.ora # *mandatory parameter*
# DATABASE_CONTROL_FILE_RESTORE NO                              # YES | NO
<<<
>>> ACSD
ACS_REPOSITORY /oracle/A10/acs/acsrepository                    # *mandatory parameter*
# ADMIN_ASSISTANT NO                                            # NO | <server> <port>
<<<
>>> STANDARD
COPYSERVICES_HARDWARE_TYPE SVC                                  # *mandatory parameter* SVC | DS | SAN_NSERIES | NAS_NSERIES
COPYSERVICES_PRIMARY_SERVERNAME cim_srv                         #
VOLUMES_DIR /oracle/A10/acs/volumes                             # *mandatory parameter*
# COPYSERVICES_SECONDARY_SERVERNAME                             #
# COPYSERVICES_USERNAME superuser                               #
# SVC_COPY_RATE 80                                              # num
# COPYSERVICES_COMMPROTOCOL HTTPS                               # HTTP | HTTPS
# COPYSERVICES_CERTIFICATEFILE NO_CERTIFICATE                   # NO_CERTIFICATE | <certificate file>
COPYSERVICES_SERVERPORT 5999                                    # *mandatory parameter*
# FLASHCOPY_TYPE COPY                                           # COPY | INCR | NOCOPY
# COPYSERVICES_TIMEOUT 6                                        # num
# RESTORE_FORCE NO                                              # YES | NO
<<<
```

Examples (SAP with Oracle)

Example overall disk layout for an SAP with Oracle environment

Refer to this example when configuring the disk layout in an SAP with Oracle environment.

The following figure shows file systems involved in a sample disk layout.

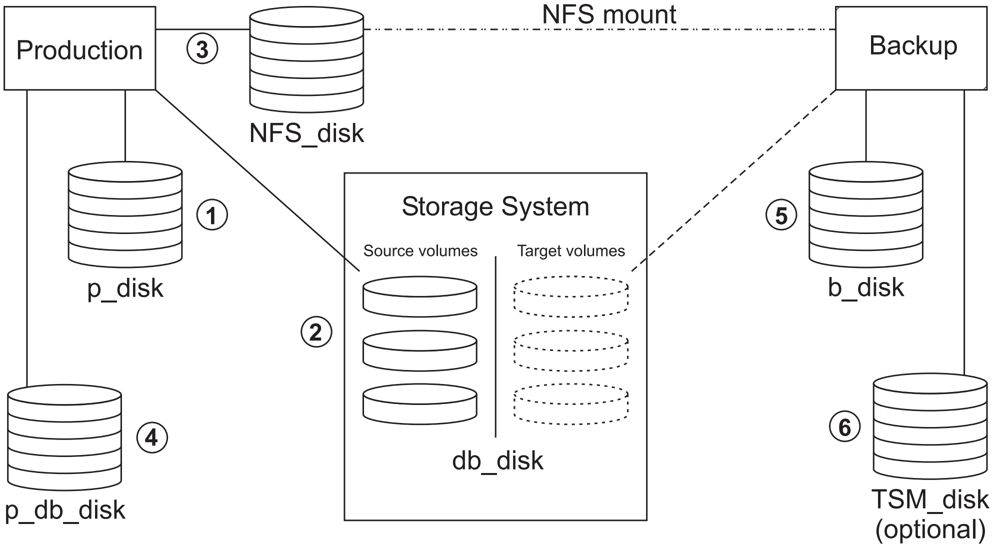


Figure 11. Example Overall Disk Layout

The respective disk categories contain the following disk types that are used for the various file systems:

1. Local disks on the production system (p_disk category) for the file systems

   ```
   /oracle/A01
   /usr/sap/A01
   /usr/sap/trans
   ```

2. Source volume disks on the production system (db_disk category) for the file systems

   ```
   /oracle/A01/sapdata1          part of VG sapfcl1
        /oracle/A01/sapdata2      part of VG sapfcl2
        /oracle/A01/sapdata3      part of VG sapfcl2
        /oracle/A01/sapdata4      part of VG sapfcl3
        /oracle/A01/sapdata5      part of VG sapfcl3
        /oracle/A01/sapdata6      part of VG sapfcl3

        /oracle/A01/origlogA      part of VG sapfcs1
        /oracle/A01/origlogB      part of VG sapfcs1

        /oracle/A01/mirrlogA      part of VG sapfcs2
        /oracle/A01/mirrlogB      part of VG sapfcs2
   ```

   The sapdata<x> file systems were placed in different VGs just for test/development purposes; they could also have been in a common one.

   Usually, brbackup backs up all Oracle control files specified in file $ORACLE_HOME/dbs/init<SID>.ora:

   ```
   /oracle/<SID>/sapdata1/cntrl/cntrl<SID>.dbf
   /oracle/<SID>/origlogA/cntrl/cntrl<SID>.dbf
   /oracle/<SID>/saparch/cntrl/cntrl<SID>.dbf
   ```

   With older releases, only the first Oracle control file specified in init<SID>.ora was part of the FlashCopy backup process.

   To avoid having the file system /oracle/<SID>/saparch and all the disks of its volume group become part of the FlashCopy backup process, it is required to reallocate the control files into file systems that are part of the FlashCopy backup (the ″sapdata<x>″ file systems). The list of control files in $ORACLE_HOME/dbs/init<SID>.ora was changed using the following files:

   ```
   /oracle/A01/sapdata1/cntrl/cntrlA01.dbf
        /oracle/A01/sapdata2/cntrl/cntrlA01.dbf
        /oracle/A01/sapdata3/cntrl/cntrlA01.dbf
   ```

and the affected .dbf files properly recreated in the new locations.

3. 'Shared disks' on the production system (NFS_disk category) for the directories and file systems
```
/oracle/A01/920_64
/oracle/A01/sapbackup
/oracle/A01/sapreorg
/sapmnt/A01
```
4. Local disks on the production system (p_db_disk category) for the file systems
```
/oracle/A01/saparch
```
5. Local disks on the backup system (b_disk category) for the file systems
```
/oracle/A01
/usr/sap/A01
/usr/sap/trans
```
6. (TSM Server) Disks for the Tivoli Storage Manager server (TSM_disk category) for the file systems used for the Tivoli Storage Manager databases, logs, and storage volumes.

Example profile for Data Protection for Snapshot Devices for *SAP® with Oracle*

Refer to this example when editing the Data Protection for Snapshot Devices profile.

The following depicts a sample profile:

```
>>> GLOBAL
ACS_DIR <Home of Oracle instance owner>/acs                     # directory for logs, password file, etc.
ACSD <hostname> 57328                                           # <server> <port>
# TRACE NO                                                      # YES | NO
<<<
>>> OFFLOAD
BACKUP_METHOD BACKINT                                           #
PROFILE <$ORACLE_HOME>/dbs/init<SID>.utl                        # path to UTL file
<<<
>>> ACSD
ACS_REPOSITORY <Home of Oracle instance owner>/acsrepository    # *mandatory parameter*
# ADMIN_ASSISTANT NO                                            # NO | server port
<<<
>>> STANDARD
COPYSERVICES_HARDWARE_TYPE SAN_NSERIES                          # *mandatory parameter* SVC | DS | SAN_NSERIES | NAS_NSERIES
COPYSERVICES_PRIMARY_SERVERNAME <servername>                    #
# COPYSERVICES_SECONDARY_SERVERNAME                             #
COPYSERVICES_USERNAME <username>                                # username for copyservices server
PROD_INITIATOR_GROUP <production system initiator group>        #
BACK_INITIATOR_GROUP <backup system initiator group>            #
<<<
```

Example Target Volumes Files

Example target volumes file (ESS or DS configuration)

Refer to this example when editing the target volumes file for an ESS or DS storage subsystem configuration.

The following three samples illustrate the same environment setup. It is clear that the first one is the most convenient to implement.

```
#=====================================================================#
#===
#===  This file contains setup information about source/target volumes
#===  as they will be used in the FlashCopy function.
#===
#===  The target volumes file identifies the target volumes to be used
#===  for a FlashCopy backup.
#===  The file conforms to the following naming convention:
#===
#===  <dbm-instance>.<database-name>.<device-class>.<partition-num>.fct
#===
#===  where
#===  <dbm-instance> = DB2 instance name
#===  <database-name> = DB2 database alias
#===  <device-class> = device class specified in the DP for Snapshot
#===                   Devices profile or as a vendor option
#===  <partition-num> = 'NODEnnnn', where nnnn = partition number
#===  (leading zeroes)
#===  and resides in the directory specified by the VOLUMES_DIR
#===  parameter in the DP for Snapshot Devices profile.
#===
#===  It is required to embed the TARGET_VOLUME  parameter
#===  between the topic start parameter (>>> volumes_set_x)
#===  and topic end parameter (<<< volumes_set_x), where x
#===  indicates the target volume set you would like to use.
#===
#===
#===
#===  Note: On the parameter statement TARGET_VOLUME, the
#===       1st value  is   target_volume_serial_number
#===       2nd value  is   source_volume_serial_number  or  -
#===       3rd value  is   Size=2.0_GB  or  -
#===
#===       If you specify source volume serial number and size,
#===       you must ensure the target volume size is the same.
#===
#===       A target volume must be available in the same hardware
#===       unit inwhich the source volume is accessed.
#=====================================================================#


#
#*************************** first sample ****************************#
#

>>> volumes_set_1
#=====================================================================#
# For  e a c h  target volume which is planned to be used in the
# FlashCopy operation the volume serial number must be specified as
# the 1st parameter  followed by - -
# The characters '-' will be replaced by a (source) volume serial
# number and the Size found for that source volume (if the size matches
# that of the target volume) by DB2 ACS or DP for Snapshot Devices
# once the FlashCopy function has been has been started on the production
# system and identified all (source) volumes.
#
#
# Replace all statements below with your installation values.
#
# Definition is required for each target volume.
#=====================================================================#
TARGET_VOLUME 11815089 - -
TARGET_VOLUME 11915089 - -
TARGET_VOLUME 11A15089 - -
TARGET_VOLUME 11B15089 - -
TARGET_VOLUME 41015089 - -
TARGET_VOLUME 41115089 - -
<<< volumes_set_1

#=====================================================================#
```

```
#
#************************** second sample ****************************#
#

#=====================================================================#

>>> volumes_set_1
TARGET_VOLUME 11815089 11C15089 -
TARGET_VOLUME 11915089 11D15089 -
TARGET_VOLUME 11A15089 11E15089 -
TARGET_VOLUME 11B15089 11F15089 -
TARGET_VOLUME 41015089 41515089 -
TARGET_VOLUME 41115089 41415089 -
<<< volumes_set_1

#=====================================================================#



#
#*************************** third sample ****************************#
#

#=====================================================================#

>>> volumes_set_1
TARGET_VOLUME 11815089 11C15089 Size=6.1_GB
TARGET_VOLUME 11915089 11D15089 Size=6.1_GB
TARGET_VOLUME 11A15089 11E15089 Size=6.1_GB
TARGET_VOLUME 11B15089 11F15089 Size=6.1_GB
TARGET_VOLUME 41015089 41515089 Size=1.2_GB
TARGET_VOLUME 41115089 41415089 Size=1.2_GB
<<< volumes_set_1
```

Example target volumes file (SAN Volume Controller configuration)

Refer to this example when editing the target volumes file for an SAN Volume Controller storage subsystem configuration.

The following three samples illustrate the same environment setup. It is clear that the first one is the most convenient to implement.

```
#=====================================================================#
#===
#===  This file contains setup information about source/target volumes
#===  as they will be used in the FlashCopy function.
#===
#===  The target volumes file identifies the target volumes to be used
#===  for a FlashCopy backup.
#===  The file conforms to the following naming convention:
#===
#===
#===  <dbm-instance>.<database-name>.<device-class>.<partition-num>.fct
#===
#===  where
#===  <dbm-instance> = DB2 instance name
#===  <database-name> = DB2 database alias
#===  <device-class> = device class specified in the DP for Snapshot
#===                   Devices profile or as a vendor option
#===  <partition-num> = 'NODEnnnn', where nnnn = partition number
#=== (leading zeroes)
#===  and resides in the directory specified by the VOLUMES_DIR
#===  parameter in the DP for Snapshot Devices profile
#===
#===  It is required to embed the TARGET_VOLUMES  parameter
#===  between the topic start parameter (>>>volumes_set_x)
#===  and topic end parameter (<<<volumes_set_x) where x should
#===  indicate the target volume set you would like to use.
#===
#===
#===  Note: On the parameter statement TARGET_VOLUME, the
#===       1st value  is   target_volume virtual disk name
#===       2nd value  is   source_volume virtual disk name  or  -
#===       3rd value  is   Size=2.0_GB  or  -
#===
#===       If you specify source volume name and size,
#===       you must ensure the target volume size is the same.
#===
#===       A target volume must be available in the same SVC cluster
#===       in which the source volume is accessed.
#======================================================================#


#
#************************** first sample ***************************#
#

>>> volumes_set_1
#======================================================================#
# For  e a c h  target volume which is planned to be used in the
# FlashCopy operation the virtual disk name must be specified as
# the 1st parameter  followed by - -
# The characters '-' will be replaced by a (source) volume name
# and the Size found for that source volume (if the size matches
# that of the target volume) by DB2 ACS or DP for Snapshot Devices
# once the FlashCopy function has been started on the production system
# and identified all (source) volumes.
#
#
# Replace all statements below with your installation values.
#
# Definition is required for each target volume.
#======================================================================#
TARGET_VOLUME cluster1 - -
TARGET_VOLUME svdftgt1 - -
TARGET_VOLUME svdftgt2 - -
TARGET_VOLUME svdftgt3 - -
TARGET_VOLUME svdftgt4 - -
TARGET_VOLUME svdftgt5 - -
<<< volumes_set_1

#======================================================================#



#
#************************** second sample ***************************#
#

#======================================================================#

>>> volumes_set_1
TARGET_VOLUME cluster1 svdfsrc1 -
TARGET_VOLUME svdftgt1 svdrsrc2 -
TARGET_VOLUME svdftgt2 svdfsrc3 -
TARGET_VOLUME svdftgt3 svdfsrc4 -
TARGET_VOLUME svdftgt4 svdfsrc5 -
TARGET_VOLUME svdftgt5 svdfsrc6 -
<<< volumes_set_1

#======================================================================#
```

```
#
#*************************** third sample *****************************#
#

#======================================================================#

>>> volumes_set_1
TARGET_VOLUME cluster1 svdfsrc1 Size=6.1_GB
TARGET_VOLUME svdftgt1 svdrsrc2 Size=6.1_GB
TARGET_VOLUME svdftgt2 svdfsrc3 Size=6.1_GB
TARGET_VOLUME svdftgt3 svdfsrc4 Size=6.1_GB
TARGET_VOLUME svdftgt4 svdfsrc5 Size=1.2_GB
TARGET_VOLUME svdftgt5 svdfsrc6 Size=1.2_GB
<<< volumes_set_1
```

Example target volume file (mirror setup on ESS or DS configuration)

Refer to this example when editing the target volumes file for a mirror setup on an ESS or DS storage subsystem configuration.

The following sample illustrates the setup of a target volumes file as it is required to run the FlashCopy backup when the AIX LVM mirrors have been set up in the ESS unit 13158 (see the definition in the ′volumes_set_1′ topic) for one FlashCopy backup run and with the mirrors set up in the ESS unit 12067 (see the definition in the ′volumes_set_2′ topic) for another backup run. The two copy sets of LVs have been set up according to the requirements for setting up a copy set which means that 2 ESS units are needed. Only one of the 3 parameter setup possibilities for the parameter TARGET_VOLUME will be used in this sample:

```
#-----------------Start of sample target volumes file  -----------------------
#===
#===  This file contains setup information about source/target volumes
#===  as they will be used in the FlashCopy function.
#===
#===  The target volumes file identifies the target volumes to be used
#===  for a FlashCopy backup.
#===  The file conforms to the following naming convention:
#===
#===  <dbm-instance>.<database-name>.<device-class>.<partition-num>.fct
#===
#===  where
#===  <dbm-instance> = DB2 instance name
#===  <database-name> = DB2 database alias
#===  <device-class> = device class specified in the DP for Snapshot
#===                   Devices profile or as a vendor option
#===  <partition-num> = 'NODEnnnn', where nnnn = partition number (leading zeroes)
#===
#===  and resides in the directory specified by the VOLUMES_DIR parameter in the
#===  DP for Snapshot Devices profile
#===
#===  It is required to embed the TARGET_VOLUME  parameters
#===  between the topic start parameter (>>>volumes_set_x)
#===  and topic end parameter (<<<<<volumes_set_x) where x should
#===  indicate the target volume set you would like to use.
#===
#===
#===  Note: On the parameter statement TARGET_VOLUME, the
#===       1st value  is   target_volume_serial_number
#===       2nd value  is   source_volume_serial_number  or  -
#===       3rd value  is   Size=2.0_GB  or  -
#===
#===      If you specify source volume serial number and size,
#===      you must ensure the target volume size is the same.
#===
#===      A target volume must be available in the same hardware unit in
#===      which the source volume is accessed.
#-------------------------------------------------------------------#

>>> volumes_set_1
#-------------------------------------------------------------------#
# HARDWARE_ID_LVM_MIRROR
# Defines in an AIX LVM Mirror environment the hardware unit which
# contains a complete set of at least 1 copy of all DB LVs
# which are to be the object of the backup process.
# Only the source volumes of the specified unit will be used
# on the production system by DP for Snapshot Devices for the FlashCopy process.
#
# Possible parameter values :  XXXXX
# where XXXXX is the 5 digit hardware unit number.
#
# Parameter definition can  o n l y  be used if an appropriate
# setup has been done as defined in the DP for Snapshot Devices manual.
#
# DEFAULT : NOT DEFINED
#
#-------------------------------------------------------------------#
HARDWARE_ID_LVM_MIRROR 13158

#-------------------------------------------------------------------#
#
# For  e a c h  target volume which is planned to be used in the
# FlashCopy operation the volume serial number must be specified as
# the 1st parameter  followed by - -
# The characters '-' will be replaced by a (source) volume serial
# number and the Size found for that source volume (if the size matches
# that of the target volume) by DB2 ACS or DP for Snapshot Devices
# once the FlashCopy function has been started on the production system
# and identified all (source) volumes.
#
#
# Replace all statements below with your installation values.
#
#-------------------------------------------------------------------#

TARGET_VOLUME       40913158 - -
TARGET_VOLUME       40A13158 - -
TARGET_VOLUME       40B13158 - -
TARGET_VOLUME       50913158 - -
TARGET_VOLUME       50A13158 - -
TARGET_VOLUME       50B13158 - -
TARGET_VOLUME       51713158 - -
TARGET_VOLUME       51813158 - -
TARGET_VOLUME       52113158 - -
TARGET_VOLUME       52313158 - -
<<< volumes_set_1

>>> volumes_set_2
HARDWARE_ID_LVM_MIRROR        12067
TARGET_VOLUME       65F12067 - -
TARGET_VOLUME       66912067 - -
TARGET_VOLUME       66012067 - -
TARGET_VOLUME       66512067 - -
TARGET_VOLUME       66112067 - -
TARGET_VOLUME       66612067 - -
TARGET_VOLUME       66712067 - -
TARGET_VOLUME       66B12067 - -
TARGET_VOLUME       66212067 - -
TARGET_VOLUME       66312067 - -
```

```
<<< volumes_set_2

#-----------------End of sample target volumes file ----------------------

The above definitions will have been updated by DB2 ACS or
DP for Snapshot Devices once 2 FlashCopy backups -
one with the copyset as defined in volumes_set_1 and
one with the copyset as defined in volumes_set_2 -
have been completed:

>>> volumes_set_1
HARDWARE_ID_LVM_MIRROR 13158
TARGET_VOLUME        40913158 40613158 Size=5.0_GB
TARGET_VOLUME        40A13158 40713158 Size=5.0_GB
TARGET_VOLUME        40B13158 40813158 Size=5.0_GB
TARGET_VOLUME        50913158 50613158 Size=5.0_GB
TARGET_VOLUME        50A13158 50713158 Size=5.0_GB
TARGET_VOLUME        50B13158 50813158 Size=5.0_GB
TARGET_VOLUME        51713158 52213158 Size=1.5_GB
TARGET_VOLUME        51813158 51413158 Size=1.5_GB
TARGET_VOLUME        52113158 51513158 Size=1.5_GB
TARGET_VOLUME        52313158 52013158 Size=1.5_GB
<<< volumes_set_1
>>> volumes_set_2
HARDWARE_ID_LVM_MIRROR        12067
TARGET_VOLUME        65F12067 63F12067 Size=5.0_GB
TARGET_VOLUME        66912067 66812067 Size=1.5_GB
TARGET_VOLUME        66012067 64012067 Size=5.0_GB
TARGET_VOLUME        66512067 64512067 Size=5.0_GB
TARGET_VOLUME        66112067 64112067 Size=5.0_GB
TARGET_VOLUME        66612067 64612067 Size=5.0_GB
TARGET_VOLUME        66712067 64712067 Size=5.0_GB
TARGET_VOLUME        66B12067 66A12067 Size=1.5_GB
TARGET_VOLUME        66212067 64212067 Size=1.5_GB
TARGET_VOLUME        66312067 64312067 Size=1.5_GB
TARGET_VOLUME        66912067 66812067 Size=1.5_GB
<<< volumes_set_2
```

Related concepts

"Overview of Data Protection for Snapshot Devices support for AIX Logical Volume Manager mirrored environments" on page 48

Appendix B. Backup and restore cycles

Information regarding the backup and restore cycles (in terms of their states) is provided to promote better understanding of the processes involved.

This information relates primarily to the basic functionality provided by the Snapshot Backup Library (as it is initiated in DB2 Advanced Copy Services, for example). It also refers to the Data Protection for Snapshot Devices mount and unmount functions in relation to the offload backup operations. The descriptions use DB2 Advanced Copy Services and DB2 commands as examples to illustrate the principles involved.

A snapshot backup will first perform a FlashCopy operation of the source volumes to target volumes on the production system. The target volumes are then made available on the backup system. There, DB2 Advanced Copy Services imports volume groups and mounts the file systems. After the backup completes, the disk environment on the backup system can be restored to its initial state in terms of the DB2 database files. This is possible when no file systems remain mounted and no volume groups remain imported.

DB2 Advanced Copy Services uses a progress status indicator (PSI) to control the status of the participating volumes and of the AIX storage management environment that exists when a DB2 Advanced Copy Services operation completes. This allows the next function to be started only when the PSI has a proper value.

A special snapshot restore is integrated into this product, which integrates the target volumes (created with the COPY or INCR option) in a disk-to-disk restore process as long as those target volumes are still in the state they were in after successful completion of the snapshot operation from the respective source volumes. The background copy within the storage system has been completed. The backup sequence number (BSN) of a backup or restore cycle will be written to the Data Protection for Snapshot Devices run logs.

Related concepts

"Restore methods overview" on page 43
Data Protection for Snapshot Devices allows a database to be restored from one of two locations.

Related reference

"Log and trace files summary" on page 228
Provides information about the log files used during backup and restore cycles.

Backup cycle

A FlashCopy backup cycle is created for each new snapshot backup request.

In order to monitor on the backup system the status of the target volumes (such as mounted file systems) involved in a backup and to run controlled DB2 Advanced Copy Services requests, DB2 Advanced Copy Servicesestablishes a new backup cycle for each new snapshot backup request after first checking whether the disk environment on the backup system is in a state that allows a new DB2 Advanced Copy Services backup to be performed. If DB2 Advanced Copy Services encounters a situation where a new backup fails, the requests terminates and requests that the database administrator to either check the procedure setup or recover from an unexpected failure within the backup run (such as a power failure) that left the disk environment in a state that must be cleaned up.

A new FlashCopy backup request creates a new backup cycle that can be successfully initiated only when these two conditions are met:

1. The preceding backup cycle successfully terminated with the required DB2 Advanced Copy Services function according to the FLASHCOPY_TYPE value as follows:
   - In the case of NOCOPY, use of 'db2acsutil delete' with the DELETE_FORCE option (sets the PSI to PSI_WITHDRAW_DONE) or
   - In the case of INCR or COPY, the snapshot backup is done without TSM backup (PSI is set to PSI_FLASHCOPY_DONE) or the unmount function (which sets the PSI to PSI_UNMOUNT_DONE) was called. In addition to the completed backup cycle, a background copy must have completed. The BSI value is either BSI_DISKONLY or BSI_DISKANDTAPE.
   - In the case of INCR or COPY, if no Tivoli Storage Manager backup or FORCED_MOUNT was requested, a new backup can always be started when the BSI value is BSI_DISKONLY.
2. In the case of a snapshot restore that started a restore cycle within the preceding backup cycle, the restore cycle has terminated completely (RSI_DISKONLY).

   Such a restore cycle can only be seen when a backup with the FLASHCOPY_TYPE value of INCR or COPY has been used for a restore (snapshot restore).

A backup cycle is identified with a unique backup sequence number (BSN) within a specific backup cycle. These control elements are used:

- A PSI to record the status of the used source/volume pairs and the status of the AIX storage management environment on the backup system.
- A BSI to record the status of a backup object (snapshot or Tivoli Storage Manager) with respect to its usability for a future restore.
- An RSI to record the usability of a restored snapshot object with regard to its progress and usability for a new snapshot backup following a snapshot restore.

Restore cycle

A restore cycle is started when an eligible backup is selected for a snapshot restore.

A backup is considered eligible for a snapshot restore when these two conditions are met:

- The original snapshot backup was performed using the COPY or INCR option within the profile.
- The device agent has signaled that the background copy process has completed for all source volume and target volume pairs. The final BSI value must be BSI_DISKANDTAPE or BSI_DISKONLY.

A snapshot restore is performed only with the latest available backup cycle and only when these two conditions exist for the last snapshot backup request:

- The selected backup is eligible for a snapshot restore.
- After a successful backup request, the PSI has been set to PSI_FLASHCOPY_DONE, PSI_MOUNT_DONE, PSI_UNMOUNT_DONE, or PSI_WITHDRAW_DONE.

A restore cycle is considered to be complete only after the device agent detects that all background copy processes are complete. Once the agent has detected this completion, it changes the initial RSI value from RSI_START to RSI_DISKONLY. After a snapshot restore completes successfully, you can restart the database and its applications even if the restore cycle is not yet completed. However, you still must wait for the completion of the restore cycle before the database can be backed up again as a snapshot.

Monitoring the FlashCopy background copy progress

The device agent periodically checks for the completion of the background copy processes when the COPY or INCR option is used for a FlashCopy backup and restore.

This check occurs even after the DB2 Advanced Copy Services function has completed. Once the device agent detects that all processes have completed for all volumes, the device agent performs these two tasks:

- Sets the BSI to BSI_DISKONLY or BSI_DISKANDTAPE (in the case of a FlashCopy backup).
- Sets the RSI to RSI_DISKONLY (in the case of a snapshot restore).

In this way, DB2 Advanced Copy Services knows when the copy process is complete. The purpose of the device agent is to ensure that DB2 Advanced Copy Services will not initiate a FlashCopy for a set of source volumes and target volumes as long as the FlashCopy for the same set of source/target volumes in the other direction has not yet completed for all volumes.

Note: Never use the volume pairs whose copy processes were manually terminated with storage-system tools or other means for a FlashCopy or snapshot restore process, such that the normal processing is outside the control of the device agent. The device agent would not know about this intervention and would misinterpret the information (as reflecting completed copies which in reality they are not). This might cause serious problems if the successfully completed copy is needed. Using such supposedly complete (but in reality incomplete) copies on the production system results in either of these situations:

- result in a broken database and broken AIX storage environment when using an incomplete copy of a FlashCopy Backup within a restore. The BSI would be set by the device agent as BSI_DISKONLY or BSI_DISKANDTAPE because the device agent is not aware of the manual intervention.

  To resolve this situation, you need to manually recreate the AIX storage environment and restore a Tivoli Storage Manager backup.
- result in a broken database and a broken AIX storage environment when creating an incomplete copy of a snapshot restore due to the forbidden premature manual termination of the background copy activities. The RSI would be set by the device agent to RSI_DISKONLY even the copy is incomplete, because the device agent is not aware of the manual intervention.

  To resolve this situation, you might try to perform a snapshot restore rerun; in case this is not successful, you need to manually recreate the AIX storage environment and restore a Tivoli Storage Manager type backup.

Progress status indicator overview

The progress status indicator (PSI) provides information about FlashCopy processing.

The values the PSI can have and their meanings are shown in the following table:

Table 52. Possible Progress Status Indicator (PSI) Values

Value	**Meaning**	**DB2 Advanced Copy Services Function Allowed for Restart**	**Possible Cause of Failure**
PSI_PREPARE_FLASHCOPY	Set on the production system just before the snapshot request is issued to the production system.	Restart the ’db2 backup’ command with the ’use snapshot’ clause after you have fixed the failure cause. See note 1.	• Production system not set up properly
PSI_FLASHCOPY_QUERY	Set on the production system when all source and target volume queries to the Copy Services server have been done.	Restart the ’db2 backup’ command with the ’use snapshot’ clause after you have fixed the failure cause. See note 1.	• Copy Services server not available • Incorrect volume size • Target volume not available • Duplicate target volumes found in `.fct` file
PSI_FLASHCOPY_STARTED	Set on the production system just prior to the snapshot request to the Copy Services server.	Start db2acsutil with the ’DELETE_FORCE’ option to clean up the snapshot backup. Restart ’db2 backup’ with the ’use snapshot’ clause after you have fixed the failure cause.	• Copy Services server not available • Source/target relationship already exists
PSI_FLASHCOPY_DONE	Set on the production system when the snapshot request has successfully finished.	Start db2acsutil with the ’DELETE_FORCE’ option to clean up the snapshot backup, or restart ’db2 backup’ with the ’use snapshot’ clause if the background monitoring has finished.	This is not an error condition.
PSI_MOUNT_STARTED	Set on the backup system when the import volume groups, fsck’s, and mounts have been started.	Start ’tsm4acs -f unmount’ to clean up the backup system after you have fixed the failure cause. Optionally, you can start db2acsutil with the ’DELETE_FORCE’ option to clean up the snapshot repository. Restart ’db2 backup’ with the ’use snapshot’ clause.	• fsck failure

Table 52. Possible Progress Status Indicator (PSI) Values (continued)

Value	Meaning	DB2 Advanced Copy Services Function Allowed for Restart	Possible Cause of Failure
PSI_MOUNT_DONE	Set on the backup system once all the mounts have been done. Normal result when using the snapshot function.	Start ’tsm4acs -f unmount’ to clean up the backup system. Optionally, you can start db2acsutil with the ’DELETE_FORCE’ option to clean up the snapshot repository. Restart ’db2 backup’ with the ’use snapshot’ clause.	Not an error condition
PSI_UNMOUNT_DONE	Set on the backup system once all unmounts have been done.	Start db2acsutil with the ’DELETE_FORCE’ option to clean up the snapshot backup, or restart ’db2 backup’ with the ’use snapshot’ clause.	Not an error condition
PSI_WITHDRAW_STARTED	Set on the production system once ’db2acsutil delete’ has been started with the ’DELETE_FORCE’ option.	Start db2acsutil with the ’DELETE_FORCE’ option to clean up the snapshot backup and then restart ’db2 backup’ with the ’use snapshot’ clause.	Copy Services server not available
PSI_WITHDRAW_DONE	Set on the production system after all source/target volume relationships have been withdrawn. Normal result when withdrawing.	Restart ’db2 backup’ with the ’use snapshot’ clause.	Not an error condition
A new snapshot backup will reset the PSI of the previous snapshot backup.			

Backup status indicator overview

The backup status indicator (BSI) is used by Data Protection for Snapshot Devices to determine whether a snapshot backup has finished so that a snapshot restore can be started for this backup sequence number (BSN).

The values the BSI can have and their meanings are shown in the following table:

Table 53. Possible Backup Status Indicator (BSI) Values

Value	Meaning	Snapshot or Tivoli Storage Manager Restore Function Allowed for Restore	Possible Cause of Failure
BSI_START	Set on the production system when a snapshot backup request is started.	No restore is allowed for this BSN: • The backup to Tivoli Storage Manageris not yet finished (in case it was requested) • FlashCopy background process not yet finished.	Not an error condition

Table 53. Possible Backup Status Indicator (BSI) Values (continued)

Value	Meaning	Snapshot or Tivoli Storage Manager Restore Function Allowed for Restore	Possible Cause of Failure
BSI_DISKONLY	Set on the production system by the background monitoring process when it detects that the FlashCopy background process has finished successfully. Previous BSI state: BSI_START	Only snapshot restore is allowed for this BSN: • The backup to Tivoli Storage Manager is not yet finished (in case it was requested) • FlashCopy background process is finished	Not an error condition
BSI_INVALID	Set on the production system by the device agent when the snapshot run terminates with an error. Set on the backup system by the background monitoring process when it detects an error.	A restore is not allowed for this BSN	• Last FlashCopy run terminated with error • Last FlashCopy run was withdrawn before the BSI was updated to BSI_DISKONLY or BSI_DISKANDTAPE by the background monitoring process

Restore status indicator overview

The restore status indicator (RS)I is used by Data Protection for Snapshot Devices to determine whether a DB2 Advanced Copy Services restore has finished so that a new backup, with a new backup sequence number (BSN), can be started.

The following table shows the values and the meanings of the RSI:

Table 54. Possible Restore Status Indicator (RSI) Values

Value	Meaning	Snapshot Backup Allowed	Possible Cause of Failure
RSI_START	Set on the production system when a snapshot restore is started.	A new snapshot operation is not allowed: • The FlashCopy background process initiated by the last snapshot restore is not yet finished.	Not an error condition
RSI_DISKONLY	Set on the production system by the background monitoring process when it detects that the FlashCopy background process has finished successfully. Previous RSI state: RSI_START	A new snapshot operation is allowed: • The FlashCopy background process initiated by the last snapshot restore is finished.	Not an error condition

Table 54. Possible Restore Status Indicator (RSI) Values (continued)

Value	Meaning	Snapshot Backup Allowed	Possible Cause of Failure
RSI_INVALID	Set on the production system when a snapshot restore terminates with an error. Set on the production system by the background monitoring process when it detects an error.	A new snapshot operation is allowed, but a warning message is shown: • The FlashCopy background process, initiated by the last snapshot restore is not finished. • The administrator has to make sure that the production system is in a valid state, by performing a database restore from Tivoli Storage Manager	Only a warning condition: • last snapshot restore run terminated with error.

Appendix C. Special tasks

These tasks require special settings and procedures.

Special tasks for native Oracle

Information is provided about alternative procedures to adjust Data Protection for Snapshot Devices to your production environment.

These procedures assist with adjusting your production environment:

- Configuring system options files for the same server
- Configuring multiple server stanzas
- Editing your server script
- Restoring hdisks for SDD

Configuring system options files to use the same server

This procedure demonstrates how to configure system options files (dsm.sys) to point to the same Tivoli Storage Manager server.

In these examples, the client user options files (dsm.opt) in the `/usr/tivoli/tsm/client/ba/bin` and `/usr/tivoli/tsm/client/api/bin` directories are defined for a server with a TCPIP address of *arrow.la.xyzcompany.com*.

ba/bin Directory

Example: dsm.opt

```
servername tdphdw
```

Example: dsm.sys

```
servername         tdphdw
   commmethod       tcpip
   tcpport          1500
   tcpserveraddress arrow.la.xyzcompany.com
   passwordaccess   generate
   schedmode        prompted
   nodename         hdworc1
```

api/bin Directory

Example: dsm.opt

```
servername tdporc
```

Example: dsm.sys

```
servername          tdporc
   commmethod       tcpip
   tcpport          1500
   tcpserveraddress arrow.la.xyzcompany.com
   passwordaccess   prompt
   nodename         hdworc1
```

Note: The ***servername*** option in the dsm.opt and dsm.sys files define server stanza names only. The ***tcpserveraddress*** option controls which server is actually contacted.

Configuring multiple server stanzas

This procedure demonstrates how to configure multiple server stanzas in the system options file (dsm.sys).

In order to configure multiple server stanzas in the system options file (dsm.sys), copy the option settings from the Data Protection for Oracle dsm.sys file to the Data Protection for Snapshot Devices dsm.sys file. For example, a combined dsm.sys file for a server with the name *arrow*:

```
servername          tdphdw
   commmethod       tcpip
   tcpport          1500
   tcpserveraddress arrow.la.xyzcompany.com
   passwordaccess   generate
   schedmode        prompted

servername          tdporc
   commmethod       tcpip
   tcpport          1500
   tcpserveraddress arrow.la.xyzcompany.com
   passwordaccess   prompt
```

Defining settings in the server script

A Tivoli Storage Manager server script contains the necessary client steps to coordinate a partially automated backup or a fully automated backup.

You must edit your server script if you place the production executable (hdworcp) or backup executable (hdworcb) in a directory other than the Data Protection for Snapshot Devices default installation directory (`/usr/tivoli/tsm/client/tdphdw/oracle/bin`).

Data Protection for Snapshot Devices provides a sample server script (serverscript.smp.oracle) in the `/usr/tivoli/tsm/client/tdphdw/oracle/bin` directory.

Server Script Parameters

The server script contains the following values:

$1 Specifies the Tivoli Storage Manager node name for the production system.

$2 Specifies the fully qualified path and name of your profile. Your profile contains all necessary database information to successfully perform a backup.

$3 Specifies the Tivoli Storage Manager node name for the backup system. The node name for the backup system must be different from the node name for the production system.

All parameters are required.

Example server script

Below is an example of the server script provided by Data Protection for Snapshot Devices.

```
define clientaction $1 wait=y action=command object="hdworcp backup $2 $3"
if (error) goto end
if (rc_ok) goto step1
exit
step1:
define clientaction $3 wait=y action=command object="hdworcb $1"
if (error) goto end
if (rc_ok) goto step2
exit
step2:
define clientaction $1 wait=y action=command object="hdworcp monitor $2"
end:
exit
```

Restoring hdisks for Subsystem Device Drivers

Data Protection for Snapshot Devices removes the hdisk and vpath devices that correspond to the target volumes after the backup executable (hdworcb) is run on a backup system that has SDD installed.

In order to bring up the hdisk and vpath devices again, you must run the AIX **cfgmgr** command for every path on the SDD device. The output from the AIX **lsvpcfg** command may display fewer hdisk devices for the SDD device than actually exist. You can restore all the hdisks to the vpath device by issuing the following AIX commands:[9]

1. Issue
   ```
   rmdev -l <vpath#>
   ```
2. Issue
   ```
   mkdev -l <vpath#>
   ```
3. Issue
   ```
   lsvpcfg
   ```

   All paths to the SDD device should now display.

---

[9] These steps need to done for all the target volumes.

Appendix D. Troubleshooting Data Protection for Snapshot Devices

Resolving problems encountered when using Data Protection for Snapshot Devices requires tasks specific to the database environment.

Related reference

"Log and trace files summary" on page 228
Log and trace files are update during Data Protection for Snapshot Devices operations.

General troubleshooting procedure

This procedure is valid for all Data Protection for Snapshot Devices applications.

The starting point for problem determination is the log file of the ACS daemon (ascd). In this file, all components involved in the current operation are listed, together with their respective log files. The sample below shows 3 different types of entries in the log file. Messages without a prefix (starting with the timestamp) are issued by acsd itself. This means that the last message (BKI1223W) indicates that acsd is not able to send the performance data to the Administration Assistant.

Messages prefixed with 'DB' are issued by the database client (this is the application which requests the backup operation), while messages prefixed with 'DEV' are issued by the device agent (this is the application with interacts directly with the storage hardware). The numbers after the strings 'DB' or 'DEV' differentiate instances of the same application type. In the sample below (for a DB2 configuration), there are two database clients (0002 and 0003) and two device clients (0001 and 0002) connected to the ACS daemon. The clients all have their own log files. The location of these files is shown in messages BKI1515I and BKI1557I. In case of an error, these files should be checked as well, in order to provide more detailed information.

```
07/08/08 17:41:07 BKI1511I:
====================================================

 New backup operation started for database instance db2as1, database AS1.

====================================================
DB  0002 07/08/08 17:41:07 BKI1510I: New connection received.
DB  0002 07/08/08 17:41:07 BKI1513I: *****> Database client connected: Instance db2as1, database ...
DB  0002 07/08/08 17:41:07 BKI1515I: Client is logging to somehost.mydomain.com:/db2/AS1/acs/logs/...
DB  0003 07/08/08 17:41:07 BKI1510I: New connection received.
DB  0003 07/08/08 17:41:07 BKI1513I: *****> Database client connected: Instance db2as1, database...
DB  0003 07/08/08 17:41:07 BKI1515I: Client is logging to somehost.mydomain.com:/db2/AS1/acs/logs...
DEV 0001 07/08/08 17:41:09 BKI1510I: New connection received.
DEV 0002 07/08/08 17:41:09 BKI1510I: New connection received.
DEV 0002 07/08/08 17:41:09 BKI1514I: *****> Device client connected.
DEV 0002 07/08/08 17:41:09 BKI1557I: Device client is logging to somehost.mydomain.com:/db2/AS1/...
DEV 0001 07/08/08 17:41:09 BKI1514I: *****> Device client connected.
DEV 0001 07/08/08 17:41:09 BKI1557I: Device client is logging to somehost.mydomain.com:/db2/AS1/...
07/08/08 17:41:09 BKI1223W: A Problem occurred during send of performance data to the ...
```

Troubleshooting tips for Data Protection for Snapshot Devices for Oracle

Resolving problems encountered when using Data Protection for Snapshot Devices requires tasks specific to the native Oracle database environment.

If an error condition occurs during a Data Protection for Snapshot Devices event, there are several sources of information you can view to help determine what the problem might be. The sources of information are listed below. If you still encounter problems after reviewing this section, you can contact Tivoli Customer Support for assistance.

Be aware of the following information:

- Make sure to increase the size of the following two Oracle options located in the `$ORACLE_HOME/dbs/init(database_name).ora` file:

  ```
  sort_area_size = 10000000
  sort_area_retained_size = 10000000
  ```

- When using Data Protection for Snapshot Devices to back up an Oracle database, the target database being backed up *cannot* reside on the same volume group as the file system containing $ORACLE_HOME. Make sure that the Oracle Server does not share a volume group with the target database.
- When performing a full offline backup of a database, the target database on the production system must be in ″startup mount″ state at the time **acsora** is issued. Otherwise is will not be possible to restore the resulting backup without performing recovery.

  This RMAN script template will restore the database backed up offline as described in the previous paragraph. It restores control files, datafiles, and opens the database *without* any application of logs. This script must be started with the target database in a ″startup mount″ state:

  ```
  run
  {
  allocate channel ch1 type 'SBT_TAPE' parms
  'ENV=(TDPO_OPTFILE=<full path of tdpo.opt file>)';
  set until scn = <Ckp SCN for backup being restored>;
  restore control file to '<full path of 1st control file>';
  restore control file to '<full path of 2nd control file>';
  restore control file to '<full path of 3rd control file>';
  alter database mount;
  restore
  (database);
  sql 'alter database open RESETLOGS';
  release channel ch1;
  }
  ```

  The database will in an open state and in a new incarnation after this script completes. All that remains is to issue the **reset database** command to RMAN and back up the database again since the previous backups are now rendered unusable since the database is in a new incarnation.

  The `<Ckp SCN for backup being restored>` value is the Checkpoint SCN listed for the backup being restored in the RMAN **list backup** command. For example, the Checkpoint SCN is 32024 in the following list:

```
List of Backup Sets
Key  Recid  Stamp  LV  Set Stamp  Set Count Completion Time
-------------------------------------------------------------
26081 4  469212393 0   469212319      5      06-AUG-02

List of Backup Pieces
Key  Pc# Cp#  Status  Completion Time  Piece Name
----------------------------------------------------
26082 1  1  AVAILABLE   06-AUG-02    05dvf74v_1_1

Lis of Datafiles Included
File  Name          LV Type Ckp SCN  Ckp Time
----------------------------------------------
1   /dev/rmyfilelv    0  Full 32024   06-AUG-02
2   /dev/rmyrollbklv  0  Full 32024   06-AUG-02
3   /dev/rmytemplv    0  Full 32024   06-AUG-02
4   /dev/rmyuserlv    0  Full 32024   06-AUG-02
```

Note that for an offline backup, the Checkpoint SCN should be the same for all of the datafiles.

Guidelines for Oracle variables

Data Protection for Snapshot Devices processing can be impacted when certain Oracle parameter and environment variable settings are not set with appropriate values.

It is recommended that you review this information for clarification.

PFILE parameter

When setting parameters in the profile, make sure the TARGET_DATABASE_PARAMETER_FILE parameter specifies a text-based Oracle initialization parameter file (PFILE) and not an Oracle server file (SFILE). Use of an Oracle server file will cause Data Protection for Snapshot Devices processing to fail. To ensure that Oracle obtains initialization parameter settings from a text-based file and therefore, can access the TARGET_DATABASE_PARAMETER_FILE-specified value successfully, specify the PFILE parameter with the STARTUP command when starting Oracle.

TNS_ADMIN environment variable

This environment variable must be set when the SQL*Plus or Oracle Net configuration files do not reside in their default location.

Data Protection for Snapshot Devices for Oracle miscellaneous errors

Certain unique errors might display when using Data Protection for Snapshot Devices for native Oracle.

If you receive the following errors:

Data Protection for Snapshot Devices fails on the backup system in DBCS locales when the datafile or the path to the datafile contains a DBCS name.

This is an Oracle problem that has been reported to the Oracle development team. The Oracle tar number for this problem is 2367962.999.

The following procedure provides a workaround until the problem is resolved by Oracle:

1. Take the table space that contains the DBCS name in its datafile or the path to its datafile offline.

2. If the DBCS name is in the datafile, rename the DBCS datafile to an English name. If the DBCS name is in the path to the datafile, move the datafile to a path with an English name.
3. Log in to the Server Manager and issue the following command:
   ```
   ALTER TABLESPACE <dbcs_tablespace_name> RENAME DATAFILE
   'dbcs_path/dbcs_datafile' TO 'english_path/english_datafile';
   ```
4. Bring the table space online.
5. Delete the DBCS datafile (if necessary).

Although Data Protection for Snapshot Devices supports table spaces named with DBCS, datafiles or paths to the datafiles that contain DBCS must be renamed to English before running Data Protection for Snapshot Devices.

ANS1132E - ″Backup Access rule already defined for node <*nodename*>. Old rule must be deleted before new one can be defined.″

This message can be ignored. It is logged whenever Data Protection for Snapshot Devices attempts to give another node permission to access a file and the permission was previously granted.

Log and trace files summary

Log and trace files are update during Data Protection for Snapshot Devices operations.

Log and trace files are written to during backup and restore processing by these products:
- DB2
- DB2 Advanced Copy Services
- Oracle
- Data Protection for Snapshot Devices
- Storage system
- CIM
- Tivoli Storage Manager for ERP
- Operating system

Data Protection for Snapshot Devices log and trace files

Refer to these examples of the log and trace files maintained by DB2 Advanced Copy Services and Data Protection for Snapshot Devices.

Data Protection for Snapshot Devices (and DB2 Advanced Copy Services) document each operation in log files. In addition, trace files can be requested via the TRACE parameter in the profile. However, it is recommended to not activate tracing unless specifically requested by IBM Support.

The following table lists the log and trace files maintained by DB2 Advanced Copy Services and Data Protection for Snapshot Devices. These files reside in `<ACS_DIR>/logs`

Table 55. DB2 Advanced Copy Services and Data Protection for Snapshot Devices Log and Trace Files

Component	File
Management Agent (acsd)	acsd.<id>.<type>
Application client (for DB2, the Snapshot Backup Library)	client.<instance>.<db name>.<node>.<id>.<type>

Table 55. DB2 Advanced Copy Services and Data Protection for Snapshot Devices Log and Trace Files (continued)

Component	**File**
Device Agent for CIM Devices	acscim.<db hostname>.<device class>.<node num>.<id>.<type> acscimd.<db hostname>.<device class>.<node num>.<id>.<type>
Device Agent for N Series Devices (SAN)	acsnsan.<db hostname>.<device class>.<node num>.<id>.<type> acsnsand.<db hostname>.<device class>.<node num>.<id>.<type>
Device Agent for N Series Devices (NAS)	acsnnas.<db hostname>.<device class>.<node num>.<id>.<type> acsnnasd.<db hostname>.<device class>.<node num>.<id>.<type>
Device Agent for IBM XIV® Storage System Devices	acsxiv.<db hostname>.<device class>.<node num>.<id>.<type> acsxivd.<db hostname>.<device class>.<node num>.<id>.<type> xivadapter_<id>_<function>.log
Offload Agent (tsm4acs)	tsm4acs.<host>.<id>.<type>tsm4acs d.<host>.<id>.<type>
RMAN (when invoked by Data Protection for Snapshot Devices)	rman.<SID>.id.log

Notes:

- Names ending in ′-d′ are daemon processes (started with ′-D′ option).
- <id> is the date (′yyyymmdd′) for log files written by daemon processes, date and process ID (′yyyymmdd.xxxxxx′) for trace files written by daemon processes or a timestamp (yyyymmddHHMMSS) for log and trace files for other processes.
- <type> is ″log″ or ″trace″.
- <device class> can be a device class specified in the profile or ′all′ if no command line parameter ′-s device class′ was specified for the device agent. It can also be omitted for traces of the device agent.
- <instance> and <db hostname> can be ′undef′ for query/delete requests started with db2acsutil.
- <node num> is the DB2 partition number in the case of DB2 and SAP with DB2. It is ′0′ for Oracle and SAP with Oracle or it can also be omitted for Oracle and SAP with Oracle.
- <function> is backup, delete, restore, mount, unmount or reconcile.

The log file written by the Management Agent should always be used as an entry point. All major events, such as the start of a new operation or errors, are recorded here and references are made from here to the appropriate other logs. The Management Agent starts a new log file every day and records all operations of one day within a single file. If TRACE is set to YES, each component of Data Protection for Snapshot Devices creates an additional trace file, also in the `logs` directory.

Storage system log and trace files

Storage system log and trace files are updated during Data Protection for Snapshot Devices operations.

Consult the documentation for the configured storage system.

CIM log and trace files

CIM log and trace files are updated during Data Protection for Snapshot Devices operations.

Consult the CIM documentation for logging and tracing information. Currently, only the DS Open API and the SAN Volume Controller master console produce log and trace output.

Tivoli Storage Manager for ERP log and trace files

Tivoli Storage Manager for ERP log and trace files are updated during backup and restore operations.

See the section ″How To Find Files Containing Message Output (Log Files)″ in the Tivoli Storage Manager for ERP *Installation and User's Guide* for details concerning logs and traces within Tivoli Storage Manager for ERP.

Important: A trace file can be requested by specifying the TRACEFILE parameter in the Tivoli Storage Manager for ERP profile. However, do not place this file on NFS, because this might cause network problems due to the high volume of trace entries being written.

Appendix E. Internet Protocol Version 6 (IPv6) Support

For AIX and Linux, Data Protection for Snapshot Devices supports both IPv4 and IPv6 for internal communication in that it will run in IPv4, IPv6, and mixed environments. However, it does not take advantage of new IPv6 functionality.

In a mixed environment, the actual communication to be used depends on the network settings of the adapters employed. There is no option to enforce the use of a specific protocol other than by network configuration. Specifically, the acsdservice tries to listen for both IPv4 and IPv6 connection requests if the system is configured accordingly. Connection requests to acsd will be made for the addresses returned by the system for the respective port on the local host. Connection requests to other machines are made for the addresses specified by the user. Wherever TCP/IP addresses can be specified in a command line or a profile parameter, IPv6 addresses are supported. However, where an IP address and a port was traditionally specified in the format:

```
<IPv4 address>:<service or port>
```

the format needs to be changed to

```
<service or port>@<IP address>
```

if the IP address is specified in the IPV6 notation. In the case of a dotted decimal IP4 address, the traditional format can still be used.

The specification of IPv6 addresses assumes that Data Protection for Snapshot Devices is used in an environment in which IPv6 is supported by all hardware and software components involved and has been adequately tested in this environment.

Appendix F. Data Protection for Snapshot Devices Messages

Descriptions of the individual messages issued by Data Protection for Snapshot Devices are provided.

The messages begin with the prefix **BKI**, **EEO**, or **IDS** and are listed in numerical order within each category. For each message, the following information is provided:

- Message number
- Severity code

  The following letters give an indication of the severity of the action that generated the message. The severity codes and their meanings are as follows:

E	Error	Processing cannot continue.
W	Warning	Processing can continue, but problems may occur later.
I	Information	Processing continues. User response is not necessary.

- Explanation
- User Response

BKI Messages

BKI0000E Profile not specified.

Explanation:

Cannot locate the profile.

User response:

Ensure that a profile is available. (Oracle) Note that the BACKINT call must have the following form: *backint -p init<SID>.utl* .

BKI0004E Function not defined.

Explanation:

BRTOOLS, BRBACKUP, or BRARCHIVE passed an invalid argument to Data Protection for SAP.

User response:

Ensure that you have the correct version of BR*Tools installed. Valid functions are: *-f backup* or *-f restore* or *-f password* or *-f delete* or *-f inquire*.

BKI0005I Start of program at: *time*

Explanation:

Data Protection for SAP received control from a BR*Tools utility at the time denoted.

User response:

None.

BKI0006E Type for backup not defined [*type***]. Please use 'file' or 'file_online'.**

Explanation:

Data Protection for SAP expects as the backup type parameter only *file* or *file_online*.

User response:

If you start Data Protection for SAP manually to do a backup, ensure that the type option (`-t`) receives the correct arguments (file or file_online). If your Data Protection for SAP has been invoked by one of the SAP database utilities (for example, **BRBACKUP**), ensure that the SAP backup profile `init<SID>.sap` is customized correctly) .

BKI0007E Mode *mode* **requires the environment variable** *environment variables* **to be set.**

Explanation:

Not all environment variables required have been set. At least *environment variables* where missing.

User response:

Set the missing environment variables.

BKI0008E The environment variable *name* **is not set correctly. The current value is** *value***.**

Explanation:

The value of the environment variable *name* is wrong.

User response:

Set *name* to an appropriate value.

BKI0020I End of program at: *time*

Explanation:

(Oracle) Data Protection for SAP returned control to a BR*Tools utility at the time denoted. (DB2) Program tdppasswd ended at the time indicated.

User response:

None.

BKI0021I Elapsed time: *elapsedtime*

Explanation:

The time needed for the complete backup was *elapsedtime*.

User response:

None.

BKI0023I Time: *current_time***Done:** *saved_bytes (percent) of bytes***Estimated end time:** *end_time*

Explanation:

Finished saving a specific object at *current_time*. The *saved_bytes* amount of the total number of *bytes* have been saved. *percent* shows the percentage. This call will be completed at the estimated *end_time*.

User response:

None.

BKI0024I Return code is: *return code*

Explanation:

A return code of 0 means no errors or warnings occurred. If the return code is 1, at least one warning was issued by the program. If the return code is 2, at least one error message was issued.

User response:

For return codes other than 0, check the run log for warnings or error messages.

BKI0027I Time: *current_time* **Objects:** *current_num* **of** *total_num***in process:** *file_name***MGMNT-CLASS:** *management_class***TSM Server:** *server name***.**

Explanation:

Data Protection for SAP started saving *current_num* files at *current_time*. The total number of files to save is *total_num*. The file *file_name* is currently being processed. The files are transferred to the Tivoli Storage Manager server *server name*, which stores them in the management class *management_class*.

User response:

None.

BKI0032E Error opening file *file name***:** *system error description*

Explanation:

A system error occurred during opening of the file *file name*. *system error description* will describe the error in more detail.

User response:

Read the *system error description*.

BKI0048E No password for node <node> on server <server> given on command line. When entering passwords in batch mode, you must supply values for ALL stanzas in the profile.

Explanation:

The batch mode of the password function requires a data set for all TSM server stanzas in the profile.

User response:

Check the profile for active server stanzas. Use that information and try it again.

BKI0049I Please enter password for node *nodename* **on server** *server name*

Explanation:

The password for the node *nodename* on the Tivoli Storage Manager server *server name* has to be entered for storing it in the DP for SAP configuration file.

User response:

Enter the password for the corresponding Tivoli Storage Manager server.

BKI0050I Please enter password for node *nodename* **on server** *server name* **again**

Explanation:

In order to avoid typing errors, you have to enter the password twice.

User response:

Enter the password again.

BKI0051I Password successfully verified for node *nodename* on server *server name*.

Explanation:

The password for the node *nodename* on the Tivoli Storage Manager server *server name* was changed successfully.

User response:

None.

BKI0052E Password verification for node *nodename* on server *server name* failed.

Explanation:

The password you entered for the node *nodename* on the Tivoli Storage Manager server *server name* was wrong.

User response:

Enter the password again. If this error still exists, contact your Tivoli Storage Manager administrator.

BKI0053I Time: *current_time*Objects: *current_num* of *total_num*done: *file_name* with: *bytes* saved withdescription *object_desc*.

Explanation:

Data Protection for SAP completed saving *current_num* file at *current_time*. The total number of files to be saved is *total_num*. The file *file_name* with the size *bytes* is saved with the description *object_desc*.

User response:

None.

BKI0054I Time: *current_time*Objects: *current_num* of *total_num*done: *file_name* with: *bytes*restored with description *object_desc*.

Explanation:

Data Protection for SAP completed restoring of *current_num* file at *current_time*. The total number of files to be restored is *total_num*. The file *file_name* with the size *bytes* is restored with the description *object_class*.

User response:

None.

BKI0055I Object *objectname* with *size* saved with description *description*.

Explanation:

The object *objectname* was saved successfully.

User response:

None.

BKI0056I Object *objectname* with *size* restored with description *description*.

Explanation:

The object *objectname* was restored successfully.

User response:

None.

BKI0057I Time: *current_time* Object *objectname* with *size* saved with description *description*.

Explanation:

The object *objectname* was saved successfully.

User response:

None.

BKI0058I Time: *current_time* Object *objectname* with *size* restored with description *description*.

Explanation:

The object *objectname* was restored successfully.

User response:

None.

BKI0059E You have to set the environment variable DSMI_CONFIG to the full filename of the Tivoli Storage Manager client option file ’dsm.opt’.

Explanation:

Tivoli Storage Manager client option file not found.

User response:

Verify that the Tivoli Storage Manager option file `dsm.opt` is pointed to by DSMI_CONFIG.

BKI0060E The parameter *parameter* is not known.

Explanation:

The command parameter *parameter* is unknown.

User response:

Check the specified command parameter and try again.

BKI0061W The output file *file name* is not valid.

Explanation:

The specified output file *file name* could not be created.

User response:

Check that *file name* is a valid file name on your operating system. Also check that the application has the appropriate permissions to create the file within the specified directory. The directory must already exist. If the file already exists, rename the old one.

BKI0062E The input file *file name* is not valid.

Explanation:

Unable to read the input file *file name* correctly.

User response:

Check the path and name of the input file and the appropriate file access permission.

BKI0063E The UTL file *file name* is not valid.

Explanation:

Unable to read the input file *file name* correctly.

User response:

Check the path and name of the profile (UTL file) and the appropriate file access permission.

BKI0064E The option *option* is unknown.

Explanation:

An option is invalid or unknown.

User response:

Check the specified option(s) and try again.

BKI0065E The argument is missing for option *option*.

Explanation:

Every option requires an argument.

User response:

Insert the missing argument and try again.

BKI0101I Session *session*: Please enter ’cont’ to continue or ’stop’ to cancel.

Explanation:

If Data Protection for SAP is running in unattended mode (profile keyword BATCH), it terminates the current run if operator intervention is required.

User response:

Enter ’cont’ or ’stop’.

BKI0102I Your reply: *reply*.

Explanation:

The reply you made is confirmed.

User response:

None.

BKI0311E Request canceled by user.

Explanation:

(Oracle) BACKINT terminated at user’s request. (DB2) Program terminated at user’s request.

User response:

None

BKI0400I TDP is waiting for BRBACKUP

Explanation:

Data Protection for SAP is waiting for BRBACKUP to set a table space in the begin/end backup mode.

User response:

None.

BKI0405I TDP waited *num_sec* sec. for BRBACKUP in util_file_online communication.

Explanation:

This message indicates the total amount of time DP for SAP waited for BRBACKUP to set a table space in ″begin backup″ or ″end backup″ mode. The wait time given is the sum of the wait times for all table spaces participating in the backup.

User response:

None.

BKI0410E Cannot open or delete switch file *file name*. Check permissions.

Explanation:

If Data Protection for SAP is not installed correctly (as the root user on UNIX or Linux or administrator group on Windows) then Data Protection for SAP is not able to open the necessary communication file to the SAP system.

User response:

Check the file permission.

BKI0411E Maximum time waiting for BRBACKUP expired.

Explanation:

The SAP database utilities did not respond within the expected time.

User response:

Contact your SAP administrator.

BKI0412E BRBACKUP wasn't able to switch requested table space in BEGIN/END BACKUP mode.

Explanation:

Data Protection for SAP could not continue the backup, because BRBACKUP was not able to switch the requested table space in BEGIN or END backup mode. This is necessary for locking the table space.

User response:

Contact your SAP administrator.

BKI0413E Error while requesting table space switch.

Explanation:

BRBACKUP could not switch table space in BEGIN or END backup mode.

User response:

Contact your SAP administrator.

BKI0414E Error while requesting table space switch.

Explanation:

BRBACKUP reported an error while trying to switch a table space in BEGIN or END backup mode.

User response:

Contact your SAP administrator.

BKI0450I Version 2 restore: *file*

Explanation:

A restore of data backed up with Data Protection for SAP version 2 was executed.

User response:

None.

BKI0452E This version of *product* **has expired.**

Explanation:

This is a test version that has expired.

User response:

Order a release version of the product or contact your IBM/Tivoli Sales Representative.

BKI0453W This version of *product* **will expire in** *number* **days.**

Explanation:

This is a test version with a time limit. It will expire in *number* days.

User response:

Order a release version of the product or contact your IBM/Tivoli Sales Representative before the version expires.

BKI0454I * This copy is NOT FOR RESALE. *****

Explanation:

This version is not for resale.

User response:

None.

BKI0455E License file *file name* **does not exist.**

Explanation:

The license file `agent.lic` was not found where expected.

User response:

Make sure that the `agent.lic` file resides in the same directory as the `init<SID>.utl` file.

BKI0456E Unable to access license file *file name***.**

Explanation:

The license file could not be accessed.

User response:

Make sure the access permissions allow read/write access.

BKI0457E License file *file name* **contains invalid data/checksum.**

Explanation:

The license file is invalid.

User response:

Make sure you have the right `agent.lic` file for the right platform installed. `agent.lic` files are platform dependent.

BKI0458I Fake-Mode is activated.

Explanation:

This message signals that the current operation is a simulated operation. Simulations can be performed using the Administration Assistant.

User response:

None.

BKI0459E **More than one mux file is found with the same name** ***detailed backup description*****.**

Explanation:

Two or more data sources with name *detailed backup description* exist.

User response:

Contact the product administrator.

BKI0460E **No mux file was found with the name <name>.**

Explanation:

A mux file is a data structure holding internal metadata needed for restore puposes. Each backup image gets a mux file assigned.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI0461I **Created tracefile '<tracefile>' for process ID <id>.**

Explanation:

The named trace file has been created.

User response:

None.

BKI1000E **Syntax error in line** ***line*****:** ***statement***

Explanation:

The statement *statement* in the Data Protection for SAP profile is unknown or incorrect.

User response:

Correct the error and try again.

BKI1001E **Syntax error in file** ***file name*****. Exiting Program.**

Explanation:

A syntax error has been detected in the file *file name* and the action has been halted.

User response:

Correct the error(s) in the file *file name* and try again.

BKI1002E **BACKUPIDPREFIX must be** ***number_of_characters*** **characters.**

Explanation:

The length of BACKUPIDPREFIX must be *number_of_characters* characters.

User response:

Enter a BACKUPIDPREFIX with the required length (for example, SAP___, BKI___).

BKI1003W **Please set REDOLOG_COPIES to a number between 1 and** ***max_copies*****. Now it is set to** ***act_copies*****.**

Explanation:

Data Protection for SAP currently supports 1 to 9 copies of offline (redo) log files.

User response:

Adapt the REDOLOG_COPIES settings in the Data Protection for SAP profile.

BKI1004W **You should specify the BACKUPIDPREFIX before the TRACEFILE statement, so that the BACKUPIDPREFIX can be used in the tracefile name.**

Explanation:

The BACKUPIDPREFIX is used to build the Name of the tracefile. Therefore, BACKUPIDPREFIX must be specified before the TRACEFILE statement.

User response:

Define a 6-character BACKUPIDPREFIX in the Data Protection for SAP profile (for example, SAP___, BKI___)

BKI1005W **The tracefile name** ***trace_filename*** **should be absolute.**

Explanation:

None.

User response:

Specify an absolute tracefile name, for example `/oracle/C21/saptrace/tracefile or /db2/C21/saptrace/tracefile .`

BKI1006E **The SERVERNAME must be less than** ***max_char*** **characters.**

Explanation:

You have used a SERVERNAME with more than *max_char* characters.

User response:

Use a shorter SERVERNAME.

BKI1007E The NODENAME must be less than *max_char* characters.

Explanation:

You have used a NODENAME with more than *max_char* characters.

User response:

Use a shorter NODENAME.

BKI1008E The MANAGEMENTCLASSNAME must be less than *max_char* characters.

Explanation:

You have used a MANAGEMENTCLASSNAME with more than *max_char* characters.

User response:

Use a shorter MANAGEMENTCLASSNAME.

BKI1009W Please set MULTIPLEX to a number between 1 and *max_multiplex*. Now it is set to *act_multiplex*.

Explanation:

You have set multiplexing to an unsupported number. Data Protection for SAP now uses *act_multiplex*.

User response:

Set multiplexing to a number between 1 and *max_multiplex*.

BKI1010W The configfile name *configuration_filename* should be absolute.

Explanation:

None.

User response:

Specify an absolute file name, for example `/oracle/C21/dbs/initC21.bki or /db2/C21/dbs/initC21.bki`

BKI1011W The sortfile name *sortfile_filename* should be absolute.

Explanation:

None.

User response:

Specify an absolute file name, for example `/oracle/C21/dbs/sortfile`.

BKI1012E Configfile not found or permission denied: *configuration_filename*.

Explanation:

Data Protection for SAP is unable to read the file *configuration_filename*.

User response:

This error could have various reasons, try the following:

1. Check the path of the configuration file. The path must be specified in the profile (parameter CONFIG_FILE).
2. Make sure that the file access permissions are set correctly.

BKI1013E Profile not found or permissions denied: *profile_filename*.

Explanation:

Data Protection for SAP is unable to open the profile *profile_filename*.

User response:

(Oracle) Ensure that the SAP backup profile `init<SID>.sap` contains a valid entry `util_par_file` for the Data Protection for SAP profile. (DB2) Ensure that the vendor environment file contains a valid entry `XINT_PROFILE`. Furthermore, this file must be readable by Data Protection for SAP.

BKI1016W The trace file name *file name* could not be opened for writing!

Explanation:

The trace file could not be opened for writing.

User response:

Ensure that you have specified a correct path for the trace file.

BKI1017E The server <server> is already defined. Please use another name or specify TCP_ADDRESS!

Explanation:

The named server was already defined in the profile. Server stanzas with identical names are not allowed unless the keyword TCP_ADDRESS is defined in one of them.

User response:

Update the profile accordingly and try again.

BKI1019E Failed to respond to a message received from XINT.

Explanation:

This messages indicates an internal error.

User response:

Contact IBM Support.

BKI1020W The compress info file *file name* should be absolute !

Explanation:

The argument for the parameter COMPR_INFO in the profile is an relative filename.

User response:

Always use an absolute filename as argument for the parameter COMPR_INFO.

BKI1021E *component_name* terminates the connection due to a previous error.

Explanation:

A serious error has occurred which caused a shutdown of the communication channel between the *component_name* process and this application.

User response:

Look for previous error messages to detect the root cause of the problem.

BKI1022E *component_name* terminates the connection due to a previous error.

Explanation:

See message BKI1021E.

User response:

See message BKI1021E.

BKI1023W Could not establish connection to log server *log server name*.

Explanation:

In the Data Protection for SAP profile, log server *log server name* is specified (keyword LOG_SERVER). However, a connection to the server named could not be established. No log records are sent to the log server.

User response:

- Check that the server name defined with keyword LOG_SERVER is spelled correctly in the Data Protection for SAP profile.
- Make sure there is a SERVER section in the profile for the log server defined with keyword LOG_SERVER.
- Check the corresponding SERVER section and correct any setup problems.
- Make sure that the log server named is available.

BKI1024E The file <filename> occurs twice in the <infile>.

Explanation:

The named file name occurs multiple times in the infile which is a violation of the interface specification.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI1200E Cannot read/write file: *file name*.

Explanation:

The program is unable to read or write a data file (file name) of a table space being backed up or restored.

User response:

Check the file access permission of the affected file(s). Try again. If the problem still exists, contact the product's administrator.

BKI1201E There are no Tivoli Storage Manager Servers available.

Explanation:

Data Protection for SAP cannot locate a Tivoli Storage Manager server. This may be due to a configuration problem or to a problem while trying to connect to the Tivoli Storage Manager server. Most probably, a preceding error message points to the cause of the problem.

User response:

Look for and respond to preceding error messages. You may also want to check the Data Protection for SAP profile and the IBM Tivoli Storage Manager client options and client system options files.

BKI1202E You must specify either MAX_SESSIONS, or all three specific session options (MAX_ARCH_SESSIONS, MAX_BACK_SESSIONS, and MAX_RESTORE_SESSIONS).

Explanation:

Information on the number of Tivoli Storage Manager client sessions to be established by Data Protection for SAP is missing from the profile.

User response:

In the Data Protection for SAP profile, either specify a value for keyword MAX_SESSIONS, or specify values for the three specific session parameters (MAX_ARCH_SESSIONS, MAX_BACK_SESSIONS, and MAX_RESTORE_SESSIONS).

Any of the specific options can be specified in combination with MAX_SESSIONS. Then, it overrides the value of MAX_SESSIONS for the specific function.

BKI1203E Not enough sessions available (number of sessions required and number of sessions available).

Explanation:

The sum of available sessions specified in the various server statements (parameter SESSIONS) does not cover the required number of sessions (parameter MAX_SESSIONS).

User response:

Change the values of the corresponding parameters in the Data Protection for SAP profile, so that the condition mentioned in the explanation is fulfilled.

BKI1205E If you want *num_redo* **REDOLOGCOPIES on Tivoli Storage Manager-Server servername, you should give me at least** *num_mc* **different Archive Management Classes.**

Explanation:

Data Protection for SAP requires that the number of different Archive Management Classes (parameter BRARCHIVEMGTCLASS) on the Tivoli Storage Manager servers is equal to or greater than the number of redo log or log file copies (parameter REDOLOG_COPIES).

User response:

Define at least as many different Archive Management Classes as log file copies requested.

BKI1206W If you want *num_redo* **REDOLOGCOPIES on Tivoli Storage Manager Server** *server name***, you should give me at least** *num_mc* **different Archive Management Classes.**

Explanation:

The message appears during a BRBACKUP run. A BRARCHIVE run afterwards would fail.

User response:

Define at least as many different Archive Management Classes as log file copies requested.

BKI1207E Directory backup not supported

Explanation:

This option is not yet available.

User response:

Wait for a future release of Data Protection for SAP, which supports this option.

BKI1208W The object *file name* **will be retried [***retry_num***]**

Explanation:

An error occurred while processing object *file_name*. Data Protection for SAP is repeating the action according to the number of retries specified in the profile. *retry_num* is the current retry count.

User response:

If the problem persists check for and respond to preceding error messages

BKI1209E Object not found or not accessible *objectname***.**

Explanation:

The object cannot be located.

User response:

The backup integrity is affected. Contact SAP or IBM Support.

BKI1210E Input file not found or not accessible *file name***.**

Explanation:

Data Protection for SAP cannot locate the temporary file named. This file contains the list of Oracle objects to be backed up or restored. It is passed to DP for SAP by one of the BR*Tools utilities.

User response:

Ensure that you have the correct version of BR*Tools installed. For details, check with the release notes (RELNOTE).

BKI1211E There is something wrong with your CONFIG_FILE *file name***.**

Explanation:

There is a problem with your Data Protection for SAP configuration file setup.

User response:

Check the file permission and the file name specified in the Data Protection for SAP profile keyword CONFIG_FILE.

BKI1212W The file *file name* was not found in the manual sorting file.

Explanation:

The file you want to back up was not found in the manual sorting file.

User response:

Check and correct the manual sorting file so that it contains all the files you are backing up.

BKI1214E TSM Error: *error text*

Explanation:

The specified TSM error occurred.

User response:

Check *error text* and correct the problem. For further information you may want to refer to *IBM Tivoli Storage Manager Messages*, SC32-9090.

BKI1215I Average transmission rate was *number* **GB/h (***number* **MB/sec).**

Explanation:

The average transmission rate is displayed.

User response:

None.

BKI1216E There are no BRBACKUPMGTCLASSES available.

Explanation:

The BRBACKUPMGTCLASSES you have specified in your `init<SID>.utl` file are not correct.

User response:

Check the management classes on the TSM server and specify correct ones.

BKI1217E There are no BRARCHIVEMGTCLASSES available.

Explanation:

The BRARCHIVEMGTCLASSES you have specified in your init<SID>.utl file are not correct.

User response:

Check the management classes on the TSM server and specify correct ones.

BKI1218E Environment variable TEMP not set.

Explanation:

The required environment setup is incomplete.

User response:

Set the environment variable TEMP and try again.

BKI1222E Version mismatch error. Check setup (version_1:version_2).

Explanation:

Different components with inconsistent versions are used.

User response:

Check your setup or contact IBM Support.

BKI1223W A problem occurred during send of performance data to Administration Assistant .

Explanation:

There was a problem sending the performance data to the Administration Assistant over the network.

User response:

Check your setup or contact IBM Support.

BKI1224W Unable to initialize connection to Administration Assistant.

Explanation:

No operational data could be sent to the Administration Assistant during database backup or restore .

User response:

Check the logs for further information and try again.

BKI1227I Average compression factor was *number***.**

Explanation:

The data transferred had been compressed by the factor *number*.

User response:

None

BKI1228W Server *server name* **can not be used with password access method GENERATE in this environment. The process is running with user ID** *number* **but the effective user ID is** *number***.**

Explanation:

The user ID and the effective user ID of the process are different. In order to utilize the password access method GENERATE the IDs must be equal.

User response:

Change the value for the parameter

″PASSWORDACCESS″ in the file dsm.sys (UNIX and Linux) or *servername*.opt (Windows) from ′generate′ to ′prompt′. Reset the password for this node at the Tivoli Storage Manager server and run (for Oracle) `backint -f password` or (for DB2) `backom -c password` . This prompts you for the password and stores it encrypted in the Data Protection for SAP configfile. Each time your password expires you have to repeat the last step.

BKI1229E Value for parameter BUFFSIZE (actual *cur_number*, maximum *max_number*) is too large for BUFFCOPY mode PREVENT.″

Explanation:

To utilize the BUFFCOPY mode PREVENT the value for the parameter BUFFSIZE must not be larger than *max_number*.

User response:

In the Data Protection for SAP profile, specify a BUFFSIZE less or equal to *max_number* if you need to prevent copying buffers when passing data between Tivoli Storage Manager components. If you need large buffers you can set option BUFFCOPY to SIMPLE or AUTO. As a consequence, buffers are copied when data is passed between Tivoli Storage Manager components.

BKI1230E The following file was not processed: *path*.

Explanation:

The operation was terminated due to a previous error. As a consequence, the file named could not be processed. The cause of the error should be found in an earlier message.

User response:

Check for and respond to preceding error messages.

BKI1231E Maximum number of retries for file <filename> exceeded.

Explanation:

The number of retries configured in the profile keyword ′FILE_RETRIES′ for the named file were reached.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support person

BKI1505E Operation aborted because a different operation by this database client is already running.

Explanation:

Different concurrent operations of the same type were started for the same database. This is not supported. The current operation is aborted.

This message is also issued when a cooperative operation of two or more participating partitions was started, but the profile settings used for the various partitions do not match.

User response:

Wait until the currently running operation has ended and try again. Make sure that multiple operations are not started concurrently for a database.

If this is a cooperative operation with two or more participating partitions, check that the profile settings of the various partitions (for example, DEVICE_TYPE, MAX_VERSIONS, etc.) do not differ. If they do, fix the profile settings, cancel the current operation, and start the operation again. Also, investigate the possibility of sharing the same profile among all partitions.

BKI1506E Failed to execute command *command*. Output follows:

Explanation:

The system tried to execute the command cited. During execution, an error occurred. The output received from the command shell is listed following the message.

User response:

Determine the cause of the problem from the command and the output listed in the message, and resolve the problem.

BKI1507E The process needs to run with root authority.

Explanation:

The current process requires root authority.

User response:

Start the process under an account with root authority.

BKI1508E The service *service_name* has terminated due to a previous error. Please check all logs for additional information.

Explanation:

The cited service is no longer available.

User response:

Check the appropriate logs for the cause of its termination.

BKI1509E Authentication failure. The password specified does not qualify for accessing *component*.

Explanation:

To access the named component, a password is required. However, the password provided could not be verified.

User response:

Make sure that the password files used by the different components of the system match.

BKI1510I New connection received.

Explanation:

The server received a new connection request.

User response:

None.

BKI1511I New *type_of_operation* **operation started for database instance** *instance***, database** *database_name***.**

Explanation:

A connection request resulted in the start of a new operation of the type indicated.

User response:

None.

BKI1512E An error occurred during shutdown: *Error information*

Explanation:

During shutdown of the component, a problem occurred. The error information is given.

User response:

Resolve the problem indicated by the error information.

BKI1513I Database client connected: Instance *instance***, database** *database_name***, partition** *partition_number*

Explanation:

This message follows a message BKI1511I and indicates the connection of one of the database clients taking part in the operation. A database client is an instance of the snapshot backup library representing a single partition of the database.

User response:

None.

BKI1514I Device client connected.

Explanation:

This message follows a message BKI1511I and indicates the connection of one of the device clients taking part in the operation. A device client is an instance of the device agent for the storage device.

User response:

None.

BKI1515I Client is logging to *file_name***.**

Explanation:

The client's log messages are written to the indicated file.

User response:

None.

BKI1517I Deleting target data container defined by *container_description***.**

Explanation:

The data in the container indicated is removed.

User response:

None.

BKI1518E Internal error: The system is trying to use the same device agent, although the synchronization mode is not PARALLEL.

Explanation:

The system has been told to use the same device agent for multiple database clients, but the database indicated serial synchronization mode. This setup is not supported.

User response:

Contact your IBM support personnel.

BKI1519E A failure occurred during initialization of one or more of the nodes participating in this operation. Please check the logs for more information.

Explanation:

Some problem occurred during the initialization of a new operation. The problem may be with any component required for this operation.

User response:

Check the acsd log file for messages BKI1515I to determine the log file names of the participating agents. Check the log files of each component for the cause of the problem.

BKI1520E **Volume *volume_name* is shared across partitions. Volume sharing is not allowed.**

Explanation:

At least two partitions own data residing on the volume indicated. This setup is not supported.

User response:

With the current disk layout of the database, the requested function cannot be used. If you want to use the function, change the disk layout of the database so that each data volume is dedicated to a partition.

BKI1521I **Retaining *number* backups**

Explanation:

When enforcing profile parameter MAX_VERSIONS, the indicated number of backups is kept.

User response:

None.

BKI1522E **The requested meta-information (subject="*description*") is not available.**

Explanation:

Some meta-information about each backup is stored in the repository. An error occurred when trying to retrieve part of this information.

User response:

Contact your IBM support personnel.

BKI1523W **Warning: The following containers were reused without being explicitly released:** *description*

Explanation:

The containers defined by the description are used by the current backup. They were used before by a different backup. This message is expected in SAN environments where data containers are usually kept until they are reused. In this case, this message does not indicate a problem.

User response:

None.

BKI1525E **The process *service_name* is in an inconsistent state. Please check for previous errors and restart the process afterwards.**

Explanation:

The process indicated cannot continue with inconsistent data.

User response:

Check the logs for messages pointing to the cause of the inconsistency. After resolving any problems, restart the process.

BKI1526E **A configuration file (profile) must be provided.**

Explanation:

An operation was started without providing a profile.

User response:

Check the user documentation on how to provide the profile to the current process. Start the process again using a valid configuration file.

BKI1529E **The device '*device_type*' you entered is not supported by the wizard.**

Explanation:

The device type represents a certain type of storage device. While using the setup wizard, a device type was entered that is not supported by the current version of the wizard.

User response:

Refer to your user documentation for a list of the device types that are supported by default. Specify one of the supported types.

BKI1530E **Failed to launch the device agent for *device_type*. Please consult your user documentation to make sure that all requirements for the specified device are met.**

Explanation:

The system was unable to launch the appropriate device agent for the type indicated because some of its requirements are not met.

User response:

Refer to your user documentation and make sure that the system is set up correctly for the specified device type.

BKI1534E **Unexpected version *actual_version* of the repository located in *path*. Expected version:** *supported_version*

Explanation:

The server located the repository in the path indicated. However, the version of the repository located on disk does not match the current version of the server.

User response:

Make sure to use the correct instance of the server. Ensure that the path of the repository was specified correctly. Refer to the release notes for a list of possible incompatibilities.

BKI1535E **Unexpected characteristics (bitwidth=*number*) of the repository located at *path*. Expected bitwidth:** *number*

Explanation:

The repository located in the path indicated was saved to disk using a bit width different from the bit width the server is using to load the repository.

User response:

Make sure to use the correct instance of the server. Ensure that the path of the repository was specified correctly. Refer to the release notes for a list of possible incompatibilities.

BKI1536E **The repository located at *path* is not valid.**

Explanation:

A repository could not be found at the location indicated by *path*.

User response:

Ensure that the path of the repository was specified correctly. Do not edit any files in the repository *path*.

BKI1537E **The repository located at *path* was written with an incompatible protocol (*protocol_version*). Expected protocol:** *protocol_version*

Explanation:

The repository found at the location indicated was written to disk using the protocol version named. However, the server currently supports the expected protocol version.

User response:

Ensure that the path of the repository was specified correctly. Do not edit any files in the repository *path*.

BKI1538E **Unexpected repository type. The path ′*path*′ does not point to a repository of type "*protocol_type*".**

Explanation:

The repository located in the path indicated was written to disk using a protocol different from the protocol supported by the server process.

User response:

Make sure to use the correct instance of the server. Ensure that the path of the repository was specified correctly. Refer to the release notes for a list of possible incompatibilities.

BKI1539E **Root privileges required. Could not change user ID to root.**

Explanation:

The requested operation requires root privileges. However, the process could not acquire them.

User response:

Make sure the appropriate privileges (s-bit) are granted to the executable.

BKI1540E **/etc/inittab entries are limited to 127 characters. Please consult your user documentation for information on manually completing the installation procedure.**

Explanation:

The command line generated by the setup function exceeds 127 characters. This situation requires user intervention. The setup function did not update /etc/inittab.

User response:

Refer to your user documentation for information on what entries to add to /etc/inittab.

BKI1541E **/etc/inittab was not updated because some of the processes have apparently already been added. Please re-run the setup after calling the setup script with option ′-a disable′ if you want to change to a standard setup.**

Explanation:

During the automatic setup, entries for this product were detected in /etc/inittab. This is an indication that the product was not previously uninstalled.

User response:

Run the setup with option ′-a disable′ and then start the installation process again. If the entries in /etc/inittab should be retained, refer to your user documentation for information on how to complete the installation manually.

BKI1542E **Failed to uninstall because some of the processes to be uninstalled are still listed in /etc/inittab. Please re-run the setup after stopping the component by calling the setup script with option ′-a stop′.**

Explanation:

Before uninstalling the product, the affected processes must be stopped. This is done by running the setup script with the option ’-a stop’, which will remove the entries from /etc/inittab and stop the processes.

User response:

Refer to your user documentation for information on the uninstall process. Run the setup with the option ’-a stop’ and then continue uninstalling.

BKI1543E The component is still referenced within the /etc/inittab. In order to terminate the component rerun the setup script with option ’-a stop’.

Explanation:

The setup utility detected that the product is still active in the system. Apparently, its entries in /etc/inittab are not yet removed.

User response:

Call this process again with the option ’-f stop’.

BKI1544E New entries cannot be added to /etc/inittab because it already contains too many entries starting with ’ac’. Please refer your user documentation for a manual setup of this package.

Explanation:

During setup, an unusually high number of entries beginning with ’ac’ were detected in /etc/inittab. /etc/inittab was not modified.

User response:

Determine if these entries are expected, or if they were added due to a problem. If these entries are required, refer to your user documentation for information on how to complete the installation manually.

BKI1545E IBM Tivoli Storage Manager for Advanced Copy Services is currently running.

Explanation:

This failure happens during (de)installation and indicates that not all TSM for ACS components could be stopped.

User response:

Check that no backup or restore is currently running and retry the operation. If you have customized the process of starting TSM for ACS, it might be necessary to manually stop it by undoing those customization steps.

BKI1546E IBM Tivoli Storage Manager for Advanced Copy Services was not started.

Explanation:

This failure happens during installation and indicates that not all TSM for ACS components could be started successfully.

User response:

Check that all TSM for ACS components have the appropriate access rights and retry the operation. Contact the support function if the operation continues to fail.

BKI1547E Failed to remove the data associated with the deleted backup ***backup_id*****.**

Explanation:

The backup named was deleted. However, its data could not be removed from the repository and from the storage device.

User response:

Look for a previous message pointing to the cause of the problem. Resolve any problems indicated there. Once the cause of this problem is resolved, the daemon will take care of the deleted backups eventually.

BKI1548E Failed to monitor the data associated with the deleted backup ***backup_id*****.**

Explanation:

A background daemon is supposed to monitor the states of backups in order to determine if data needs to be deleted from the storage device. However, the monitor was not able to access the appropriate data.

User response:

Look for a previous message pointing to the cause of the problem. Resolve any problems indicated there. Once the cause of this problem is resolved the daemon will take care of the deleted backups eventually.

BKI1549E Failed to load *component_name* **due to the following reason:** *error_information***.**

Explanation:

The system was unable to load the named component of the product.

User response:

Check the error information given in the message. Resolve any problem indicated.

BKI1550W Unable to perform required operations for container ’<container>’ for <time>.

Explanation:

Any operation for the named container is suspended for the named period of time due to it is locked.

User response:

As soon as the container was unlocked, retry the required operation.

BKI1553I ***Component_name*** **is logging to** ***path*****.**

Explanation:

The file denoted is the log file of the named component.

User response:

If you need to check the log of the indicated component, look for this message to identify the log file to examine.

BKI1554W The agent ’*component_name*’ terminated with exit code *number.*

Explanation:

The process denoted ended with the given exit code.

User response:

Check the agent’s log for any messages pointing to a problem. Resolve any problem indicated.

BKI1555I Profile successfully created. Performing additional checks. Make sure to restart all ACS components to reload the profile.

Explanation:

The setup wizard created a new profile. The profile will be validated.

User response:

Restart the ACS components after the wizard ends, in order to activate the new settings.

BKI1556E Some data of backup *backup_id* are unavailable. It is impossible to restore the data requested.

Explanation:

The system detected that some of the data originally contained in the backup is no longer available. The occurrence of this message depends on the type of storage device employed. For example, if an earlier backup data was restored from an N-Series device, some data of a later backup will be destroyed.

User response:

The backup is no longer complete and cannot be used for the requested operation. Try the operation with a different backup.

BKI1557I Device agent is logging to *path*.

Explanation:

The device agent’s log messages are written to the file named.

User response:

None.

BKI1558E There are no mount agents registered for participant(s) *participant_list*

Explanation:

During a snapshot backup run, TSM for ACS detected that for the listed participant(s) no TSM for ACS device agent was started with the ’force mount’ (-F) option. Typically, a participant corresponds to a DB2 partition. The current snapshot backup run will be deleted.

User response:

Make sure that for each participant (DB2 partition) a TSM for ACS device agent is started with the mount force option (-M) on the offload system.

BKI1559E Failed to verify consistency of data container (*data_container*)

Explanation:

During a snapshot backup run, TSM for ACS detected that the listed data container (typically an AIX volume group or an N Series volume) could not be imported/mounted successfully on the offload system. The current snapshot backup run will be deleted.

User response:

Check the TSM for ACS device agent log/trace file for errors and restart the snapshot backup after the problem is corrected.

BKI1560E Not all file systems have been validated by the mount agents!

Explanation:

During a snapshot backup run, TSM for ACS detected that not all file systems could be mounted successfully on the offload system. The current snapshot backup run will be deleted.

User response:

Check the TSM for ACS device agent log/trace file for errors and restart the snapshot backup after the problem is corrected.

BKI1561E **Profile name <profile_name> does not point to a file.**

Explanation:

The profile specification should be a fully qualified filename. Otherwise, it is assumed to be relative to the current directory of the command that issues the message, which may not be the desired directory.

User response:

Correct the name.

BKI1562E **Deleting the backup as requested is impossible while any part of it is mounted.**

Explanation:

A request was sent to delete a backup. However, some parts of the backup were still mounted. Presumably, a restore operation or an off-loaded tape backup is pending or in progress. Please note that an offloaded tape backup requires the snapshot backups of all partitions of the database.

User response:

Wait until the operation in progress has ended, then issue the delete request again.

BKI1563I **The snapshot backup defined by timestamp** *timestamp* **for instance** *instance***, database** *database_name***, and partition** *partition_number* **cannot be restored.**

Explanation:

This message appears when backups are queried for a restore. It indicates that a snapshot backup was encountered that is not in a restorable state. For example, snapshot backups created with a FLASHCOPY_TYPE of NOCOPY are not restorable. When queried for restore, unrestorable snapshot backups are not returned to the caller and therefore cannot be selected for restore.

User response:

None.

BKI1564W **Backup <id> is marked for deletion. You need to unmount before it can be physically deleted.**

Explanation:

A snapshot backup with the named id can only be deleted if all of its assigned file systems are unmounted successfully.

User response:

Issue the offload agent with the command ’-f unmount’. After all resources are freed, the deletion of the snapshot backup will be started.

BKI1568I **Removing backup <*backup_id*> from the repository because it has not been found on the storage device during reconciliation.**

Explanation:

During reconciliation the backup with id <*backup_id*> has not been found on the storage device. Therefore it is deleted from the repository to keep the repository and the valid backups on the storage in sync.

User response:

None.

BKI1569I **Updating backup <*backup_id*> in the repository because some parts of it have not been found on the storage device during reconciliation.**

Explanation:

Some parts of the backup with id <*backup_id*> have not been found on the storage box. The backup will be marked as incomplete in the repository and is not restorable anymore.

User response:

None.

BKI1570W **The following container could not be deleted from the storage box during reconciliation: <*volume_name*>.**

Explanation:

The volume <*volume_name*> could not be deleted from the storage box. It is not needed anymore because there is no corresponding backup in the repository.

User response:

Ignore the warning or try to delete the volume from the storage device manually.

BKI1571W **The specified value for ’RECON_INTERVAL’ is 0. Be aware that every time a background monitor is started a reconcile will be scheduled so that other background operations will never be scheduled. This should be used for testing purposes only.**

Explanation:

If RECON_INTERVAL is 0 every time a background monitor is started it will start reconciliation. Other background operations as deletion or monitoring will never be scheduled.

User response:

Change RECON_INTERVAL to a value greater than 0 if you want to avoid this behavior.

BKI1572I Starting reconciliation for device class <*device_class_name*>.

Explanation:

The reconciliation will be started for the device class <*device_class_name*> of the profile.

User response:

None.

BKI1573I The container <*volume_name*> has been successfully deleted from the storage box. It didn't belong to any backup in the repository.

Explanation:

The volume <*volume_name*> has been successfully deleted from the storage box during reconciliation because it didn't belong to any backup in the repository.

User response:

None.

BKI2000I Successfully connected to *component_name* on port *portnumber*.

Explanation:

One of the Data Protection for SAP modules BACKINT or theThe backup library *libtdp_r3* initiated a successful connection to the background process *component_name* on port *portnumber*.

User response:

None.

BKI2001E Socket error while connecting to *component_name*: *reason*.

Explanation:

The background process *component_name* is not running.

User response:

Start *component_name* manually and try again.

BKI2003I File *file_name, BID* deleted.

Explanation:

The file *file_name* with the backup ID *BID* was deleted from the Tivoli Storage Manager.

User response:

None.

BKI2007E Unknown Port: *port*

Explanation:

The port specified for communication between *component_name* and BACKINT or the backup library is unknown.

User response:

Check the port value specified when *component_name* was started. Additionally, check the environment variable *PROLE_PORT* for the BACKINT environment. These two values must match.

BKI2008E Unable to connect to *component_name*.

Explanation:

Internal error.

User response:

Contact IBM Support.

BKI2009I Deleting all versions with version number <= *version_number* on server *server_name*.

Explanation:

All full database backups and their corresponding log file backups will be deleted from Tivoli Storage Manager storage, if their version number is less than or equal to *version_number*.

User response:

None.

BKI2010E Error occurred processing FRONTEND

Explanation:

An error occurred during the frontend processing.

User response:

Check the frontend script/program and the settings in the Data Protection for SAP profile (keyword FRONTEND) and try again.

BKI2011E Error occurred processing BACKEND.

Explanation:

An error occurred during the backend processing.

User response:

Check the backend script/program and the settings in the Data Protection for SAP profile (keyword *BACKEND*) and try again.

BKI2012E Passwords do not match. Try again.

Explanation:

The first and second password you entered do not match.

User response:

Enter the password correctly.

BKI2013I Starting FRONTEND Program.

Explanation:

The frontend program is executing.

User response:

None.

BKI2014I FRONTEND program finished.

Explanation:

The frontend program is finished.

User response:

None.

BKI2015I Starting BACKEND program.

Explanation:

The backend program is executing.

User response:

None.

BKI2016I BACKEND program finished.

Explanation:

The backend program is finished.

User response:

None.

BKI2017I Blocksize is set to *num_bytes* **bytes.**

Explanation:

The operational blocksize is *num_bytes* bytes.

User response:

None.

BKI2022E Unable to change mode of file *file name***:** *description*

Explanation:

Unable to change mode of file '*file name*'. '*description*' may contain the system error text.

User response:

Check the '*description*'. If the error persists, contact your service representative.

BKI2024E Error in connection to *component_name***.**

Explanation:

The connection to *component_name* terminated unexpectedly. This message might be displayed due to previous errors or after an unexpected termination of the *component_name* process.

User response:

Check for other error messages and restart *component_name* if necessary. Try again. If the problem persists, contact IBM Support.

BKI2025E Failed to respond to a message received from *component_name***.**

Explanation:

This is an internal error

User response:

Contact IBM Support.

BKI2026E Unexpected exception in handler: *handler*

Explanation:

This is an internal error.

User response:

Contact IBM Support.

BKI2027I Using TSM API version *your API version* **(compiled with** *compiled with version***).**

Explanation:

Version information about the TSM-API.

User response:

None

BKI2028W Unable to terminate session *session***.**

Explanation:

This is an internal error during cleanup that has no effect on the success of the service.

User response:

None

BKI2029E The requested buffer allocator cannot be instantiated due to the following incompatibility: *expression***.**

Explanation:

This is an internal error.

User response:

Contact IBM Support.

BKI2031E A buffer allocator cannot simultaneously satisfy all of the following properties: *list of properties*

Explanation:

This is an internal error.

User response:

Contact IBM Support.

BKI2033E Cannot instantiate allocator of type *allocator type* **with the following additional properties:** *list of properties*

Explanation:

This is an internal error.

User response:

Contact IBM Support.

BKI2913I Version delete is configured to retain <number> backup generations. Checking for expired backups.

Explanation:

The value assigned to the profile keyword MAX_VERSIONS is equivalent to the named number of backup generations (backup generation = full+incr+logs) to be retained on TSM.

User response:

None.

BKI4000W The attributes of file *file name* **cannot be restored. Reason: errno** *(error_num) error_desc*.

Explanation:

The file *file name* was restored successfully but one or more file attributes (permission, ownership, date/time) of the file *file name* cannot be restored correctly.

User response:

Check the error number *error_num* and the error description *error_desc* to avoid this problem in the future. An initial solution could be to set the appropriate correct permission for the file *file name* manually.

BKI4001E File *file name* **cannot be created. Reason: errno (***error_num***)** *error_desc***.**

Explanation:

The file *file name* to be restored could not be created/written. It is possible, that you do not have the appropriate rights for writing the file *file name* to the destination path.

User response:

Check the error number *error_num* and the error description *error_desc* to avoid this problem in the future. Furthermore, check the write permission of the user who started the restore.

BKI4002E Error during write of file *file name***. Reason: errno (***error_num***)** *error_desc***.**

Explanation:

An error occurs during the restore process of the file *file name*.

User response:

Check the error number *error_num* and the error description *error_desc* to avoid this problem in the future.

BKI4005E Error allocating memory block for file *file name***. BLOCKSIZE may be too large.**

Explanation:

Unable to request new memory blocks during the backup of file *file name*.

User response:

Verify that you have set a valid value for BLOCKSIZE. If you are not sure what value is valid, comment it out so the default value is used. Furthermore, you can check if you have enough RAM available with your machine. Also, check the memory usage during backup. It may be necessary to stop another application, increase memory, or change the configuration.

BKI4007E File *filename* **cannot be read. Reason: errno(***errno number***)** *errno text***.**

Explanation:

Data could not be read due to some system error. Check *errno text* for further information. If this error recurs, this might indicate some hardware problems.

User response:

Contact your system administrator.

BKI4008E File *filename* **cannot be opened. Reason: errno(***errno number***)** *errno text***.**

Explanation:

Could not open the file *file name* due to some system specific problems.

User response:

Contact your system administrator.

BKI4009E Not enough space to write file *file name*. Possible reasons: disk full or ulimit exceeded.

Explanation:

The system rejected a request to write data into file *file name*. The storage media might not have enough free space to keep the file or the system rejected writing the file due to administrative resource constraints such as ulimits.

User response:

Contact your system administrator.

BKI4010E SAP requires the file <filename> to be a regular file.

Explanation:

To be able to support SAP environments the named file has to be a regular file.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI4011W The backup device type (<filetype> <devicetype> <devsubtype>) differs from the restore device type (<filetype> <descr> <descr>) for <name>.

Explanation:

A mismatch between the device types during backup and restore was detected.

User response:

Check the logs for further information.

BKI4012E Unexpected EOF for file '<filename>' after reading <number> bytes.

Explanation:

The end of file was reached unexpectedly.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI4013I CreateFile() with dwFlagsAndAttributes='<attribute>'.

Explanation:

A file with the nmed attribute was created.

User response:

None.

BKI4014E File '<filename>' cannot be accessed. Reason: errno(<number>) <errormsg>

Explanation:

A named file could not be accessed either for reading or writing.

User response:

Check the file permissions and if necessary adjust them accordingly. Try again.

BKI5000E Tivoli Storage Manager Error: *error_message*

Explanation:

During a connection of Data Protection for SAP to Tivoli Storage Manager server, a Tivoli Storage Manager error *error_message* occurred.

User response:

Use the Tivoli Storage Manager Messages guide and correct the Tivoli Storage Manager server error. Try your last action again.

BKI5001E Tivoli Storage Manager Error: *error_message*

Explanation:

During a connection of Data Protection for SAP to Tivoli Storage Manager server, a Tivoli Storage Manager error *error_message* occurred.

User response:

Use the Tivoli Storage Manager Messages guide and correct the Tivoli Storage Manager server error. Try your last action again.

BKI5002E Tivoli Storage Manager Error: *error_message*

Explanation:

See BKI5001E.

User response:

See BKI5001E.

BKI5003E Tivoli Storage Manager Error: *error_message*

Explanation:

See BKI5001E.

User response:

See BKI5001E.

BKI5004W **Tivoli Storage Manager Error:** *error_message*

Explanation:

See BKI5001E.

User response:

See BKI5001E.

BKI5005E **Tivoli Storage Manager Error:** *error_message*

Explanation:

See BKI5001E.

User response:

See BKI5001E.

BKI5006E **Tivoli Storage Manager Error:** *error_message*

Explanation:

See BKI5001E.

User response:

See BKI5001E.

BKI5007E **Tivoli Storage Manager Error:** *error_message*

Explanation:

See BKI5001E.

User response:

See BKI5001E.

BKI5008E **Tivoli Storage Manager Error:** *error_message*

Explanation:

See BKI5001E.

User response:

See BKI5001E.

BKI5009E **Tivoli Storage Manager Error:** *error_message*

Explanation:

See BKI5000E.

User response:

See BKI5000E.

BKI5010E **Tivoli Storage Manager Error:** *error_message*

Explanation:

See BKI5000E.

User response:

See BKI5000E.

BKI5011E **Tivoli Storage Manager Error:** *error_message*

Explanation:

See BKI5000E.

User response:

See BKI5000E.

BKI5012E **Cannot open TSM API message text file. Check if DSMI_DIR is set correctly. Current value of DSMI_DIR is:** *value*

Explanation:

The TSM-API could not be initialized.

User response:

Correct the value of the environment variable DSMI_DIR.

BKI5013E **Value for** *name* **is too long. Current value:** *value*

Explanation:

The value of the environment variable *name* has too many digits.

User response:

Check if the variable is set correctly.

BKI5014E **Tivoli Storage Manager Error:** *error_message*

Explanation:

See BKI5000E.

User response:

See BKI5000E.

BKI5015W **Data description could not be restored, because it was backed up with a newer version (objInf=support information)**

Explanation:

The TSM server hosts backups (data description) which were made with a new version of backint or backom, which ignores this data in further processing.

User response:

Upgrade the product.

BKI5016I **Time:** *current_time* **New TSM session created: MGMNT-CLASS:** *management_class*, **TSM-Server:** *server_name*, **type:** *session_type*.

Explanation:

A new session to TSM server *server_name* has been established at *current_time*. Data will be stored in management class *management_class*.

User response:

None.

BKI5017E **Internal Tivoli Storage Manager Error: Transaction succeeded although it was expected to fail.**

Explanation:

An internal Tivoli Storage Manager error occurred.

User response:

Retry the action. If the error occurs again contact IBM Support.

BKI5018E **The requested buffer has a size (***current_size* **bytes) that is smaller than requested** *requested_size*.

Explanation:

The request for a new buffer was successful. The buffer, however, does not have the requested size.

User response:

Check if the system is running low on memory and retry the action. If the error occurs again contact IBM Support.

BKI5019E **Error during delete of object <filename>:<object>**

Explanation:

A named file could not be deleted from a TSM server.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI5020E **Error while deleting objects :<objects>**

Explanation:

One or more named objects could not be deleted from a TSM server.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI5021W **No data was deleted on the TSM Server because the environment variable ″XINT_FUNCTION_DELETE″ is set to ″DISABLE″.**

Explanation:

The delete function was disabled temporarily.

User response:

If the delete function has to be re-activated, unset the environment variable XINT_FUNCTION_DELETE and try again.

BKI5022W **Error during version delete. Not all backups that have expired could be removed.**

Explanation:

The database backup finished successfully. Nevertheless, the deletion of expired backup sets failed.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6201I **Checking status of database.**

Explanation:

The actual status of the database will be checked to ensure a valid state for the subsequent operation.

User response:

None.

BKI6202E **The log mode for this database is NOARCHIVELOG.**

Explanation:

The log mode for this database is NOARCHIVELOG.

User response:

Change the log mode for this database to ARCHIVELOG.

BKI6203E **The Oracle database is currently in read-only mode.**

Explanation:

The Oracle database is currently designated as read-only. Processing stops.

User response:

Remove the read-only mode of the Oracle database and try again.

BKI6204E The Backup type is online but the mount mode is either nomount or startup restricted.

Explanation:

The Backup type is online but the mount mode is either nomount or startup restricted.

User response:

Change the mount mode to startup mount.

BKI6205I Changing Oracle mode to: <mode>.

Explanation:

The operational mode of the Oracle database is changed to the named mode.

User response:

None.

BKI6206E No table space was found for the Oracle database.

Explanation:

No table space was found for the Oracle database.

User response:

Make sure the correct database system identifier (SID) is specified.

BKI6207E Oracle database data files were not found.

Explanation:

Oracle database data files were not found.

User response:

Make sure the correct database system identifier (SID) is specified.

BKI6208E Oracle database control files were not found.

Explanation:

Oracle database control files were not found.

User response:

Make sure the correct database system identifier (SID) is specified.

BKI6209E The database failed to shut down during the FlashCopy operation.

Explanation:

The database attempted to shutdown because the backup type parameter is set to offline. The database failed to shutdown.

User response:

Manually shutdown the database you are trying to back up, then run the operation again.

BKI6210E Failed to open the output file: <filename>

Explanation:

The named output file could not be opened.

User response:

Either the file doesn’t exist or the permissions are not sufficient for the requested operation. Check that the directory exists where an attempt is being made to access the output file and that sufficient permissions are granted. Try again.

BKI6211E Failed to copy the database controlfile. Please check log file ’<filename>’.

Explanation:

The Oracle database control file doesn’t exist.

User response:

Make corrective actions regarding the information to be found in the named log file and try again.

BKI6212I Suspend database.

Explanation:

The Oracle database to be flashed is going to be supended.

User response:

None.

BKI6213E An error occurred while attempting an ’alter system suspend’ action. More details: <errormsg>

Explanation:

An error occurred while attempting an ’alter system suspend’ action. Details can be found in the named message.

User response:

Make sure the Oracle database to be backed up is running, then try to suspend the system with a command line invocation. If the system suspends successfully, run the operation again.

BKI6214I Resume database.

Explanation:

The Oracle database to be flashed is going to be resumed.

User response:

None.

BKI6215E An error occurred while attempting an ’alter system resume’ action. More details: <errormsg>

Explanation:

An error occurred while attempting an ’alter system resume’ action. Details can be found in the named message.

User response:

Make sure the Oracle database to be backed up is running, then try to resume the system with a command line invocation. If the system resumes successfully, run the operation again.

BKI6216E Failed to get Oracle version information.

Explanation:

Failed to get Oracle version information using sqlplus.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6217I Database switched to next logfile.

Explanation:

The database switched to the next logfile.

User response:

None.

BKI6218E Backup ID to delete not specified.

Explanation:

To delete a backup a valid backup id has to be specified.

User response:

Specifiy a valid backup id and try again.

BKI6219I Backup to TSM: <filename>

Explanation:

Backing up the named file to TSM.

User response:

None.

BKI6220I Using Oracle profile section : <section>

Explanation:

The named Oracle profile section is used for the started operation.

User response:

None.

BKI6221I Database profile: <filename>

Explanation:

Using the named database profile.

User response:

None.

BKI6222E Database profile ’<filename>’ not found.

Explanation:

The named database profile was not found.

User response:

Check if the named profile exists and try again.

BKI6223I Detected control file: <filename>

Explanation:

The named Oracle control file was found.

User response:

None.

BKI6224I Create control file copy: <filename>

Explanation:

A named Oracle control file copy will be created.

User response:

None.

BKI6225I Create database parameter file ’<filename>’ from SPfile.

Explanation:

A named Oracle database parameter file will be created.

User response:

None.

BKI6226E Default directory for database parameter file ’<filename>’ not found.

Explanation:

The name Oracle parameter file could not be found within the default directory.

User response:

Ensure a valid Oracle parameter file exists in the default directory and try again.

BKI6227I Parameter ’database_control_file_restore’ is set to yes in the profile. You will need to do the incomplete recovery after the restore.

Explanation:

The Oracle database control file is requested for restore.

User response:

None.

BKI6228E The database seems to be running. Restore not possible.

Explanation:

A running Oracle database was detected and therefore a restore is not possible.

User response:

Check if the started restore operation is valid. If yes, stop the running database and try again.

BKI6229I Restoring control file <controlfile>

Explanation:

The named control file will be restored.

User response:

None.

BKI6230I Set table space files in backup mode.

Explanation:

The table space files of the participating table spaces will be set in backup mode.

User response:

None.

BKI6231I End backup mode for table space files.

Explanation:

The backup mode for table space files of the participating table spaces will be reset.

User response:

None.

BKI6232I Looking for the latest backup.

Explanation:

An attempt is being made to pick the most current valid backup image for the requested operation.

User response:

None.

BKI6233I Restoring backup with ID <id>.

Explanation:

The backup with the named id will be restored.

User response:

None.

BKI6234E No backup found which could be restored.

Explanation:

There was no snapshot backup found which can be restored.

User response:

Verify your environment. If one or multiple valid snapshot backup exist and the restore still fails, contact your IBM support personnel.

BKI6235I Deleting backup with ID <id>.

Explanation:

The named snapshot backup is going to be deleted.

User response:

None.

BKI6236E Failed to delete backup with ID <id>. Reason: <reason>

Explanation:

The snapshot backup with the named id could not be deleted.

User response:

Check the logs and the named output for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6237E Backup failed. Please check RMAN log.

Explanation:

The offloaded backup to TSM using RMAN failed.

User response:

Make corrective actions regarding the information to be found in the named log file and try again.

BKI6238E Failed to switch logfiles. This is the output of the failed command:<output>

Explanation:

The command failed.

User response:

Check the logs and the named output for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6239E Failed to detect read mode. This is the output of the failed command:<output>

Explanation:

The command failed.

User response:

Check the logs and the named output for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6240E Failed to create a pfile from spfile. This is the output of the failed command:<output>

Explanation:

The command failed.

User response:

Check the logs and the named output for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6241E The tablespace file ’<filename>’ is a link and not a real file.

Explanation:

The named tablespace file has to be a real file. Instead, a link was detected.

User response:

Verify your environment. If the problem cannot be resolved contact your IBM support personnel.

BKI6242E Raw devices are not supported. (’<devicename>’)

Explanation:

Raw devices are currently not supported.

User response:

For further details on this issue, contact your IBM support personnel.

BKI6243E Failed to excute sql cmd ’<command>’. This is the output of the failed command:<output>

Explanation:

The named sql command failed.

User response:

Check the logs and the named output for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6250E Error during initialization: <description>

Explanation:

An error resulting in the named description was detected during the initialization phase of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6251E Error during start of backup: <description>

Explanation:

An error resulting in the named description was detected during the start of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6252E Error during partitioning: <description>

Explanation:

An error resulting in the named description was detected during the partitioning phase of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6253E Error during preparation of snapshot: <description>

Explanation:

An error resulting in the named description was detected during the preparation phase of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6254E **Error during creation of snapshot: <description>**

Explanation:

An error resulting in the named description was detected during the creation of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6255E **Error during verification of snapshot: <description>**

Explanation:

An error resulting in the named description was detected during the verification phase of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6256E **Error during write of meta-information: <description>**

Explanation:

An error resulting in the named description was detected during write of meta-information assigned to a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6257E **Error during retrieval of meta data: <description>**

Explanation:

An error resulting in the named description was detected during retrieval of meta data assigned to a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6258E **Error during query-initialization: <description>**

Explanation:

An error resulting in the named description was detected during the snapshot query-initialization phase.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6259E **Error during retrieval of query information: <description>**

Explanation:

An error resulting in the named description was detected during retrieval of query information of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6260E **Error during end of query: <description>**

Explanation:

An error resulting in the named description was detected during the end of query for snapshot phase.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6261E **Error during start of restore: <description>**

Explanation:

An error resulting in the named description was detected during the start of the snapshot restore phase.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6262E **Error during restore: <description>**

Explanation:

An error resulting in the named description was detected during the restore of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6263E **Error during end of restore: <description>**

Explanation:

An error resulting in the named description was detected during finishing of a snapshot restore operation.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6264E Error during start of delete: <description>

Explanation:

An error resulting in the named description was detected during the start of the snapshot delete phase.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6265E Error during end of delete: <description>

Explanation:

An error resulting in the named description was detected during finishing of a snapshot delete operation.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6266E Restoring Oracle control files failed. Oracle control files are on raw volumes in the production server and those are supposed to be created manually on the backup server. It failed because of either control files are not created on the backup server or created incorrectly. Please check log file *filename*.n

Explanation:

On the production server the Oracle control files reside on raw volumes. On the backup server they need to be restored in order to perform the backup to TSM. This process did fail.

User response:

Examine the content of the *filename*. It contains the output from the Oracle RMAN. A possible reason could be that the raw devices for the control files have not been created on the backup server.

BKI6267E Restoring Oracle control files failed. Please check log file *filename*.

Explanation:

On the backup server the Oracle control files need to be restored in order to perform the backup to TSM. This process did fail.

User response:

Examine the content of the *filename*. It contains the output from the Oracle RMAN.

BKI6501I Initializing ’<function>’ request.

Explanation:

The offload agent will be initialized for a new function request.

User response:

None.

BKI6502I Executing ’<function>’ request.

Explanation:

The offload agent is executing a function request.

User response:

None.

BKI6503I Terminating ’<function>’ request.

Explanation:

The offload agent is terminating a function request. This also includes a cleanup of required resources.

User response:

None.

BKI6504E The ’<function>’ request failed.

Explanation:

A tsm4acs function, such as mount or unmount, failed unexpectedly.

User response:

Check the tsm4acs log as well as the appropriate device agent log and management agent log for further details.

BKI6505E Forced ’<function>’ requires the instance, database and snapshot timestamp filter arguments.

Explanation:

If a function is started with the option ’-F’ (forced) the filter arguments for the instance, database and snapshot timestamp also have to be specified to ensure the workflow will be applied only to one specific snapshot backup.

User response:

Specify the instance (-i), database (-d) and snapshot timestamp (-T) filter arguments as well.

BKI6506I Backup <backup id> was created with option TSM_ONLY. It is marked for deletion after the first TSM backup attempt.

Explanation:

The backup corresponding to <backup id> has been deleted. This is because the backup was made with TSM_BACKUP option TSM_ONLY and the TSM backup associated with this snapshot image has recently completed (successfully or unsuccessfully).

User response:

None.

BKI6507E Function ’<function>’ is not supported.

Explanation:

The function request is not supported by the offload agent.

User response:

Check the specified function.

BKI6508I Initializing partition(s) ’<partition(s)>’ of database ’<database name>’ as <type>.

Explanation:

The participating database partitions will be initialized on the target system. Valid initialization types are snapshot, standby and mirror.

User response:

None.

BKI6509E Failed to initialize partition(s) ’<partition(s)>’ of database ’<database name>’.

Explanation:

The offload agent was not able to initialize one or more database partitions.

User response:

Check the offload agent log as well as the DB2 diagnostic log (db2diag.log) for further details.

BKI6510I Partition(s) ’<partition(s)>’ of database ’<database name>’ initialized successfully.

Explanation:

The participating database partitions were initialized successfully.

User response:

None.

BKI6511E The snapshot backup timestamp filter is not allowed in combination with tape backups.

Explanation:

The data to be off-loaded are typically under control of a versioning mechanism of either the backup mover or Tivoli Storage Manager. If multiple snapshots are in the queue to be off-loaded and the snapshot timestamp filter argument (-T) is incorrect, there is a potential risk of bypassing the established version control mechanism and losing tape backup images.

User response:

Do not specify the snapshot backup timestamp filter (-T) in combination with the function ’tape_backup’.

BKI6512I The ’<function>’ request for database ’<database name>’ with partitions (<partition(s)>) processed successfully.

Explanation:

The selected function for the participating partitions of a database was processed successfully.

User response:

None.

BKI6513I The resources of database ’<database name>’ with partitions (<partition(s)>) are already mounted.

Explanation:

All required file systems are already mounted on the target system.

User response:

None.

BKI6514E The specified filter did not result in a match in the snapshot repository.

Explanation:

The repository does not contain a snapshot backup that can be associated with the given filter arguments.

User response:

Check all specified filter arguments and try again.

BKI6515E A snapshot backup currently offloaded to tape is no longer mounted.

Explanation:

: A tsm4acs tape_backup workflow consists of the steps: mount, tape backup, unmount. When entering the unmount-phase, tsm4acs could not find the snapshot backup that was just backed up to tape. In principle, the tape backup might have finished successfully but some kind of a failure was detected that prevents the tape_backup cleanup phase from completing.

User response:

Check the tsm4acs log as well as the appropriate device agent log for further details.

BKI6516E Another '<function>' request for a snapshot backup is already running.

Explanation:

tsm4acs has detected that another request, such as mount or tape_backup, for a snapshot backup is running.

User response:

A new tsm4acs request can only be started if the old request has finished.

BKI6517I A snapshot backup exists which is already mounted.

Explanation:

The tsm4acs mount-request will not be executed due to an already mounted snapshot backup on the offload system.

User response:

None.

BKI6518I No snapshot backup exists which is currently mounted.

Explanation:

The tsm4acs unmount-request will not be executed because there is currently no snapshot backup mounted on the offload system.

User response:

None.

BKI6519I No snapshot backup is currently pending to be offloaded to tape.

Explanation:

The tsm4acs tape_backup request will not be executed because there is no snapshot backup in the TAPE_BACKUP_PENDING state.

User response:

None.

BKI6520I Starting database instance '<instance name>'.

Explanation:

The database instance on the target system will be started.

User response:

None.

BKI6521I Database instance '<instance name>' was started successfully.

Explanation:

The database instance on the target system was started.

User response:

None.

BKI6522W Database instance '<instance name>' already started.

Explanation:

The database instance on the target system is already running.

User response:

The offload agent workflow should not be affected. In general, no action is required.

BKI6523E Database instance '<instance name>' could not be started.

Explanation:

The database instance on the target system could not be started.

User response:

Check the DB2 diagnostic log (db2diag.log) for further details.

BKI6524I Stopping database instance '<instance name>'.

Explanation:

The database instance on the target system will be stopped.

User response:

None.

BKI6525I Database instance '<instance name>' was stopped successfully.

Explanation:

The database instance on the target system was stopped.

User response:

None.

BKI6526W Database instance ’<instance name>’ already stopped.

Explanation:

The database instance on the target system was already stopped.

User response:

Check the DB2 diagnostic log (db2diag.log) for indication of whether an unexpected failure was the cause. Also check the tsm4acs log for indications that the workflow, which includes shutdown of the database instance on the target system, reported unexpected failures.

BKI6527E Database instance ’<instance name>’ could not be stopped.

Explanation:

The database instance on the target system could not be stopped.

User response:

Check the DB2 diagnostic log (db2diag.log) for further details.

BKI6528E The file containing the list of partitions and hosts to be off-loaded could not be created.

Explanation:

The ’rah’ host file is used by DB2 to determine the database partitions that must be processed in a DPF environment. By default, this file is ’db2nodes.cfg’. tsm4acs uses a temporary ’rah’ host file to be able to handle only a subset of partitions.

User response:

The temporary ’rah’ host file used by tsm4acs will be created under ’$HOME/sqllib’, where $HOME is the home directory of the DB2 instance owner. Ensure that the appropriate permissions are set and enough free space is available.

BKI6530E The default database path could not be determined.

Explanation:

The value of the default database path (DFTDBPATH) stored in the database manager configuration could not be retrieved.

User response:

Check the DB2 diagnostic log (db2diag.log) for details. Further, verify the database manager configuration to be issued by the DB2 instance owner as follows: `db2 get dbm cfg | grep DFTDBPATH`. Also for a more detailed analysis, enable the trace facility for the offload agent and re-execute the function.

BKI6531I Cataloging database ’<database name>’ on path ’<path>’.

Explanation:

The database on the target system will be cataloged.

User response:

None.

BKI6532I Database ’<database name>’ on path ’<path>’ cataloged successfully.

Explanation:

The database on the target system was cataloged successfully.

User response:

None.

BKI6533E Failed to catalog database ’<database name>’ on path ’<path>’.

Explanation:

The database on the target system could not be cataloged.

User response:

Check the DB2 diagnostic log (db2diag.log) for further details. Additionally, for a more detailed analysis enable the trace facility of the offload agent and re-execute the function.

BKI6537I Database ’<database name>’ on path ’<path>’ already cataloged.

Explanation:

The database on the target system was already cataloged.

User response:

None.

BKI6539W The retry threshold for the snapshot backup was exceeded.

Explanation:

If tsm4acs is running in the daemon mode (-D), only one attempt will be made to offload a tape from a snapshot backup. This restriction was imposed to prevent an excessive number of offload retries for a snapshot backup.

User response:

A snapshot backup for which the retry threshold was exceeded can only be offloaded to tape using the manual mode of tsm4acs (-f tape_backup).

BKI6540I **<Start time>: Starting backup of database ′<database name>′, partition(s) ′<partition(s)>′ with the following options: METHOD <offload backup method> SESSIONS <number of sessions> OPTIONS <options> BUFFERS <number of buffers> BUFFERSIZE <buffer size> PARALLELISM <degree of DB2 parallelism>**

Explanation:

The off-loaded tape backup was started using the ′db2 backup database′ command. The set of listed backup parameters gives a brief summary about the options and values that were used for the backup.

User response:

None.

BKI6541I **End_time Instance Database Partition Snapshot_ID Tape_backup_ID**

Explanation:

The backup is finished. A backup result table for all participating partitions of the database will be generated.

User response:

None.

BKI6542I **<end time><instance name><database name><partition><snapshot id><tape backup id>**

Explanation:

One entry of the backup result table reflects one partition of the database. The backup for a database partition succeeded if a valid tape backup ID (DB2 tape backup timestamp) was inserted. If the tape backup for a partition failed, the tape backup ID is set to ′-′.

User response:

None.

BKI6544I **Snapshot backup suspend time: <suspend time>**

Explanation:

The snapshot backup suspend time specifies the minimum recovery time for all participating partitions.

User response:

None.

BKI6545I **Write control file <ctrlfile>**

Explanation:

The offload agent is writing the Oracle control file to a local file system.

User response:

None.

BKI6546I **Write database parameter file <paramfile>**

Explanation:

The offload agent is writing the database parameter file to a local file system.

User response:

None.

BKI6547I **Do not overwrite database parameter file.**

Explanation:

The offload agent will not overwrite the database parameter file.

User response:

None.

BKI6548I **Start backup of database instance ′<instance>′.**

Explanation:

The offloaded tape backup of the named database instance was started.

User response:

None.

BKI6549I **Finished backup of database instance ′<instance>′ successfully.**

Explanation:

The offloaded tape backup of the named database instance finshed successfully.

User response:

None.

BKI6555I **Selected snapshot backup with ID ′<id>′.**

Explanation:

The snapshot backup with the named id was selected to work with. The format of a snapshot id in that context is: <instance>,<database>,<timestamp>.

User response:

None.

BKI6556E Failed to retrieve metadata.

Explanation:

The metadata assigned to a snapshot backup could not be retrieved.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6557I The ’<function>’ request for database ’<dbname>’ processed successfully.

Explanation:

The offload agent has completed the named function successfully.

User response:

None.

BKI6558I The resources of database ’<dbname>’ are already mounted.

Explanation:

The offload agent has detected that all required resources of the named database are already mounted.

User response:

None.

BKI6560E Backint could not be found at ’<directory>’.

Explanation:

The offload agent was unable to find the backint executable file needed for offloading the data to TSM.

User response:

The offload agent expects the backint executable at the default TSM for ERP installation location. Ensure that backint can be found accordingly and try again.

BKI6600E Unexpected error during ’<function>’.

Explanation:

The offload agent has terminated unexpectedly due to an internal error while executing either a mount or an unmount request.

User response:

Check the logs of the involved components (management agent, offload agent, device agent) for further details and descriptions regarding the failure.

BKI6901I Response to Init request.

Explanation:

The device agent is responding to an initialization request.

User response:

None.

BKI6902I Response to Partition request.

Explanation:

The device agent is responding to a partitioning request.

User response:

None.

BKI6903I Response to Prepare Flash request.

Explanation:

The device agent is responding to a prepare snapshot request.

User response:

None.

BKI6904I Response to Restore request.

Explanation:

The device agent is responding to a snapshot restore request.

User response:

None.

BKI6905I Response to Flash request.

Explanation:

The device agent is responding to a snapshot backup request.

User response:

None.

BKI6906I Response to Verify request.

Explanation:

The device agent is responding to a verify request.

User response:

None.

BKI6907I Response to Complete Restore request.

Explanation:

The device agent is responding to a complete restore request.

User response:

None.

BKI6908I Response to Expiration request.

Explanation:

The device agent is responding to a snapshot backup expiration request.

User response:

None.

BKI6909I Response to Monitor request.

Explanation:

The device agent is responding to a background monitor request.

User response:

None.

BKI6910E Could not set user ID to <userid>. Error <error> - <errormsg>.

Explanation:

The user id of the device agent process could not be switched internally to the named user id.

User response:

Check the permissions of the binary and try again.

BKI6911E The effective user ID <userideff> of the process could not be set to the user <userid>. Error <error> - <error_msg>. Check that the device agent executable has the s-bit set.

Explanation:

Due to insufficient permissions of the device agent executable, the user id of the device agent process could not be switched internally to the named user id.

User response:

Check that the device agent binary has the s-bit set and try again.

BKI6912E Background operation shutting down in order to give precedence to a concurrent operation.

Explanation:

The background monitoring operation was canceled due to an operation of a higher precedence.

User response:

Check if the directory exists and further, if the permissions of the directory are set appropriately. Try again.

BKI6913E Wrong parameter provided with option ’-c’.

Explanation:

The device agent specific command option ’-c’ consists of the two sub-components server and port, whereby the port is optional. If a server and port is specified, these values have to be seperated by a ’:’.

User response:

Use the command option ’-c’ with the argument <server>[:<port>] and try again.

BKI6914E Invalid option ’-K’ specified.

Explanation:

The device agent specific command option ’-K’ is not allowed for explicit calls of a device agent executable. That parameter is reserved only for internal workflows, whereby a device agent is called by another binary.

User response:

Remove the command option ’-K’ from the caller string and try again.

BKI6915E Could not change directory to <directory>.

Explanation:

The application was unable to change to the named directory.

User response:

Check if the directory exists and further, if the permissions of the directory are set appropriately. Try again.

BKI6917E Failed to find volume group for file: <filename>

Explanation:

The volume group for the named file could not be found.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6918E Error when reading the correlation list or during the FlashCopy of the volume pairs.

Explanation:

An internal error occurred during the FlashCopy of volume pairs.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6919E Failed to cancel the copy relationship of volume pairs: rc=<rc>.

Explanation:

The device agent was unable to cancel the copy relationship of volume pairs. The withdraw operation failed.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6920E After 'withdraw done' was finished the update of the IDS repository failed: rc=<rc>.

Explanation:

The device agent was unable to update the IDS repository.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6921E Failed to monitor the FlashCopy.

Explanation:

An internal error occurred during monitoring of the background copy.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6922E Failed to allocate memory.

Explanation:

An internal error occurred during memory allocation.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6923I <copytype> control object already initialized.

Explanation:

The named copy type control object is already initialized and will be used for further processing by the device agent.

User response:

None.

BKI6924E Failed to initialize <copytype> control object.

Explanation:

An internal device agent error occurred during the initialization of the named copy type control object.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6925E Function call '<function>' failed.

Explanation:

An error was detected during execution of the named function.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6926I Adding '<filename>' to the Disk Mapper input list.

Explanation:

The device agent added the named file to the disk mapper input list.

User response:

None.

BKI6927E Failed to find N Series volume for file '<filename>'. Error: <error>.

Explanation:

The device agent was uanble to find the volume hosting the named file.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6928E File system not found. Failed to find NFS mount point for file: ′<filename>′.

Explanation:

The device agent was unable to determine the file system hosting the named file.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6929E Not a file system of type NFS. Failed to find N Series volume for file: ′<filename>′.

Explanation:

The file system where the named file is located is not of type NFS.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6930E Volume information missing. Failed to find N Series volume for file: ′<filename>′.

Explanation:

The device agent was unable to detect the volume information for a given file.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6931E Function call ′<function>′ failed. Error: <error>.

Explanation:

An error was detected during execution of the named function.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6932E Function call ′<function>′ failed with rc=<rc>. Error: <error>.

Explanation:

An error was detected during execution of the named function.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6933I Volume ′<volume>′, snap ID = <id>.

Explanation:

The device agent is using the named volume as a snap volume.

User response:

None.

BKI6935I Unmounting ′<mountpoint>′.

Explanation:

The device agent is unmounting the named mount point.

User response:

None.

BKI6936E Failed to unmount ′<mountpoint>′.

Explanation:

The unmount of the named mount point failed.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6937I Mounting ′<mountpoint>′.

Explanation:

The device agent is mounting the named mount point.

User response:

None.

BKI6938E Failed to mount ′<mountpoint>′.

Explanation:

The mount of the named mount point failed.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6939I Prepare for snap restore, volume ’<volume>’, snap ID = <id>.

Explanation:

The device agent is preparing the named volume for snap restoring.

User response:

None.

BKI6940I Prepare flash of group ’<group>’.

Explanation:

The device agent is preparing the named group for flashing.

User response:

None.

BKI6941I <copy services server><copy services user><*><copy services type><copy services time out>**

Explanation:

Prints information about the configured storage device which will be used by the device agent workflow.

User response:

None.

BKI6942E The storage device ’<device>’ is not handled by this device agent.

Explanation:

The device agent cannot be used in combination with the named storage device.

User response:

Check the setup of your system landscape (hardware, software). If the problem cannot be resolved contact your IBM support personnel.

BKI6943I Hardware version installed: <major>.<minor>

Explanation:

The device agent has checked the version of the storage hardware to be used.

User response:

None.

BKI6944I NLS and tracing are already initialized.

Explanation:

The initialization of the NLS and of the trace facility were already done.

User response:

None.

BKI6945I File system ’<filesystem>’ was already unmounted.

Explanation:

The named file system is already unmounted and will be omitted from the unmount process.

User response:

None.

BKI6946E The environment variable ’ODMDIR’ is not specified. Please verify that the DB2 registry parameter DB2ENVLIST contains the value ’ODMDIR’. To set the DB2ENVLIST you need to issue the command: db2set -i <DB2 instance name> DB2ENVLIST=’<current envlist> ODMDIR’

Explanation:

On AIX, the device agent needs the ODM for internal purposes and has to be able for accessing the ODM components located under ’ODMDIR’.

User response:

Check the runtime environment for the environment variable ’ODMDIR’. If not specified, set it to the correct value. On AIX, for example, this would be typically ’/etc/objrepos’. Further, the environment variable has to be registered within the DB2 profile registry variable DB2ENVLIST. Finally, the DB2 instance has to be restarted to activate the environmen adjustments.

BKI6947W File system ’<filesystem>’ is already mounted.

Explanation:

The named file system is already mounted. This means that the target set where the named file system is located will be skipped by the device agent.

User response:

Ensure there is a valid reason why that file system is already mounted. If so, no further action is required. Otherwise, it is recommended to check why this file system was already mounted.

BKI6948E The container <*container_id*> has already been created. Please specify another name.

Explanation:

The container with id <*container_id*> has already been created previously. Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6949E Creation of the container <*container_id*> failed because no preceding group has been found or the preceding group is not valid. Current group is: <*group_id*>. Please specify a valid group at first using the <*command*> command.

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6950W The output file '<filename>' is not valid.

Explanation:

The named output file could not be created or the permissions are insufficient.

User response:

Check for the right permissions and try again. If the problem cannot be resolved contact your IBM support personnel.

BKI6951E Version mismatch error. Please check setup (<version>:<version>).

Explanation:

The version of the device agent on one side and the version of the management agent on the other side don't match. Only binaries of identical version signatures are compatible.

User response:

Ensure the version signature of all participating binaries are identical. This can be checked either based on the logs or by issuing the commands with the command option '-v'.

BKI6952E Error in connection to TSM ACS management agent.

Explanation:

The device agent was unable to connect to the TSM ACS management agent.

User response:

Ensure the ACSD keyword of the global profile section has a valid hostname/port value combination assigned. Try again.

BKI6955E <*container_id*> is not a valid container. Please specify a valid container.

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6956E The usability state <*usablility_state*> is not supported.

Explanation:

Error in communication protocol between the device agent and the storage device adapter. The given usability state <*usablility_state*> is not valid.

User response:

Contact your IBM support personnel.

BKI6962I Response to File System Service request (<function>).

Explanation:

The device agent is responding to a file system service request to service the named function.

User response:

None.

BKI6967E The directory <directory> has nested mount points that are stored on more than one volume group. This is currently not supported.

Explanation:

The application sent a request to recursively backup all data stored beneath <directory>. TSM for ACS cannot fulfill this backup request because the data stored in this directory path resides on file systems that are stored on multiple volume groups. This is currently not supported.

User response:

Migrate the data underneath <directory> to a single file system or migrate the file systems mounted underneath this directory tree to a common volume group. Note that the directory structure could also contain links to files residing in other file systems. In this case you might be able to resolve this problem by simply removing those links.

BKI6968E **<*command_1*> is not a valid keyword, expected <*command_1*>.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6969E **Found non-database files on the file systems to restore. Please provide a negative list or perform restore with option 'no_check' to allow overwriting those files.**

Explanation:

Although the previously mentioned files were not requested to be restored, they would be overwritten, because they reside on a file system that will be entirely overwritten during restore. In order to allow overwriting those files during restore they need to be added to a 'negative list' or the checking to prevent files from being overwritten needs to be disabled.

User response:

Edit the 'CLIENT' section of the profile. You can either set the parameter 'NEGATIVE_LIST' to 'NO_CHECK', to allow TSM for ACS to overwrite any file residing on a file system that will be restored, or you can set the parameter 'NEGATIVE_LIST' to point to a file (the 'negative list') which contains a list of all files and directories that are allowed to be overwritten. Any directory you add to the 'negative list' is processed recursively.

BKI6970I **Snapshot restore successful.**

Explanation:

The snapshot restore of a snapshot backup finished successfully.

User response:

None.

BKI6971E **Adding the key <*key*> to the container <*container*> failed because it already exists. Please use the <*command*> command if you want to update the key.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6972E **Updating the key <*key*> in the container <*container*> failed because it does not exist. Please use the <*command*> command if you want to add the key.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6973E **The group <*group*> has already been created. Please specify another name.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6974E **<*group*> is not a valid group. Please specify a valid group.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6975E **Adding the key <*key*> to the group <*group*> failed because it already exists. Please use the <*command*> command if you want to update the key.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6976E **Updating the key <*key*> to the group <*group*> failed because it does not exist. Please use the <*command*> command if you want to add the key.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6977E The #<*first_command*> <*parameter*> command has to be preceded by a #<*second_command*> command.

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6978E <*command*> is not a valid keyword when updates to containers and groups are expected.

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6279E Script has continued without waiting. Expected output <*command*> from script but was: <*output*>.

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6980W Received #WARNING command with parameters: <*warning*>.

Explanation:

A warning message has been received from the storage device with the parameters: <*warning*>.

User response:

Check the content of the warning.

BKI6981E Received #ERROR command with parameters: <*error*>.

Explanation:

An error message has been received from the storage device with the parameters: <*error*>.

User response:

Check the content of the error message.

BKI6982W The script <*adapter_name*> returned with code 1. The logfile might contain further warnings.

Explanation:

The storage device adapter had a return code of 1.

User response:

Please check the device agent logfile for further warnings.

BKI6983E The following files have not been partitioned: <*file_names*>

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6984E Error during prepare phase. Nothing known about group <*group_name*>. It has not been created in the partition phase.

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI7048I The default port to connect to *server_name* will be used.

Explanation:

A server port for the connection to the named server was not explicitly specified. Therefore, the default port is used.

User response:

Make sure the named server is listening to the default port. In the case of connection failures, specify the server port in the profile.

BKI7049I The default ProLE port will be used.

Explanation:

The port for the internal communication of Data Protection for SAP is set during installation. The message indicates that this port is being used.

User response:

None.

BKI7051E **The environment variable XINT_PROFILE is not set. It must be set and contain the fully qualified path to the *.utl file to be used.**

Explanation:

The way Data Protection for SAP works is specified in a profile. When called, Data Protection for SAP looks for the environment variable XINT_PROFILE which must contain the fully qualified path to the profile.

User response:

Check the environment for XINT_PROFILE of the user who started Data Protection for SAP.

BKI7053E **Service setup failed due to previous error.**

Explanation:

Initialization of the product failed due to previous errors.

User response:

Check the product log file for further detailed messages.

BKI7055E **Service open failed due to previous error in data mover.**

Explanation:

The command could not be started due to previous errors.

User response:

Check the product log file for further detailed messages.

BKI7056E **Service open failed because configured TSM server could not be accessed.**

Explanation:

The command could not be started because the TSM server defined in the profile could not be accessed.

User response:

Check the product log file for further detailed messages.

BKI7057E **Service open failed because all configured sessions are currently in use.**

Explanation:

The command could not be started because all configured sessions in the profile are currently in use.

User response:

With Oracle RMAN the number of channels configured either in SAP profile or the RMAN script must be less or equal to the maximum number of allowed sessions (MAX_SESSIONS). If multiple servers are used see the User’s Guide for further details. Also check the Data Protection for SAP log file for further detailed messages.

BKI7058E **Service open failed because more than one file was found with the same name.**

Explanation:

The command could not be started because two or more files with the same name were found.

User response:

Check the product log file for further detailed messages.

BKI7059E **Service open failed because a file was not found.**

Explanation:

The command could not be started because a file specified was not found.

User response:

Check the product log file for further detailed messages.

BKI7060I *product* **<version>.<release>.<modification> (<build number>) <build date> session: process ID**

Explanation:

This message is to verify the version of the shared library used for backup. On UNIX and Linux systems this message will be written multiple times into the log per backup depending on the RMAN setup. On Windows, it is written just once.

User response:

None, if the right version is used. If the version within the log does not match the installed version, see ’RMAN Problem Resolution’ in the *Data Protection for SAP® Installation and User’s Guide*.

BKI7061I **Continuing to restore from next data copy.**

Explanation:

A saved data copy could not be restored from the primary data source. Due to multiple data copies available, the unit will switch to the next available data copy and continue to restore.

User response:

Although the data could be restored it should be investigated, why one of the data sources were not available.

BKI7301W Data exchange file from Data Protection for Snapshot Devices for SAP®, <*filename*>, does not exist.

Explanation:

The referenced file is expected by Data Protection for SAP® to exist and to contain information from Data Protection for Snapshot Devices for SAP® about the actual snapshot operation.

User response:

The absences of this files indicates a problem during the snapshot operation performed by Data Protection for Snapshot Devices for SAP®. Please check the logs of DP for Snapshot Devices for SAP® to determine the cause of the problem and try again.

BKI7303W Profiles for Data Protection for Snapshot Devices for SAP® are different. backup: *file name* **restore:** *file name*

Explanation:

During backup the profile used by DP for Snapshot Devices can be determined automatically. For restore and inquire operations the profile for DP for Snapshot Devices must be specified in the profile using the parameter FCS_FILE. For restore DP for Snapshot Devices must use the same profile as for backup.

User response:

Correct the entry for the FCS_FILE parameter in the profile (init<SID>.utl).

BKI7304I Performing DISK ONLY backup

Explanation:

The data for this backup is stored on snapshot-type disks only and will not be sent to TSM.

User response:

None

BKI7305E Error during call to Data Protection for Snapshot Devices for SAP® *error message*

Explanation:

DP for Snapshot Devices could not process the requested operation successfully. Processing may not stop at this point. Depending on the type of request (backup to both TSM and snapshot disks or to snapshot disks only, restore of data which is available in both modes) there are possibilities to recover from this error and continue operation.

User response:

Use the information from *error message* and the output of DP for Snapshot Devices to determine the cause of the problem and try again.

BKI7307W Data Protection for Snapshot Devices for SAP® reported an error during a snapshot-type operation. Do you want to continue to backup to TSM?

Explanation:

The backup was requested to be stored on both the TSM server and the snapshot-type disks. The snapshot operation has failed. Backup can continue to save data on the TSM server only.

User response:

Enter ′stop′ if you want to solve the cause of this error and to try again. Enter ′cont′ if you want to save this data on the TSM server only.

BKI7308E DISK ONLY backup has failed.

Explanation:

The current backup tried to store data on snapshot-type disks only and did not finish successfully.

User response:

Check the output from DP for Snapshot Devices prior to this error message to detect the root cause of this error and try again.

BKI7309W Data Protection for Snapshot Devices for SAP® reported an error during a snapshot-type operation. Do you want to continue to restore from TSM?

Explanation:

The data you wanted to be restored is located on the TSM server and on snapshot-type disks. The snapshot operation has failed. The process can continue to restore data from the TSM server.

User response:

Enter ′stop′ if you want to resolve the cause of this error and to try again. Enter ′cont′ if you want to restore from the TSM server.

BKI7310W Data Protection for Snapshot Devices for SAP® reported an error during a snapshot-type operation. CAUTION: Not all file systems are available. Do you want to retry the operation?

Explanation:

In contrast to message BKI7309W not all file systems are mounted. In this case it is not possible to continue the restore from the TSM server.

User response:

Enter 'stop' if you want to terminate this restore process. Enter 'cont' if you want to retry the snapshot process.

BKI7311I Profile used by DP for Snapshot Devices for SAP®:

Explanation:

The message shows the name of the profile used by DP for Snapshot Devices.

User response:

None

BKI7312W Profile for DP for Snapshot Devices for SAP® not specified in profile. For restore this must be specified

Explanation:

For restore and inquire operation in conjunction with DP for Snapshot Devices this parameter is mandatory. Without this parameter a restore using DP for Snapshot Devices is not possible and Data Protection for SAP will continue to inquire/restore from the TSM server only.

User response:

Add the parameter FCS_FILE to the Data Protection for SAP profile

---

BKI7313W Inquire results from DP for Snapshot Devices for SAP® are not available

Explanation:

Data Protection for SAP® was unable to retrieve information from DP for Snapshot Devices about available backups on snapshot-type disks. This message may be issued in consequence of message BKI7305E.

User response:

Check the output from DP for Snapshot Devices to determine the cause of the error and try again.

BKI7314E The data you want to restore is not available on the TSM server.

Explanation:

If a restore from snapshot-type disks can not be finished successfully Data Protection for SAP tries to continue to restore data from the Tivoli Storage Manager server. But if the backup was performed on snapshot disks only, the data can not be found on the TSM server.

User response:

Check the output from DP for Snapshot Devices prior to this error message to detect the root cause of this error and try again.

BKI7315W The copy process of the files you want to restore is not yet finished. If you continue the files will be restored from TSM.

Explanation:

The snapshot process running in the background has not finished moving the files from the source to the target volumes. A snapshot restore of these volumes is currently not possible.

User response:

After that message you will be asked if you want to continue or stop this operation. If you want to wait until the snapshot process has finished choose 'stop' and the restore attempt will terminate. If you choose 'continue' an attempt is made to restore the data from TSM if available.

BKI7316I The following backup types for the BACKUPID *Backup ID* have been found: - TSM - Snapshot

Explanation:

The backup for the backup ID *Backup ID* was stored on the Tivoli Storage Manager as well as on snapshot-type disks. For restore both data sources can be used.

User response:

None.

BKI7318E The DP for Snapshot Devices for SAP® profile *file name* is not valid.

Explanation:

The profile for DP for Snapshot Devices specified in `init<SID>.utl` could not be accessed.

User response:

Check the file name and the permissions for this file and try again.

BKI7319I Start TSM restore

Explanation:

The restore uses data from Tivoli Storage Manager.

User response:

None

BKI7320I Start restore from snapshot.

Explanation:

The restore is using data from snapshot-type disks.

User response:

None

BKI7321E **The DP for Snapshot Devices for SAP® profile *file name* found in parameter FCS_FILE of the DP SAP profile can not be used if you need to restore this backup.**

Explanation:

In the Data Protection for SAP profile the FCS_FILE parameter is set, however the DP for Snapshot Devices profile specified either

- is not a DP for Snapshot Devices profile
- does not point to the same DP for Snapshot Devices configuration file which was used by the preceding DP for Snapshot Devices `splitint` operation.

User response:

You need

- to correct the FCS_FILE parameter thus a valid DP for Snapshot Devices profile is used, for example the file DP for Snapshot Devices had used when running its snapshot function in the preceding brbackup task (see preceding message BKI7303W)
- to ensure that if different DP for Snapshot Devices SAP profiles are used, all use the same control file (the value of the IDS_CONTROL_FILE parameter in the DP for Snapshot Devices profile)

BKI7322E **Request for a partial restore or restore from snapshot with ’brrestore -m all’ is not supported. In case of brrestore attempt rerun with -m full.**

Explanation:

DP for Snapshot Devices can only restore the whole content of a backup and not only a subset of a disk backup as requested. Most likely this is caused by running brrestore with the option ’-m all’.

User response:

Restore complete backups only: run brrestore with the option ’-m full’.

BKI7323W **Request for a partial restore or restore from snapshot with ’brrestore -m all’ is not supported. If you want to restore the backup: - with a snapshot-type restore enter ’stop’ and rerun brrestore with ’-m full’ - from TSM enter ’cont’**

Explanation:

This message has the same reason as message BKI7322E, but in this case the data is also available from the TSM server. So you may continue to restore this data without the snapshot functionality from TSM server.

User response:

Enter ’stop’ if you want to try to restore a different set of files. Enter ’cont’ if you want to restore this data from TSM server.

BKI7324E **Restore of multiple backup IDs in one run from a snapshot is not possible.**

Explanation:

The data requested for this restore belongs to multiple backup IDs

User response:

Make sure the files you want to restore belong to one single backup ID and try again.

BKI7535W **Error executing command *command name*. Reason: errno (*error number*) *explanation*.**

Explanation:

The command *command name* could not be executed successfully.

User response:

Check the explanation *explanation* and the preceding output of the command execution to detect the cause of the error.

BKI7536I **Execute command *command name*.**

Explanation:

The command *command name* is executed by the application. This message is followed by the output of the command executed.

User response:

None

BKI8201E **SIMULATION CANCELED BY PRODUCTION OPERATION!!!**

Explanation:

The current operation was a simulation performed via the Administration Assistant. This simulation was canceled since a production operation (backup or restore) has been started.

User response:

Check your backup schedule and run simulations only when no other operations are scheduled.

BKI8300I ***Function_name* returned with code *return_information*.**

Explanation:

This message indicates that the named API function ended with the specified return information.

User response:

If the return information indicates a problem, look for preceding error messages in the log files. Otherwise, no response is required.

BKI8301E *Product_name*: **Exception caught in function** *function_name*. **Error information: '***error_information***'**

Explanation:

The named product implementing the DB2 Advanced Copy Services API received an error in the named API function. The error information is shown.

User response:

Analyze the error information to find the cause of the problem. Resolve any problems indicated.

BKI8302E *Product_name*: **Exception caught in function** *function_name*. **More information may be available in file** *log_file_name*. **Error information: '** *error_information***''**

Explanation:

The named product implementing the DB2 Advanced Copy Services API received an error in the named API function. The error information is shown.

User response:

Analyze the error information and the appropriate log files to find the cause of the problem. Resolve any problems indicated.

BKI8303E **No <segment_name> section found for the instance '<id>'.**

Explanation:

An error was detected while parsing the named profile segment name section.

User response:

Check the named profile segment name section and make appropriate adjustments.

BKI8304W **The following error occurred while verifying the configuration for section '<section>':**

Explanation:

An error was detected while parsing the named profile section.

User response:

Check the named profile section and make appropriate adjustments.

BKI8305E **Invalid option** *option* **in options string: '***options_string***'.**

Explanation:

An invalid option was found while parsing the options string specified in the 'db2' command.

User response:

Correct the command and try again.

BKI8306E **The keyword** *keyword* **is not allowed multiple times within the profile.**

Explanation:

The keyword indicated was found more than once in the profile. However, this keyword must not be specified multiple times.

User response:

Correct the profile.

BKI8307E **The parameter** *keyword* **must be specified in the profile.**

Explanation:

A required keyword is missing in the profile.

User response:

Correct the profile.

BKI8308E **Single argument required for parameter** *keyword***.**

Explanation:

The keyword indicated requires a single value. However, two or more values are found in the profile.

User response:

Correct the profile.

BKI8309E **Missing argument for parameter** *keyword***.**

Explanation:

In the profile, a value is missing for the named parameter.

User response:

Correct the profile.

BKI8310E **The keyword** *keyword* **is not allowed.**

Explanation:

An invalid keyword was detected in the profile.

User response:

Correct the profile.

BKI8311E For parameter *keyword*, both server and port must be specified.

Explanation:

A value of the named parameter is missing from the profile.

User response:

As the value for the specified parameter, specify both server and port.

BKI8312E Error while parsing parameter *keyword*. In order for '*value1*' to be valid '*value2*' is required to be an existing directory.

Explanation:

Value1 was found to be an invalid value for the parameter named. For this specific parameter, a file name can be specified whose path must already exist in the system.

User response:

Specify the name of a file in an existing path.

BKI8313E *Product_name*: interface problem in function *function_name*: Invalid value of *parameter: value*

Explanation:

The named product detected an interface problem in the named API function. An invalid value was found for *parameter* in one of the API data structures.

User response:

Contact your IBM support personnel.

BKI8314E *Product_name*: interface problem in function *function_name*: The session is already in use by a different operation.

Explanation:

The named product detected an interface problem in the named API function. Either the session handle is used for various operations simultaneously, or the functions are called in an order not supported by the current version of the library.

User response:

Contact your IBM support personnel.

BKI8315E *Function_name*: The following object is not under the control of *product_name*: *path*

Explanation:

The named product implementing the DB2 Advanced Copy Services API detected a problem in the named API function: The path passed by the database is not under the control of the product.

User response:

Make sure the database to be backed up meets the requirements for employing snapshot backups.

BKI8316E *Product_name*: interface problem in function *function_name*: Empty group list passed by DB2.

Explanation:

The named product detected an interface problem in the named API function: The database passed a group list containing no elements.

User response:

Contact your IBM support personnel.

BKI8317W *Product_name*: Verification of configuration requested by user. No backup started.

Explanation:

The user requested a verification of the configuration. The backup flow continued without errors up to the point where the snapshot would actually be done and was then cancelled. The system is ready for a snapshot backup, but no action beyond verification has been taken so far.

User response:

None.

BKI8318E *Product_name*: interface problem in function *function_name*: Not enough space provided to write meta data.

Explanation:

The named product detected an interface problem in the named API function: The buffer provided by the database is too small to contain the requested meta data.

User response:

Contact your IBM support personnel.

BKI8319W Error while deleting old versions. This problem does not affect the new backup. Error information: '*error_information*'

Explanation:

After a successful backup, the system tries to remove older backups of the database according to the value of profile parameter MAX_VERSIONS. However, a problem occurred while trying to remove expired backups. The new backup is not affected by this problem.

User response:

Check the appropriate log files in order to determine the cause of the problem. Resolve any problems indicated. In case the storage device runs out of storage because outdated snapshot backups have not been removed, delete these snapshot backups manually.

BKI8320I **Deleting full backup** *backup_id - backup_key***.**

Explanation:

After a successful backup, the system tries to remove older backups of the database according to the value of profile parameter MAX_VERSIONS. During this process, the full backup listed is removed.

User response:

None.

BKI8321I **Deleting partial backup** *backup_id* **for node:***host:partition_number***.**

Explanation:

After a successful backup, the system tries to remove older backups of the database according to the value of profile parameter MAX_VERSIONS. During this process, the backup listed for the named partition is removed.

User response:

None.

BKI8322E **Interface problem: Current database partition** *number* **not listed in the partition list.**

Explanation:

The partition list passed by the database does not contain the named partition participating in an operation.

User response:

Contact your IBM support personnel.

BKI8323E *Product_name***: Problem occurred while processing** *function_name***. Please check log file** *log_file_name* **for more information. Error information: '***error_information***'**

Explanation:

The named product implementing the DB2 Advanced Copy Services API received an error in the named API function. The error information is shown.

User response:

Analyze the error information and the appropriate log files to find the cause of the problem. Resolve any problems indicated.

BKI8324E *Product_name***: Problem occurred while processing** *function_name***: Device agent returned code** *return_information***.**

Explanation:

The named product implementing the DB2 Advanced Copy Services API received an error from the device agent in the named API function. The device agent's return information is given.

User response:

Check the appropriate log files to find the cause of the problem. Resolve any problems indicated.

BKI8325E **Failed to determine hostname.**

Explanation:

The system was not able to determine the host name of the machine.

User response:

Make sure the system setup allows for querying the hostname via system function gethostname(). Ensure that the requirements for doing snapshot backups are met.

BKI8326E **Failed to create log directory** *path***.**

Explanation:

The log path indicated is not available in the system and could also not be created.

User response:

Check the properties of the path indicated and make sure that its properties and the properties of the parent directory are set accordingly. Make sure all prerequisites for doing snapshot backups are met.

BKI8327E **Invalid value specified for parameter** *keyword***:** *value*

Explanation:

A parameter value is not valid.

User response:

In case the parameter was specified in the profile correct the profile. In case the parameter was specified as a command line option, correct the entry.

BKI8328E *Product_name* **must be licensed to set parameter** *keyword* **to a value of** *value***.**

Explanation:

Selected functions are supported only with a full TSM license.

User response:

If you need the functionality requested, obtain a full TSM license and install the license file. Otherwise, in case the parameter was specified in the profile, correct the profile or, in case the parameter was specified as a command line option, correct the entry.

BKI8330E **Parameter *keyword* requires ’YES’, ’NO’, or number.**

Explanation:

For the named parameter, only numeric values, ’YES’, and ’NO’ are accepted.

User response:

Correct the profile or the call as appropriate.

BKI8331E **The parameter *keyword1* is not allowed if *keyword2* is set to *value*.**

Explanation:

There is a dependency between parameters *keyword1* and *keyword2*. If the latter is set to the value named, *keyword1* must not be specified.

User response:

Correct the profile or the call as appropriate.

BKI8332E **Failed to parse parameter *keyword*. File names in the profile need to be fully qualified.**

Explanation:

As the value of the parameter indicated, a fully qualified file name is expected. However, the specified value is not a fully qualified path.

User response:

Correct the profile or the call as appropriate.

BKI8333E **In order to enable the parameter *keyword1* you need to set *keyword2* to *value*.**

Explanation:

There is a dependency between parameters *keyword1* and *keyword2*. If *keyword1* is specified, *keyword2* must be given the specific value indicated in the message.

User response:

Correct the profile or the call as appropriate.

BKI8334E **Profile section *section_name* is required for function *operation*.**

Explanation:

The specified profile section is required in order to perform the requested operation. However, it is not included in the profile.

User response:

Correct the profile.

BKI8335E **Profile section *section_name* refers to a value for *keyword* that differs from the one used at backup time. Expected value: *value*.**

Explanation:

The profile parameter named must not change its value between backup and restore. However, in the named profile section, the parameter has a value different from the value it had at backup time. This value is given in the message.

User response:

Correct the profile by setting the indicated parameter to the value indicated in the message.

BKI8336E **Invalid value specified for option *keyword:value***

Explanation:

An option value is not valid.

User response:

Correct the call.

BKI8337E **Error while parsing profile: Missing section name.**

Explanation:

The profile is organized into named sections. However, a section name was not found.

User response:

Check that the profile name is specified correctly or that the default profile is a valid profile. Refer to your user documentation for the syntax of the profile or use the profile wizard to create a new profile.

BKI8338E **Error while parsing profile: Section *section_name* is not allowed to be nested.**

Explanation:

In the profile, the named section starts before the previous section ends. However, the section in question cannot be nested.

User response:

Correct the profile.

BKI8339E Error while parsing profile: Profile section *section_name* **is not valid.**

Explanation:

An invalid section name was found in the profile.

User response:

Correct the profile.

BKI8340E Error while parsing profile: Profile section *section_name* **must not be specified more than once.**

Explanation:

In the profile, only a single section with the name indicated can be specified. However, during parsing, a second occurrence was detected.

User response:

Correct the profile.

BKI8341E Error while parsing profile: Profile section *section_name* **missing.**

Explanation:

The required profile section indicated was not found in the profile.

User response:

Correct the profile.

BKI8343W The parameter *keyword1* **of** *keyword2 value2* **has changed its value from** *value1* **to** *value3***.**

Explanation:

The profile parameter named must not change its value between backup and restore. However, in the named profile section, the parameter has a new value *value3* different from the value *value1* it had at backup time. Both values are given in the message.

User response:

Check the log file for problems that may result from the change of parameter values. If so, you may want to change the profile, restoring parameter *keyword1* to the value it had when creating the backup in order to perform a specific operation.

BKI8344E Path *path* **is listed more than once for partitioning.**

Explanation:

This is a DB2 - TSM interface problem.

User response:

Contact your IBM support personnel.

BKI8345E Error while parsing parameter *keyword***. '***path***' is required to be** *type_information***.**

Explanation:

A path of the type indicated in the message is expected as a value of the named parameter. However, the specified path was not found to be of the correct type.

User response:

Correct the profile or the call as appropriate.

BKI8349I Deleting incomplete backup *backup_id-backup_key* **.**

Explanation:

After a successful backup, the system tries to remove older backups of the database according to the value of profile parameter MAX_VERSIONS. During this process, the incomplete backup listed is removed. A backup becomes incomplete when parts of its data expire. This can happen when a backup that is marked 'destructively restorable' is restored.

User response:

None.

BKI8351E Parameter <parameter> requires 'AUTO' or a decimal value.

Explanation:

The value specified for the named parameter does not comply with the defined range of values.

User response:

Check the named profile keyword and make appropriate adjustments.

BKI8352E Parameter <parameter> requires a decimal value.

Explanation:

The value specified for the named parameter does not comply with the defined range of values.

User response:

Check the named profile keyword and make appropriate adjustments.

BKI8353E Parameter <parameter> requires a value greater than '0'.

Explanation:

The value specified for the named parameter does not comply with the defined range of values.

User response:

Check the named profile keyword and make appropriate adjustments.

BKI8354E Parameter <parameter> requires 'NO' or 'YES'.

Explanation:

The value specified for the named parameter does not comply with the defined range of values.

User response:

Check the named profile keyword and make appropriate adjustments.

BKI8355E Parameter <parameter> requires 'ALL' or a comma separated list of decimal values.

Explanation:

The value specified for the named parameter does not comply with the defined range of values.

User response:

Check the profile keyword DBPARTITIONNUM and make appropriate adjustments.

BKI8356E <product_name>: interface problem in function <function>: Invalid call sequence; the library was not initialized.

Explanation:

An invalid internal call sequence was detected during execution of a dedicated function.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI8357E <product_name>: interface problem in function <function>: Invalid call sequence; the operation was not initialized.

Explanation:

An invalid internal call sequence was detected during execution of a dedicated function.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI8359E The profile parameter <parameter> has the wrong value '<value>'. The expected value is '<value>'.

Explanation:

A profile parameter (or keyword) has a wrong value assigned. An alternate value is expected.

User response:

Check the named TSM for ERP profile keyword and make appropriate adjustments.

BKI8360E Invalid <keyword> specified in the profile.

Explanation:

The value specified for a keyword is either wrong or is missing.

User response:

Check the named TSM for ERP profile keyword and make appropriate adjustments.

BKI8361E Found non-database files on the file systems to back up. Please provide a negative list or clean your file systems.

Explanation:

Although the previously mentioned files were not requested to be part of the backup, they will be copied because they reside on a file system that will be backed up in its entirety. In order to allow backing up those files, they need to be added to a 'negative list' or the checking for such files needs to be disabled. Note that in case of a restore, these files would typically be restored, even if this were not desired.

User response:

Edit the 'CLIENT' section of the profile. You can either set the parameter 'NEGATIVE_LIST' to 'NO_CHECK', to allow TSM for ACS to back up any file stored in a file system that will be backed up, or you can set the parameter 'NEGATIVE_LIST' to point to a file (the 'negative list') that contains a list of all files and directories that are allowed to be processed during backup. Any directory you add to the 'negative list' is processed recursively. Note that there is only one 'negative list' for backup and restore. See BKI6969E for restore.

BKI8362E The trace parameters YES, NO, ON, and OFF cannot be set in conjunction with other trace parameters.

Explanation:

The values YES, NO, ON and OFF in conjunction with the TRACE keyword do not allow further trace flags to be set. They are mutually exclusive.

User response:

Check the TSM for ERP profile keyword TRACE and make appropriate adjustments.

BKI8363E The value <value> is not a valid trace flag.

Explanation:

The value specified for the TRACE keyword is invalid.

User response:

Check the TSM for ERP profile keyword TRACE and make appropriate adjustments.

BKI8364E Error while parsing parameter CONFIG_FILE. Directory ′<directory>′ for node ′<node>′ does not exist.

Explanation:

The base directory containing the TSM for ERP configuration file(s) for any participating DB2 partition does not exist or cannot be accessed.

User response:

Ensure that the directory denoting the base part of the CONFIG_FILE value (left part of the %DB2NODE substring) exists and has the right permissions.

BKI8365E The server stanza for LOG_SERVER ′<server>′ is missing.

Explanation:

A TSM server stanza used by the LOG_SERVER keyword is missing either in the option file (dsm.opt) or in the system options file (dsm.sys).

User response:

Either the value of the LOG_SERVER keyword in the TSM for ERP profile has to be adjusted or an entry must be made or adjusted in the appropriate option file.

BKI8366E The values for parameter <parameter> are expected to be in the range 0 to 6.

Explanation:

The values of the keyword USE_AT have to be in the range of 0 to 6.

User response:

Check the TSM for ERP profile keyword USE_AT and make appropriate adjustments.

BKI8367E You cannot freeze the filesystem without suspending or shutting down the database.

Explanation:

The prerequisites for freezing the filesystem are either to suspend the database or to bring the database offline.

User response:

Ensure either to suspend the database or to bring the database offline and try to freeze the filesystem again.

BKI8368E An invalid argument is specified for keyword <keyword>.

Explanation:

The specified argument could not be converted into an equivalent integer value.

User response:

Check the keyword argument and try again. If the problem cannot be resolved contact your IBM support personnel.

BKI8369E Failed to execute <program>. Reason: <reason>.

Explanation:

The execution of <program> failed.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI8370E The profile option TARGET_DATABASE_SUSPEND= OFFLINE is not allowed for an online database backup.

Explanation:

A snapshot backup of a database that was not suspended can only be done in offline mode.

User response:

Start the BRBACKUP utility with the option ′-t offline -d util_vol′ and try again.

BKI8371E The profile parameter NEGATIVE_LIST is not allowed. Use BR*TOOLS option ″-n″ to specify the negative list.

Explanation:

The negative list value has to be specified in the init<SID>.sap profile via the option ′util_vol_nlist = (<nfile_name1>, <nfile_name2>, ...) | no_check′.

User response:

Adjust the init<SID>.sap profile accordingly and try again.

BKI8372E The profile option TARGET_DATABASE_SUSPEND=YES requires a backup of type volume_online.

Explanation:

A snapshot backup of a database that was suspended can only be done in online mode.

User response:

Start the BRBACKUP utility with the option ′-t online -d util_vol′ and try again.

BKI8373W Operation will execute with force option (-F).

Explanation:

The operation started will be run in forced mode, e.g. delete.

User response:

None.

BKI8374W Operation will terminate with an error because backint was executed with the verify option (-V).

Explanation:

The verify option simulates the requested option and does not create a valid backup or restore. In order to prevent the calling process from regarding the current operation as successful, the verify option will always yield a nonzero return code.

User response:

Do not use the verify option if you want to create a backup or restore.

BKI8375E The value of the environment variable ORACLE_SID is not allowed to have more than <number> digits.

Explanation:

The length of the ORACLE_SID value violates the defined range.

User response:

Check the current value of ORACLE_SID and if necessary, correct it according to the allowed length. Try again.

BKI8376E Verification of snapshot failed. Reason: <reason>

Explanation:

The snapshot backup could not be verified successfully.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI8377E Function <function> does not support multiple backup ids within a single operation.

Explanation:

TSM for ACS was requested to perform a volume <function> operation simultaneously for a set of objects that were backed up with multiple volume backup requests. This is currently not supported.

User response:

Use backups stored on the TSM server to perform redirected restores or adjust the restore command.

BKI8378E Redirected restore of volume backups is not supported yet.

Explanation:

TSM for ACS does not support restores to an alternate data location. The restore always needs to be made to the original data location.

User response:

Use backups stored on the TSM server to perform redirected restores.

BKI8379E Infile contains an invalid value: ′<value>′

Explanation:

Each record of the infile has to start either with the string ′#NULL′ or with the backup Id.

User response:

Ensure each record of the infile satisfies the requirements. If the problem cannot be resolved contact your IBM support personnel.

BKI8380E The profile option TSM_BACKUP=YES requires a snapshot backup of all partitions of the database.

Explanation:

The profile option TSM_BACKUP=YES implies offloading a snapshot backup to TSM. If this option is specified, all database partitions have to be part of the snapshot backup.

User response:

Specify the ′ALL DBPARTITIONNUMS′ clause as part of the DB2 backup command and try again.

BKI8381W The following error occurred while verifying the configuration for server ’<server_name>’ in the profile:

Explanation:

The profile section for server <server_name> is not correct. The actual error is following this message.

User response:

Adjust the profile and correct the error following this message.

BKI8382E The previous error(s) can be prevented by executing restore with negative list set to ’no_check’.

Explanation:

An error occurred while inspecting file systems for files that should be excluded during the backup/restore operation. This error precedes the current message. Note that the file system inspection can be turned off by setting the parameter ’NEGATIVE_LIST’ to ’NO_CHECK’.

User response:

Resolve the root cause for this problem (previous error) or change the value of the parameter ’NEGATIVE_LIST’ to ’NO_CHECK’.

Depending on the application type, this can be accomplished by

- (for DB2 and native Oracle) editing the TSM ACS profile and set the parameter ’NEGATIVE_LIST’ to ’no_check’
- (for SAP® for Oracle) editing the BR*Tools profile *.sap and set the parameter ’util_vol_nlist’ to ’no_check’

Note that changing ’NEGATIVE_LIST’ to ’NO_CHECK’ implies that TSM for ACS would potentially backup all files residing on the requested file systems. This true even if they were not explicitly requested and resided on the requested file systems, and even if they were not explicitly requested during the backup. At restore time all of these objects would typically be restored.

BKI8383E BR*Tools are required to set the environment variable BI_RUN for volume backups.

Explanation:

This is a unique ID from a BR*Tools run (normally it is the name of the BR*Tools log). If this variable is set then BACKINT recognizes that a call from BR*Tools 7.10 or higher was triggered.

User response:

Ensure that BR*Tools 7.10 or later is used and rerun the operation.

BKI8384E Failed to determine the APPLICATION_TYPE of the profile. Please invoke wizard with option -m <application type>.

Explanation:

’acsd -f wizard’ was invoked to modify an existing profile, and the APPLICATION_TYPE could not be identified by inspecting this profile. This is required in order to properly adjust the profile.

User response:

Provide the application type when invoking the wizard with options ’acsd -f wizard -m <application type>’. The preferred method, however, is to call the setup script without options.

BKI8385E In order to create a new profile the wizard needs to be invoked with option -m <application type>.

Explanation:

’acsd -f wizard’ was invoked to create a new profile. In this case it is required to specify the application type with option -m.

User response:

Provide the application type when invoking the wizard by using the options ’acsd -f wizard -m <application type>’. Alternatively, you can use the database-specific version of the setup script (`setup_<database>.sh`) to create a new profile and configure TSM for ACS.

BKI8386E Parameter *parameter name* **requires a decimal value of 0 or greater.**

Explanation:

The value specified for the named parameter does not comply with the defined range of values.

User response:

Check the named profile keyword and make appropriate adjustments.

BKI8387W Found additional files on the file systems to backup: *filename*

Explanation:

Although the previously mentioned files were not requested to be part of the backup, they will be copied because they reside on a file system that will be backed up in its entirety.

User response:

Edit the ’CLIENT’ section of the profile. You can either set the parameter ’NEGATIVE_LIST’ to ’NO_CHECK’, to allow TSM for ACS to back up any file stored in a file system that will be backed up, or you can set the parameter 'NEGATIVE_LIST' to point to a file (the 'negative list') that contains a list of all files and directories that are allowed to be processed during backup. Any directory you add to the 'negative list' is processed recursively. Note that there is only one 'negative list' for backup and restore. See BKI6969E for restore.

BKI8389W **The following volume groups or file systems are currently not accessible:** *volume groups* **or** *file systems*

Explanation:

The listed volume groups or file systems are not accessible. TSM ACS tries to verify that only database files reside in the volume groups or file systems that will be restored. But it was encountered that it was not possible to access the file systems (in the volume groups) to verify the database files because the file systems are not mounted or the volume groups are not imported, or both. This warning message is followed by message BKI9390E which gives more information.

User response:

This is just a warning message. Follow the instructions of the user response of BKI8390E.

BKI8390E **Failed to validate that only database files will be overwritten during restore, because some of the database file systems are currently not accessible. Please import volume groups and/or mount all file systems and restart the restore. If you cannot mount the file systems as a consequence of a disaster or a failing previous restore operation, this error can be prevented by executing restore with negative list set to 'no_check'.**

Explanation:

TSM ACS tries to verify that only database files reside in the volume groups / file systems that will be restored. But it was encountered that it was not possible to access the file systems (in the volume groups) to verify the database files because the file systems are not mounted and/or the volume groups are not imported.

User response:

There are two options to solve this problem:

1. Import all volume groups and mount all file systems that contain database files.
2. If the first option is not possible as a consequence of a disaster or a failing previous restore operation, the negative list check cannot be performed at all and must be switched to 'no_check'. Depending on the application type, this can be accomplished by
   - (for DB2 and native Oracle) editing the TSM ACS profile and set the parameter 'NEGATIVE_LIST' to 'no_check'
   - (for SAP® for Oracle) editing the BR*Tools profile *.sap and set the parameter 'util_vol_nlist' to 'no_check'

Note that changing NEGATIVE_LIST to NO_CHECK implies that TSM for ACS would potentially backup all files residing on the requested file systems. This true even if they were not explicitly requested and resided on the requested file systems, and even if they were not explicitly requested during the backup. At restore time all of these objects would typically be restored.

BKI8511I **The command is:** *command name***.**

Explanation:

This is an information message echoing the command.

User response:

None.

BKI8512I **Return code is:** *return code***.**

Explanation:

This message shows the return code of the Backup Object Manager.

Valid return codes:

0
The requested action was performed successfully.

1
The requested action was performed successfully; however, some warnings were issued.

2 or greater
The requested action could not be performed due to errors. In this case, an error message should be logged, too.

User response:

None if the return code is 0.

If the return code is greater than 0, analyze the error and/or warning messages. Resolve errors before starting the action again.

BKI8513W **'TDP_DIR' is not set. The temporary path will be used.**

Explanation:

The environment variable 'TDP_DIR' is not set and therefore, the log will be written to the system's temporary path instead.

User response:

Set the 'TDP_DIR' environment variable.

BKI8514W ’TDP_DIR’ is not set correctly. The temporary path will be used.

Explanation:

The variable TDP_DIR is set but contains an invalid path. All run logs will be written to the machines temporary directory instead.

User response:

Check and reset the environment variable TDP_DIR.

BKI8520E No command was specified.

Explanation:

`backom` was called without a command line.

User response:

Check the command syntax and correct the call.

BKI8521E Command option *command option* **requires an argument.**

Explanation:

A command option requiring an argument was specified without an argument.

User response:

Check the command syntax and correct the call.

BKI8522E Invalid command *command***.**

Explanation:

backom was called with an invalid command.

User response:

Check the command syntax and correct the call.

BKI8523E Error during *action***.**

Explanation:

An error occurred while performing the named action.

User response:

Look for other error messages in order to analyze the problem.

BKI8524E Table space online restore is not allowed.

Explanation:

Either the database setup or the kind of backup prevents an online table space backup.

User response:

If you need to do a table space restore it must be done offline.

BKI8525E The DB2 instance name can consist of at most 8 characters.

Explanation:

The name given for the DB2 instance does not comply with the DB2 naming conventions.

User response:

Correct the DB2 instance name.

BKI8526E The DB2 database alias can consist of at most 8 characters.

Explanation:

The name given for the DB2 alias does not comply with the DB2 naming conventions.

User response:

Correct the DB2 alias name.

BKI8527E Invalid node. Specify it in the format *node format***.**

Explanation:

The name given for the DB2 node does not comply with the DB2 naming conventions. Node numbers must be specified in the displayed format, for example ’NODE0000’ or ’0000’.

User response:

Correct the DB2 node number.

BKI8528E Invalid timestamp. It must consist of 14 digits with format yyyymmddhhmmss or digits and wildcards * or ?.

Explanation:

Specify digits in the format ’yyyymmddhhmmss’ or mixed with wildcards ’*’ or ’?’.

where:

- yyyy is the year, specified as four digits,
- mm is the month, specified as two digits, with leading zero for the months January to September,
- dd is the day of the month, specified as two digits, with leading zero for days 1 to 9,
- hh is the hour of the day, 00 to 23, with leading zero for hours 0 to 9,
- mm is the minutes of the hour, 00 to 59, with leading zero for minutes 0 to 9,
- ss is the second of the minute, 00, to 59, with leading zero for seconds 0 to 9.

Any digits can be replaced by wildcards ’*’ or ’?’, where

- * means any number of any digits,
- *?* means exactly one digit of any value.

User response:

Correct the timestamp.

BKI8529E **Invalid log sequence number. Specify it in the format** *log sequence format***.**

Explanation:

The information on the log sequence number(s) does not comply with the expected format. Accepted log sequence numbers are for example ’123’ or ’S0000123.LOG’.

User response:

Correct the log sequence number(s).

BKI8530E **Profile** *file name* **does not exist or cannot be accessed.**

Explanation:

Either an existing file could not be opened, or a file could not be created.

User response:

Check the attributes of the file and/or its directory. For backup processing, read access is required for the files to be backed up. For restore processing, write access is required for the target location of the files to be restored.

BKI8531E **Directory** *file path* **does not exist or cannot be accessed.**

Explanation:

A file path cannot be accessed.

User response:

Check the attributes of the file and/or its directory. For backup processing, read access is required for the files to be backed up. For restore processing, write access is required for the target location of the files to be restored.

BKI8532E **Invalid log chain number. Specify it in the format** *log chain format***.**

Explanation:

The information on the log chain number(s) does not comply with the expected format. Accepted log chain number(s) are for example ’123’ or ’C0000123’. *file path*

User response:

Correct the log chain number(s).

BKI8533E **A timestamp range is not allowed for the command** *command* **.**

Explanation:

A timestamp range is not allowed for command `restore database`, `restore tablespace`, `restore tablespace online` and `restore DB2 history file`. Only a single timestamp argument can be used.

User response:

Correct the timestamp command option.

BKI8534E **Command option** *command option* **is missing.**

Explanation:

A command was issued without specifying a required command option.

User response:

Check the command syntax and correct the call.

BKI8535E **Invalid output mode. Specify one of the keywords** *keyword list***.**

Explanation:

Only the listed keyword values are allowed with the output mode command option `-m`.

User response:

Correct the output mode command option.

BKI8536E **Wildcard characters are not allowed for command** *command***.**

Explanation:

For the BackOM commands ’restore database’, ’restore tablespace’, ’restore tablespace online’ and ’restore DB2 history file’ it’s not allowed to specify the wildcard characters ’*’ and ’?’ in a timestamp command option.

User response:

Correct the timestamp command option.

BKI8537E **The path** *path* **is not absolute.**

Explanation:

A command line argument requires a fully qualified path which was not given.

User response:

Specify the fully qualified path.

BKI8538E The TDI *file name* cannot be processed.

Explanation:

The TDI file could not be parsed because of errors. There are more specific parser error messages before this message occurs.

User response:

Check for and respond to preceding error messages in the Backup Object Manager log.

BKI8540I Using *component_name* at *host name*:*port number*.

Explanation:

The *component_name* service named is used for the current action.

User response:

None.

BKI8541I Using profile *profile path*.

Explanation:

The profile named is used for the current action.

User response:

None.

BKI8542E Profile *profile path* cannot be read.

Explanation:

The Backup Object Manager tried to use the profile named but the profile was not available or could not be read. The location of the profile is specified via command line as argument to option ′-e′ or in environment variable ′XINT_PROFILE′.

User response:

Make sure that the profile is available at the location specified in option ′-e′ on the command line or in environment variable ′XINT_PROFILE′.

Check the attributes of the profile and the corresponding directory and make sure that the file can be accessed.

BKI8543I Querying TSM for file(s) *file list*.

Explanation:

The Backup Object Manager checks if the files listed are available on the TSM server(s) specified in the corresponding profile.

User response:

None.

BKI8545I No *image type* image(s) found.

Explanation:

A request could not be satisfied because the files to be processed are not available on the TSM server.

User response:

Check if the file(s) were specified correctly in the request.

BKI8546E Environment variable *environment variable* is not set or not set correctly.

Explanation:

A required environment variable is not set at all or has a value that is not allowed.

User response:

Check the documentation for the appropriate values of the environment variable named and set its value accordingly.

BKI8548I Elapsed time: *time value*.

Explanation:

After restore and delete, the time elapsed during the action is displayed.

User response:

None.

BKI8549E Unable to create file *file name*.

Explanation:

During restore, the file to be restored cannot be created in the target location.

User response:

Check if there is sufficient space available for the file to be restored.

Check the attributes of the target directory; write access is required.

If the target file already exists, check that write access is granted

---

BKI8550W Environment variable *environment variable* for output mode has wrong value. Using default.

Explanation:

The default output mode can be overridden by the named environment variable. Accepted values are ″short″, ″normal″, or ″detailed″. The system default is ″short″ for actions on DB2 log files, ″normal″ otherwise.

User response:

Specify an appropriate value for the environment variable named, or remove the environment variable.

BKI8551E Not all data written to ***file path*****.**

Explanation:

Restoring raw or DB2 log file data ended before all data retrieved from TSM could be written to the file named.

The file is incomplete.

User response:

Make sure there is sufficient space for the data to be restored.

BKI8552E File ***file path*** **could not be closed.**

Explanation:

After restoring raw or DB2 log file data, the target file could not be closed.

User response:

Retry the action.

BKI8555E Variable 'DB2DBDFT' or command option 'alias' is required.

Explanation:

The password command needs the name/alias of the database, for which the Data Protection for SAP configuration file has to be adapted.

User response:

Either set the environment variable DB2DBDFT or provide the command option 'alias' with the password command and try again.

BKI8556E Unable to get hostname.

Explanation:

The machines hostname could not be determined.

User response:

Check the TCP/IP configuration of the machine.

BKI8557E The config file ***file name*** **could not be created.**

Explanation:

Data Protection for SAP tries to create the configuration file named if it is not present at the location specified by the Data Protection for SAP profile keyword CONFIG_FILE. However, the file cannot be created. This may either be caused by an incorrect path specified by keyword CONFIG_FILE, or the user may not have the appropriate permissions for creating the file.

User response:

Make sure the path specified by keyword CONFIG_FILE is correct and the permissions are set appropriately.

BKI8558I Setting TSM password for partition ***partition number*** **on host** ***host name*****.**

Explanation:

The Data Protection for SAP TSM password is set on the host named for the DB2 partition indicated.

User response:

None.

BKI8559W For partition ***partition number*** **switch to host** ***host name*** **and issue the command again.**

Explanation:

When verifying the TSM password, the Data Protection for SAP configuration file is modified.

If the Data Protection for SAP profile keyword CONFIG_FILE points to an NFS mounted (UNIX or Linux) or a shared (Windows) path accessible to all hosts in a DB2 ESE (EEE) environment, for example the instance home, all configuration files of the various partitions can be modified simultaneously. If, in contrast, keyword CONFIG_FILE points to a local path, only the configuration files of the local partitions can be modified. In this case, the password verification needs to be done from each host. The message indicates the partitions whose associated configuration files are not accessible. In order to avoid this administrative overhead, it is recommended to place the Data Protection for SAP configuration files in a file system shared by all hosts hosting a partition of the database.

User response:

Make sure to verify the TSM password(s) for all partitions of the database.

BKI8560E Partition ***partition number*** **not found in the database configuration.**

Explanation:

The DB2 partition specified could not be found in the database configuration.

User response:

Check the configuration of the DB2 ESE(EEE) environment (`db2nodes.cfg`, environment variable DB2NODE) and try again.

BKI8561W Database ’alias’ not listed in the system database directory.

Explanation:

The database ’alias’ does not exist. Because there is a dependency between the alias and the settings for Data Protection for SAP there might be problems during database backup or restore runs. Nevertheless, the Data Protection for SAP configuration file (init<alias>.utl) will be created and adapted.

User response:

Check if the alias specified does match to an entry in the DB2 system database directory. Further, check the argument for the Data Protection for SAP profile keyword CONFIG_FILE and if necessary adapt it appropriately.

BKI8584I Delete command completed successfully.

Explanation:

The object(s) specified with the delete command were successfully deleted from the TSM server.

User response:

None.

BKI8585W Delete command completed successfully, but had warning(s).

Explanation:

The object(s) specified with the delete command were deleted with warning(s) from the TSM server.

User response:

Check the Backup Object Manager log file for further detailed messages and if required, do the requested interventions manually.

BKI8586I Delete command was aborted.

Explanation:

The delete command was aborted by the user. No object(s) were deleted from the TSM server.

User response:

None

BKI8587E Delete command failed due to an error.

Explanation:

The delete command failed during execution. Not all objects were deleted from the TSM server.

User response:

Check the Backup Object Manager log file for further detailed messages and try to resolve the error which led to the delete failure. Retry the action. If the error still exists, contact the IBM Support.

BKI8588E Delete command has not been started or no delete result information is available.

Explanation:

This message indicates that an operation did not complete successfully. Typically, some other error condition was detected before.

User response:

Contact the IBM Support.

BKI8589E Query command failed due to an error.

Explanation:

The query command failed during execution. Not all queried objects can be displayed.

User response:

Check for and respond to preceding error messages in the Backup Object Manager log. In the absence of preceding error messages, contact IBM Support.

BKI8610I Restoring *type* ...

Explanation:

The restore of *type* has started.

User response:

None.

BKI8612I Continuing restore ...

Explanation:

The database restore continues.

User response:

None.

BKI8613E Terminating restore ...

Explanation:

An error occurred, and the database restore terminates.

User response:

Check for and respond to preceding error messages in the Backup Object Manager and the shared library run logs. Additional information may be found in the DB2 diagnostic log (db2diag.log).

BKI8615I Restore command completed successfully.

Explanation:

The object(s) specified with the restore command were successfully restored from the TSM server.

User response:

None.

BKI8616W Restore command completed successfully. Warning(s) encountered.

Explanation:

The object(s) specified with the restore command were restored with warning(s) from the TSM server.

User response:

Check the Backup Object Manager log file for further detailed messages and if required, do the requested interventions manually.

BKI8617I Restore command was aborted.

Explanation:

The restore command was aborted by the user. No object(s) were restored from the TSM server.

User response:

None.

BKI8618E Restore command failed due to an error.

Explanation:

The restore command failed during execution. Not all objects were restored from the TSM server.

User response:

Check the Backup Object Manager log file for further detailed messages and try to resolve the error which led to the restore failure. Retry the action. If the error still exists, contact the IBM Support.

BKI8619E Restore command has not been started or no restore result information is available.

Explanation:

This message indicates that an operation did not complete successfully. Typically, some other error condition was detected before.

User response:

Check for and respond to preceding error messages in the Backup Object Manager log.

BKI8621I Restoring file ***file name*****...**

Explanation:

The system started restoring the file indicated.

User response:

None.

BKI8622I Deleting ***type*** **...**

Explanation:

The deletion of *type* has started.

User response:

None.

BKI8623I Deleting file ***file name*** **...**

Explanation:

The system started deleting the file indicated.

User response:

None.

BKI8626W The TDI ***file name*** **could not be deleted.**

Explanation:

The system tried to remove the TDI image from TSM, but did not succeed.

User response:

Try to remove the image manually using the Backup Object Manager raw delete facility.

BKI8630E The command option ***option*** **must be a number.**

Explanation:

An invalid argument was specified for command option *option*.

User response:

Correct the command syntax.

BKI8631I Backup command completed successfully.

Explanation:

The backup operation completed successfully; the backup image can be used for restoring. In the case of a full database backup, the TDI image was generated and stored to TSM, too.

User response:

None.

BKI8632W Backup command completed successfully. Warning(s) encountered.

Explanation:

The backup operation completed successfully; the backup image can be used for restoring. However, some problems occurred.

User response:

Check the warning messages and take corrective actions if necessary.

BKI8633I Backup command was aborted.

Explanation:

The backup operation was cancelled by user interaction. No backup image was created.

User response:

None.

BKI8634E Backup command failed due to an error.

Explanation:

No backup was made due to previous errors.

User response:

Check for and respond to preceding error messages in the Backup Object Manager log.

BKI8635E The command option *option* **must be a floating point number.**

Explanation:

An invalid argument was specified for command option *option*.

User response:

Correct the command syntax.

BKI8636E The command option *option* **must be one of** *values***.**

Explanation:

An invalid argument was specified for command option *option*.

User response:

Correct the command syntax.

BKI8637I *Type online/offline* **backup of** *alias* **started ...**

Explanation:

A backup operation of database *alias* of type *type* has started.

User response:

None.

BKI8638I *Type online/offline* **backup of table space(s)** *tablespace#1,...,tablespace#n* **of** *alias* **started ...**

Explanation:

A backup operation of table space(s) *tablespace#1 ... tablespace#n* of database *alias* of type *type* was started.

User response:

None.

BKI8639I Including log files in backup image ...

Explanation:

The DB2 log files are stored as part of the backup image.

User response:

None.

BKI8640I Using *number* **buffers with a size of** *size* **...**

Explanation:

For backup or restore operations, the indicated number of buffers of the size displayed are used.

User response:

None.

BKI8641I Using *number* **session(s) ...**

Explanation:

For backup or restore operations, the indicated number of TSM sessions is used.

User response:

None.

BKI8642I Using a degree of parallelism of *number* **...**

Explanation:

For backup or restore operations, the degree of parallelism is displayed.

User response:

None.

BKI8643I Using vendor library at *lib path* **...**

Explanation:

For backup or restore operations, the named vendor library is used.

User response:

None.

BKI8644W Offline backups cannot include log files. The option -L is being ignored.

Explanation:

An offline backup operation was started, requesting the DB2 log files to be included. This is not possible with an offline backup. The backup is done without including DB2 log files.

User response:

Make sure to backup DB2 log files separately.

BKI8651W Your version of DB2 does not support including log files. The option -L is being ignored.

Explanation:

A backup was started, requesting the DB2 log files to be included, but your version of DB2 does not support this feature. For including DB2 log files in the backup image, DB2 V.8.2 or later is required.

User response:

Make sure to backup DB2 log files separately.

BKI8652I Detected DB2 version *version* with *number* bits.

Explanation:

The indicated DB2 version was detected by Backup Object Manager.

User response:

None

BKI8653I Using autonomic buffer size and number of buffers ...

Explanation:

The buffer size and the number of buffers used for backup or restore is automatically determined by DB2.

User response:

None

BKI8654I Using an autonomic buffer size with *number* buffers ...

Explanation:

The buffer size used for backup and restore is automatically determined by DB2. The number of buffers to be used was specified in the call to the Backup Object Manager.

User response:

None.

BKI8655I Using an autonomic number of buffers with a size of *size* ...

Explanation:

The number of buffers to be used for backup and restore are determined by DB2. The buffer size to be used was specified in the call to the Backup Object Manager.

User response:

None.

BKI8656I Using an autonomic degree of parallelism...

Explanation:

The number of DB2 processes (UNIX or Linux) or threads (Windows) used for reading or writing data from/to table space containers during backup and restore is determined by DB2.

User response:

None.

BKI8657W *Number* is not a valid partition number. Assuming partition 0.

Explanation:

The partition number specified in the call to Backup Object Manager does not denote a valid partition of the database. Therefore, the default partition 0 will be used by DB2 and by Backup Object Manager.

User response:

If your database is not partitioned do not specify the partition number for further actions.

BKI8658E *Number* is not a partition number of the database or does not denote a partition on this host.

Explanation:

The partition number specified does not denote a valid database partition or is not the partition located on the system where Backup Object Manager is called. Backup Object Manager can only operate on partitions residing on the same host.

User response:

Either change *number* to a partition number of a local partition, or start Backup Object Manager from the same host where the partition resides.

BKI8659I **Creating table space definition information ...**

Explanation:

The table space definition information (TDI) is being created in memory.

User response:

None.

BKI8660I **Saving table space definition information ...**

Explanation:

The table space definition information (TDI) is being stored on the TSM server.

User response:

None.

BKI8661W **Could not create TDI. The backup cannot be used for redirected restore with BackOM.**

Explanation:

The system could not collect the table space definition information. The backup was made without TDI. As a result, the backup can be used for restoring the system, but it cannot be used for restoring to a different location.

User response:

Ensure that your database is enabled to accept CLI connections.

BKI8662W **Could not save TDI. The backup cannot be used for redirected restore with BackOM.**

Explanation:

The system could not save the TDI on TSM. The backup was made without TDI. As a result, the backup can be used for restoring the system, but it cannot be used for restoring to a different location.

User response:

Check for and respond to preceding error messages in the Backup Object Manager log.

BKI8663W **The TDI contains device containers. The backup cannot be used for redirected restore with BackOM.**

Explanation:

A backup of a database using device containers was requested. The backup was successful, it can be used to restore the system, but it cannot be used for restoring to a different location. Restoring to a different location is not supported with device containers.

User response:

None.

BKI8664E **Connecting to *alias* using CLI failed. The return code was *return code*.**

Explanation:

The system tried to connect to the database named via the CLI. The operation did not succeed and returned the error code indicated.

User response:

Ensure that your database is enabled to accept CLI connections.

BKI8665I **The backup timestamp is: *timestamp*.**

Explanation:

The DB2 backup finished successfully with the timestamp *timestamp*.

User response:

None.

BKI8666I **Redirecting table space *table space* with ID *id*.**

Explanation:

The named table space is restored to the location requested.

User response:

None.

BKI8667W **Table space *tablespace* with ID *id* was not redirected because its container on the source system *SID* is not located in a path starting with *path* .**

Explanation:

The named table space of type SMS was not redirected because the definition of the table space container in the source system does not match the database characteristics that Backup Object Manager expects and that are cited in the message. Therefore, Backup Object Manager tries to restore the table space to a location identical to the location in the original system.

User response:

Make sure that the table space mentioned can be restored to the original location. This requires that the user initiating the redirected restore has the appropriate permissions for placing the table space container in this location and that the table space can be restored without overwriting other data.

In order to avoid this situation in the future, the administrator of the source system may want to recreate the table space according to the database characteristics Backup Object Manager expects.

BKI8668I TDI created successfully.

Explanation:

The metadata concerning the phyiscal database layout necessary for automatic redirected restores driven by BackOM were created successfully.

User response:

None.

BKI8669I Free space of device with ID 'id' containing the container storage path 'storage_path' is <free_space>.

Explanation:

After assigning a container storage path to a dedicated device the remaining free space is calculated and returned to the user.

User response:

None.

BKI8670I Remaining free space of device with ID 'id' after assigning container 'container_name' of size <size> is <free_space>.

Explanation:

After assigning or creating a tablespace container on a dedicated device the remaining free space is calculated and returned to the user.

User response:

None.

BKI8671I Using automatic storage path(s) <storage_path>.

Explanation:

A dedicated automatic storage path will be used.

User response:

None.

BKI8672I Redefining container path(s) of automatic storage tablespace <tablespace_name> with ID <id>.

Explanation:

The path(s) an automatic storage tablespace uses as a starting point for the container(s) will be redefined.

User response:

None.

BKI8690E Free space test for container *path* failed. Only *free bytes* MB free space left but *required bytes* MB required.

Explanation:

The system requires a table space container of the size indicated at the path named, but there is not sufficient free space available to create it.

User response:

Try to make available the free space required, for example by

1. Removing some files on the volume or file system the container is to reside on.
2. Increasing the size of the file system the container is toi reside on.
3. Shrinking the size of the container requested so that it fits in the free space.

Note: Backup Object Manager assumes that a small part (0.05%) of the free space will be required by the operating system for administrative use. As a consequence, only 99.95% of the free space on the volume or file system is actually available.

BKI8692E The requested data could not be retrieved.

Explanation:

The TDI data of a backup image could not be retrieved and displayed.

User response:

Look for and respond to preceding error messages.

BKI8693E More than one TDI file matches your query.

Explanation:

More than one TDI file matching the search criteria was found on TSM.

User response:

Specify additional BackOM command options to restrict the result set.

BKI8700E Internal parser error in TDI parser.

Explanation:

An unexpected error occurred in the TDI parser.

User response:

Contact IBM Support.

BKI8701E This parser cannot process TDI version *version*.

Explanation:

The current version of Backup Object Manager is not compatible with the version the TDI image was created with. As a consequence, the TDI data cannot be processed.

User response:

Check the release notes for the appropriate migration procedure.

BKI8702E Too many errors. Bailing out.

Explanation:

The TDI parser encountered a number of errors. Restoring is stopped.

User response:

Check for and respond to preceding error messages in the Backup Object Manager log.

BKI8703E Out of memory.

Explanation:

The TDI parser encountered a token that cannot be read into the main memory. The TDI image cannot be processed, and restoring is stopped.

User response:

Contact IBM Support.

BKI8704E Error while reading input file.

Explanation:

The TDI parser tried to read more data from disk or from TSM, but did not succeed.

User response:

Ensure that the TDI image to be processed exists at the expected location and that the system has sufficient privileges to read it.

BKI8705E *error* in line *line number*.

Explanation:

The TDI parser encountered a syntax error in the line indicated. As a consequence, the TDI image cannot be analyzed.

User response:

Respond to the error message and correct your TDI image.

BKI8706E The container at *path* is inappropriate for table space *tablespace*.

Explanation:

The container at the location indicated cannot be added to the table space named because of incompatible properties.

User response:

Check the properties of the container and the table space. Ensure that the IDs of the containers are unique for the table space named.

BKI8707E Missing statement *keyword* in block *block name* near line *line number*.

Explanation:

A keyword is missing in the named block ending at the line given.

User response:

Insert the required statement in the block.

BKI8708E The [TDI] header block must be the first block.

Explanation:

The TDI image does not start with the required header ([TDI] block). Only comments or whitespace are allowed before this block.

User response:

Ensure that the [TDI] block is the first block in the TDI image.

BKI8709E The required block *block name* is missing.

Explanation:

The named block is missing in your TDI image.

User response:

Insert the missing block using valid values.

BKI8710W Duplicate block *block name* ignored at line *line number*.

Explanation:

At the line indicated, a block begins whose name was encountered before. The system ignores the duplicate block; it uses the data from the first occurrence of duplicate blocks.

User response:

Make sure that block names are unique within a TDI image.

BKI8711W Duplicate statement *keyword* ignored in line *line number*.

Explanation:

At the line indicated, a duplicate statement was encountered within a block. The system ignores the duplicate statement.

User response:

Make sure to not specify duplicate statements within a block.

BKI8728E Could not attach to instance ’instance’.

Explanation:

BackOM was not able to attach to the instance ’instance’.

User response:

First, check the system environment for possible instance candidates. Try the action again by additionally specifying the BackOM command option ’-i <instance name>’.

BKI8729I Checking system resources ...

Explanation:

Prior to starting the redirected restore by BackOM the existing system resources, e.g. free space of a file system will be checked.

User response:

None.

BKI8730I Scaling table space containers to *number* percent ...

Explanation:

All table space containers will be increased by the percentage indicated during the table space container redefinition step.

User response:

None.

BKI8731I Normalizing table space containers ...

Explanation:

All containers of a table space will be of the same size after redefinition.

User response:

None.

BKI8732E The TDI used for redirected restore contains an invalid database alias.

Explanation:

There is an invalid database alias specified in the *alias* statement of the TDI image.

User response:

Provide a valid alias.

BKI8733E The TDI used for redirected restore contains an invalid instance name.

Explanation:

There is an invalid database instance specified in the *instance* statement of the TDI image.

User response:

Provide a valid instance name.

BKI8734E The TDI used for redirected restore contains an invalid partition number.

Explanation:

There is an invalid partition number specified in the *Node* statement of the TDI image.

User response:

Provide a valid partition number.

BKI8736E Table space *tablespace* must have at least one container.

Explanation:

The TDI image defines the table space named without containers.

User response:

Ensure that there is at least one container associated with every table space.

BKI8737E Table space *tablespace* has containers with the combined storage too small.

Explanation:

The number of used pages of the table space named exceeds the combined size of its table space containers defined in the TDI image.

User response:

Ensure that every table space has containers of a combined size that is sufficient to hold the used pages of the table space.

BKI8738E **The container at *path* has a page size that is incompatible with its table space.**

Explanation:

The container indicated does not have the same page size as its table space according to the definitions in the TDI image.

User response:

Contact IBM Support

BKI8739E **The type of the container at *path* is incompatible with its table space.**

Explanation:

The container indicated cannot be used with its associated table space according to the definitions in the TDI image. SMS table spaces can only have path containers, and DMS table spaces must have file or device containers.

User response:

Ensure that the appropriate types of containers are used with each table space

BKI8740E **The path *path* of a container must not be relative.**

Explanation:

In the TDI image, the named path defining a container does not seem to be a fully qualified path.

User response:

Ensure that all paths in your TDI are fully qualified

BKI8741E **The container at *path* would overwrite existing files or directories.**

Explanation:

The TDI image contains the definition of the container indicated whose location is already in use. This is only allowed when restoring to the source database. Restoring to a different location is stopped.

User response:

Ensure that all path containers defined in the TDI image point to non-existing paths and all file containers point to non-existing files

BKI8742E **The container at *path* is a device container which is not supported.**

Explanation:

In the TDI image, a device container is defined. However, device containers are not supported by Backup Object Manager.

User response:

Do not use device containers.

BKI8743I **Local TDI check returned *return code*.**

Explanation:

The TDI with the target database table space definition was checked. If the return code given does not equal 0 errors occurred.

User response:

In the case of a non-zero return code, contact IBM Support.

BKI8744I **TDI replacement check returned *return code*.**

Explanation:

The system checked whether the table space definitions of the target TDI can replace the definitions of the source TDI. If the return code given does not equal 0 the table space definitions of the target TDI are not valid.

User response:

In the case of a non-zero return code, contact IBM Support.

BKI8745E **The TDI is invalid.**

Explanation:

The TDI with the target table space definitions is not valid. Restoring to a different location is stopped.

User response:

Check the Backup Object Manager log for the return code of the validation. Check for and respond to preceding error messages in the Backup Object Manager log.

BKI8746I **The TDI is valid.**

Explanation:

The TDI with the target table space definition is valid. Processing continues.

User response:

None.

BKI8747E **Not all table spaces of the original database are contained in the TDI.**

Explanation:

At least one table space of the original database is missing in the TDI definitions of the target database. However, a new location must be given for all table spaces of the original database. Therefore, restoring to a different location is stopped.

User response:

Provide the information on the missing table spaces and their containers.

BKI8748E The TDI does not define enough storage to hold all the data of the original database.

Explanation:

The target TDI has at least one table space whose containers are too small to hold the data of the source database.

User response:

Increase the container size or add more containers to the table spaces.

BKI8749E The page size of a table space in the TDI does not match the one of the original database.

Explanation:

The target TDI contains at least one table space with a matching ID in the source TDI, but their page sizes do not match.

User response:

Ensure that table spaces have the same page sizes in both the source and the target TDI.

BKI8750E The number of used pages of a table space in the TDI does not match the one of the original database.

Explanation:

The target TDI contains at least one table space with a matching ID in the source TDI, but the number of used pages of the target table space does not match the number of used pages in the original database.

User response:

Ensure that the number of used pages of a table space is the same in both the source and the target TDI.

BKI8751E The table space type in the TDI does not match the one of the original database.

Explanation:

The target TDI holds at least one table space with a matching ID in the source TDI, but the table space types are different.

User response:

Ensure that the type of a table space is the same in both the source and the target TDI.

BKI8752E BackOM does not support redirected restore with device containers.

Explanation:

The target TDI contains at least one definition of a device container. However, device containers are not supported by Backup Object Manager's redirected restore function.

User response:

Do not use the Backup Object Manager's redirected restore facility for device containers.

BKI8753E A container cannot be created at *path*.

Explanation:

Either the location where the table space container is to be created does not exist, or the permissions of the user are not sufficient.

User response:

Check the location and the permissions.

BKI8755I Getting reference TDI from TSM ...

Explanation:

Retrieving the appropriate TDI to be used by internal checking routines from the TSM server.

User response:

None.

BKI8756W Could not get reference TDI from TSM. No input validation is done.

Explanation:

The system could not find a TDI image matching the database backup to be restored on TSM. The restore action will be continued, but the input data cannot be validated before the restore starts.

User response:

None.

BKI8757I Performing redirected restore from *source alias* to *target alias*...

Explanation:

Redirected restore of *source alias* to *target alias* is starting.

User response:

None

BKI8758E The TDI does not contain data for table space *tablespace*.

Explanation:

A definition of the table space named is expected to be provided in the TDI, but could not be found.

User response:

Ensure that all table spaces of the source database are also defined in the target TDI.

BKI8759E Redirecting of at least one container failed.

Explanation:

The system tried to create the containers for a table space, but at least one of them could not be redirected to a different location. Usually, the location of one of the table space containers is not allowed. A list of containers the system tries to create can be found in the Backup Object Manager log. One of them failed.

User response:

Check for and respond to further error messages in the Backup Object Manager log.

BKI8760E Not all directories for the containers could be created.

Explanation:

The system tried to create the directories to place the containers in, but at least one failed.

User response:

Ensure that the system has sufficient privileges to create the directories at the desired locations.

BKI8761E The container at *path* does not have the minimum size of two extends.

Explanation:

A table space container to be created must have at least the size of two extends.

User response:

Correct the size of the container to be created.

BKI8762I Set table space container with ID *id* and name *tablespace_container*.

Explanation:

Backup Object Manager redirects a table space container to the ID and name indicated.

User response:

None.

BKI8763E The extent size of a table space in the TDI does not match the one of the original database.

Explanation:

The extend sizes of corresponding table spaces defined in the source and target TDIs must be equal. However, for at least one table space different extend sizes are defined in the source and target databases.

User response:

Define matching extend sizes for corresponding table spaces.

BKI8765I Testing redirected restore from *source alias* to *target alias* ...

Explanation:

The system is testing whether the original database can be restored to the target location. It checks whether

- the file system where the table space containers are to be created has sufficient free space. (If specified, normalizing and scaling are also considered.)
- there are existing files and directories identical to the containers defined for the target database. This would indicate that a database of same name and of same structure already exists, and data could be overridden.
- the structures of the source and target databases (table space types, page sizes, extend sizes) allow for a redirected restore.

User response:

None.

BKI8766I Check successful. Redirected restore possible with these settings.

Explanation:

The redirected restore test finished successfully. Thus, the redirected restore operation can be started with the options specified for the test run.

User response:

None.

BKI8767W Warnings occurred.

Explanation:

The redirected restore test detected one or more minor conflicts. These conflicts may or may not prevent a successful redirected restore operation. Nevertheless, it is recommended to resolve them.

User response:

Check for and respond to preceding warning messages in the Backup Object Manager log.

BKI8768E Check failed. Redirected restore not possible with these settings.

Explanation:

The redirected restore test detected one or more major errors which will prevent a successful redirected restore with these settings.

User response:

Check for and respond to preceding error messages in the Backup Object Manager log.

BKI8769E Found multiple TDIs matching the given timestamp. Additional search conditions needed.

Explanation:

More than one TDI file for a database backup image was found on the TSM server. In such a scenario, the integrity of the metadata assigned to a database backup images is violated and prevents an automatic redirected restore driven by BackOM.

User response:

Contact your IBM support personnel.

BKI8770I Getting TDI for redirected restore from TSM ...

Explanation:

The system is retrieving the TDI image from the TSM server.

User response:

None.

BKI8771E The TDI for the redirected restore could not be retrieved.

Explanation:

The TDI image specified could not be found.

User response:

Provide the correct location of the TDI image.

BKI8772E The selected database has a structure that prevents automatic cloning.

Explanation:

You tried to clone an SAP database using redirected restore, but the database does not have the default directory structure of an SAP database. The cloning facility of Backup Object Manager redirected restore cannot be used for this system.

User response:

You may use either the interactive or the batch mode of Backup Object Manager redirected restore.

BKI8773E The interactive modification of the containers failed.

Explanation:

You tried to interactively change the location of containers, but this operation failed.

User response:

Contact IBM Support.

BKI8776E You are not allowed to delete this container.

Explanation:

You tried to delete the last container of a table space. However, at least one container must be available to every table space.

User response:

Make sure that there is at least one container defined for every table space.

BKI8798E You cannot continue as there are errors.

Explanation:

You tried to start a restore operation after redefining the containers interactively, but errors were detected in the input data. The operation cannot continue.

User response:

Check all table spaces with '!!' error marks in the list and correct the definitions of their containers. Then continue.

BKI8799E A container must have a size of at least twice the extent size (minimum size for this table space).

Explanation:

The container size specified is too small. The minimum size of a container is twice the extent size.

User response:

Correct the container size.

BKI8800I The command is: ***command*****.**

Explanation:

Displays the command that was issued. The following commands are possible: `Backup`, `Restore`, `Archive/Retrieve`.

User response:

None.

BKI8801I **PID of calling process:** ***PID_number*****.**

Explanation:

Displays the process id of the DB2 process which called the shared library.

User response:

None.

BKI8802I **Found** *number* **backup image(s) on TSM server.**

Explanation:

For restore and delete operations Data Protection for SAP queries TSM for backup images by means of a timestamp and shows the number of found images.

User response:

None.

BKI8803I **The DB2 backup image size for this session is about** ***size*****.**

Explanation:

The estimated size of the data to be backed up is displayed.

User response:

None.

BKI8804W **The recovery log could not be written.**

Explanation:

After every backup or restore, Data Protection for SAP writes a record into the recovery log file `tdprlf.<SID>.<node_name>.log`. It is located in the path pointed to by environment variable TDP_DIR.

User response:

Check, if the permissions are set correctly and if there is sufficient free space in your file system.

BKI8805I **The restore was cancelled by the user. Existing data was not overwritten.**

Explanation:

The existing database is still operational.

User response:

None.

BKI8806I *product version.release.modification (Beta) build_number build_data*

Explanation:

Writes version information into the product log file.

User response:

None.

BKI8807I **Archive log file** *log number* **of chain** *log chain number***.**

Explanation:

Writes information about the log file to be archived into the product log file.

User response:

None.

BKI8808I **Retrieve log file** *log number* **of chain** *log chain number***.**

Explanation:

Writes information about the log file to be retrieved into the product log file.

User response:

None

BKI8810I **Cleaning up resources of process** ***PID_number*****.**

Explanation:

All resources used by the product will be released.

User response:

None.

BKI8812I **Committed TSM sessions will be deleted.**

Explanation:

During a backup with multiple sessions, an error occurred. The backup operation is stopped. TSM sessions already committed during this operation are being deleted from the TSM server in order to prevent them from being considered restorable.

User response:

None.

BKI8813E **Error deleting committed TSM sessions.**

Explanation:

One or more committed TSM sessions could not be deleted during the postprocessing of the failed backup run.

User response:

Use the Backup Object Manager to delete the file(s) manually..

BKI8814I **Inquire TSM with mask *search mask*.**

Explanation:

The string denoted is used to inquire TSM for backup images.

User response:

None.

BKI8815I **Information for Log Manager:** *DB2_instance DB2_database_name DB2_database_alias log_and_log_chain_number partition*

Explanation:

The information listed is provided to the DB2 Log Manager.

User response:

None.

BKI8816I **DB2 version 'version' detected**

Explanation:

TSM for ERP is running on a system where DB2 version 'version' is set up.

User response:

None.

BKI8817I **No corresponding committed TSM session(s) found. Nothing will be deleted.**

Explanation:

The cleanup of a failed TSM for ERP database backup could not find any partial TSM backup image of that run already stored on the TSM server for deletion.

User response:

None.

BKI8818W **Invalid value specified for BACKOM_LOCATION.**

Explanation:

The BackOM executable was not started for collecting database metadata due to an invalid specification.

User response:

Check the value of the TSM for ERP configuration parameter BACKOM_LOCATION. The parameter can be found in the vendor environment file and must contain the fully qualified name of the BackOM executable.

BKI8819I **The TSM objects matching 'search mask' will be deleted.**

Explanation:

The cleanup of a failed TSM for ERP database backup will delete any partial TSM backup image of that run already stored on the TSM server and matching 'search mask' .

User response:

None.

BKI8820E **No valid TSM session found.**

Explanation:

A running TSM for ERP workflow could not continue due to a missing TSM session.

User response:

Contact your IBM support personnel.

BKI8821I **Using option(s) 'options'.**

Explanation:

The 'options' string specifies vendor options that DB2 provides to the TSM for ERP library as part of the calling function. These could be options directly provided as part of the database backup or restore command or options made persistent in the database configuration, here the parameters VENDOROPT, LOGARCHOPT1 or LOGARCHOPT2.

User response:

None.

BKI8822I **Configuration parameter(s): parameters**

Explanation:

The list specifies a set of runtime parameters that the TSM for ERP library is using for the calling workflow.

User response:

None.

BKI8823W **Configuration parameter SRC_DB_ALIAS requires parameter SRC_DB_INSTANCE and vice versa.**

Explanation:

To be able to recover a database after a redirected restore using the built-in DB2 rollforward command, TSM for ERP needs both SRC_DB_ALIAS and SRC_DB_INSTANCE.

User response:

Include both parameters SRC_DB_ALIAS and SRC_DB_INSTANCE in the TSM for ERP vendor environment file and retry the database recovery.

BKI8899E Interface problem in function <function>: Value '<value>' of parameter '<parameter>' is not supported with DB2 version '<version>'.

Explanation:

An unknown action code during the program execution was encountered.

User response:

Contact your IBM support personnel.

BKI9001E Internal error: *error*

Explanation:

The following internal error: *error* has been encountered.

User response:

Contact IBM Support.

BKI9003E Incompatible components installed: *component name component name*

Explanation:

The components mentioned in the message text can not be used together. This may be the result of an incomplete upgrade.

User response:

Contact IBM Support.

BKI9005E *A* **not supported by** *B***.**

Explanation:

The installed version of product *B* does not support product *A*. Most likely you need to upgrade product *B*.

User response:

Contact the IBM Support.

BKI9006E Internal error while reading environment variable: *variable***.**

Explanation:

This is an internal error.

User response:

Contact IBM Support.

BKI9007W An error occurred while terminating the application: *the error*

Explanation:

While terminating the application, an error occurred. This has no impact on the success of the operation.

User response:

None

BKI9008E This product requires at least version *number* **of** *product name* **to be installed.**

Explanation:

The version of the application *product name* is not supported by this application. Most likely application *product name* needs to be upgraded.

User response:

Contact IBM Support.

BKI9009W The following products are not compatible: *product name* **(***product version***) and** *product name* **(***product version***).**

Explanation:

This message is similar to BKI9008E. But in this case it's not obvious which one of the products needs to be upgraded. .

User response:

Contact IBM Support

BKI9010E Could not determine installation directory for <program>. Please restart the process using a fully qualified name.

Explanation:

The name of the path where a given program is located could not be determined.

User response:

Contact your IBM support personnel.

BKI9011E There was no response received within <number> seconds; time has expired.

Explanation:

The communication between two program components was supended or stopped, which can lead to a timeout.

User response:

Contact your IBM support personnel.

BKI9013E Concurrent restore of objects being backed up with multiple device agents is not supported.

Explanation:

This special restore scenario is unsupported.

User response:

Contact your IBM support personnel.

BKI9014E Failed to load library: <library> reason: <reason>

Explanation:

The ACS library could not be loaded.

User response:

Contact your IBM support personnel.

BKI9015E Failed to locate functions in library: <library> reason: <reason>

Explanation:

One or more functions could not be found in the ACS library.

User response:

Contact your IBM support personnel.

BKI9200E Additional support information: An exception was thrown at position: *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support

User response:

Contact IBM Support.

BKI9201E Additional support information: An Exception was thrown at position: *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support

User response:

Contact IBM Support.

BKI9202E Additional support information: An Exception was thrown at position: *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9203E Additional support information: An exception was thrown at position: *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support

User response:

Contact IBM Support.

BKI9204E Additional support information: An Exception was thrown at position: *position* **(text=***description***).**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9205E Additional support information: Unable to instantiate *name* **at position** *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9206E Additional support information: Unable to use *actual* **when expecting** *expected* **at position** *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9207E Additional support information: An exception was thrown at position: *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9208E System error *errno*: *errno text* at position *position*.

Explanation:

A system call failed with *errno*.

User response:

Check *errno* and *errno text* with you system administrator. If you cannot resolve the problem, contact IBM Support.

BKI9209E Additional support information: No handler registered for message type *message*. Thrown at position: *position*.

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9210E ESD_AbortDispatchingException thrown at position: *position*.

Explanation:

An internal error occurred.

User response:

Contact IBM Support.

BKI9211E Additional support information: An Exception was thrown at position: *position*. (State *state*)

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9212E Additional support information: No handler registered for message type *type*. Thrown at position: *position*.

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9213E Internal error: A memory allocation request failed at position: *position*.

Explanation:

This error message indicates an out-of-storage condition. It may occur due to a previous error, or it may be owed to a large size of the internal buffers

User response:

Check for and respond to preceding error messages. You may also want to reduce the size of the internal buffers (keyword BUFFSIZE in the Data Protection for SAP profile).

BKI9214E Additional support information: An exception was thrown from a destructor. Callstack follows: *callstack*.

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9215E The maximum string length supported for <name> is <length>.

Explanation:

The supported string length of a system component, e.g. file name or hostname has been violated.

User response:

Check the components involved in the operation. If the problem cannot be resolved contact your IBM support personnel.

BKI9216E Additional support information: An exception was thrown at position: *position*.

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9217E Additional support information: An exception was thrown at position: *position*.

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9218E Additional support information: An exception was thrown at position: ***position*****.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9219E Additional support information: Invalid error type ***type*** **encountered.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9220E Additional support information: Second call of ***call*****.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact your IBM Support.

User response:

Contact your IBM Support.

BKI9221E The operation ended prematurely with return code <rc>. An exception was thrown at position: <file>(<line>).

Explanation:

An operation could not be finished successfully due to an unexpected termination.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI9222E A snapshot-type operation was interrupted. Additional support information: An exception was thrown at position: <file>(<line>).

Explanation:

A snapshot operation could not be finished successfully due to an unexpected interruption.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI9223E The operation will be aborted.

Explanation:

In internal error during an operation leads to an abort of that operation.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI9224E The operation will be aborted due to a previous error.

Explanation:

An internal error during an operation leads to an abort of that operation.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI9225E The keyword <*keyword*> has not been found in the line <*line*> of the file <*file_name*>. Please change it back to the original value if you modified it.

Explanation:

Occurs for example if the entries in the file /etc/inittab have been modified before a second installation.

User response:

Change the modified <*line*> in the <*file_name*> back to the original value, <*keyword*> gives a hint to what is expected.

BKI9300E Additional support information: Aborting 'send' operation. See previous error.

Explanation:

This error may have been caused by previous errors.

User response:

Check for previous errors and correct them.

BKI9301E Additional support information: State *state* **does not match state pattern** *pattern***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact your IBM Support.

BKI9302E Additional support information: Unused ESD_ReturnChannel destroyed. Dumping callstack: *callstack*

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact your IBM Support.

User response:

Contact your IBM Support.

BKI9306I Dumping callstack: *call stack***.**

Explanation:

This message is always preceded by an error message indicating the problem. It provides additional information that might help IBM Support to analyze the cause of the problem.

User response:

If you need to call IBM Support, provide the information given in this message together with the error information.

BKI9307E Did not find a winsock dll compatible with version *expected version***. Version found is** *available version*

Explanation:

The product failed to load the appropriate `winsock dll`.

User response:

Contact your system administrator

BKI9308E A socket request timed out after processing *number of bytes* **bytes** *position***.**

Explanation:

A socket request was issued with a timeout and the requested action could not be completed within the time specified. It was cancelled after processing *number of bytes* bytes.

User response:

If you need to call IBM Support, provide the information given in this message together with the error information.

BKI9309E Operation terminated due to an explicit abort request.

Explanation:

An operation was terminated due to customer intervention.

User response:

None.

BKI9310E Could not add *backup_id* **to the repository at** *path***.**

Explanation:

The system was not able to add information on the named backup to the repository located in the path indicated.

User response:

Make sure the repository path is set correctly. If you need to correct the repository location, restart the server executable afterwards. If the problem persists contact your IBM support personnel.

BKI9311E Could not find *backup_id* **in the repository at** *path***.**

Explanation:

Information on the backup denoted by the backup ID could not be found in the repository located in the path indicated.

User response:

Make sure the repository path is set correctly. If you need to correct the repository location, restart the server executable afterwards. If the problem persists contact your IBM support personnel.

BKI9312E *backup_id* **is currently locked in the repository at** *path***.**

Explanation:

The information on the backup denoted by the backup ID is currently locked by a different process. Make sure to run only a single operation using a specific backup at a time.

User response:

Wait for the other operation to finish or abort this operation. Then start again. If the problem persists contact your IBM support personnel.

BKI9313E Failed to update *backup_id* in the repository at *path*.

Explanation:

The information on the named backup could not be updated in the repository located at the path named.

User response:

Check the logs for other messages pointing to the cause of this problem. Resolve any problems indicated. If the problem persists contact your IBM support personnel.

BKI9314E Could not remove *backup_id* from the repository at *path*.

Explanation:

An attempt to remove the information on the backup named from the repository located at the path indicated failed.

User response:

Check the logs for other messages pointing to the cause of this problem. Resolve any problems indicated. If the problem persists contact your IBM support personnel.

BKI9315E Could not access the repository at '*path*' because it is currently locked by another process.

Explanation:

When starting up, the server tried to load the repository located at the path named. However, the repository was locked by a different process. This can happen if two server processes try to use the same repository. This is not supported.

User response:

Make sure each instance of the server uses its own repository.

BKI9316E The path '*path*' does not point to a valid repository location.

Explanation:

When starting up, the server could not locate its repository.

User response:

Correct the profile or the call as appropriate.

EEO Messages

EEO0020I ====>Performing Data Protection for Snapshot Devices <v1> command.

Explanation:

This message is displayed starting the specified function.

User response:

None.

EEO0022I AIX Version: <var1> Oslevel: <var2>.

Explanation:

This message displays the AIX version and oslevel.

User response:

None.

EEO0030I Number of volumes involved in the FlashCopy: <v1>

Explanation:

This message displays the number of volumes to be processed by FlashCopy.

User response:

None.

EEO0056I Received error 'errno' while disabling the new resources.

Explanation:

An error occurred when the process attempted to disable the resources obtained for performing the DB backup.

User response:

Check the error log for details.

EEO0058I Received error 'errno' while resetting the target volumes.

Explanation:

An error occurred when the process attempted to withdraw the FlashCopy relationship between the source and target volumes.

User response:

Check the error log for details.

EEO0059E The database was backed up using NOCOPY type of FlashCopy. The data in the target volumes is not valid, and cannot be used to perform a FlashCopy Restore.

Explanation:

To restore the database using a FlashCopy restore, the database needs to be backed up using the COPY or INCR type of FlashCopy.

User response:

Restore the database from the Tivoli Storage Manager server.

EEO0062E The source/target LUN information in the profile has been modified. FlashCopy Restore is currently not supported for restoring the database to a new location.

Explanation:

The source/target information in the profile cannot be modified.

User response:

Use a different profile to back up the database to different target LUNs. If you want to restore the database to a new location, restore it from the Tivoli Storage Manager server.

EEO0065E IBM2105 Copy Service CLI is not installed.

Explanation:

The ibm2105cli.rte file is not installed. The lslpp -lc ibm2105cli.rte command failed.

User response:

Make sure Copy Service CLI is installed on the host machine.

EEO0066W WARNING! Incremental FlashCopy cannot be performed on this version of ESS CopyServices CLI. A generic FlashCopy is performed instead.

Explanation:

Incremental FlashCopy is only supported on ESS Microcode and CopyServices CLI versions 2.3.0 or later. Because this version of ESS CopyServices CLI is earlier than 2.3.0, an Incremental FlashCopy cannot be performed.

User response:

Upgrade to ESS Microcode and Copyservices CLI version 2.3.0 or later to take advantage of the Incremental FlashCopy feature.

EEO0067W WARNING! Incremental change recording is enabled. Performing incremental FlashCopy instead of COPY type of FlashCopy.

Explanation:

Incremental change recording is enabled. Performing a COPY type of FlashCopy fails in this case.

User response:

If you want to perform a COPY type of FlashCopy, withdraw the persistent FlashCopy relationship for all the source ESS volumes for this database, using the DP for ESS withdraw command.

EEO0068W WARNING! Incremental Change Recording is enabled. Performing incremental FlashCopy instead of NOCOPY type of FlashCopy.

Explanation:

Incremental Change Recording is enabled. Performing a NOCOPY type of FlashCopy fails in this case.

User response:

Withdraw the persistent FlashCopy relationship for all the source volumes for this database if you are interested in a NOCOPY type of FlashCopy.

EEO0069W WARNING! Incremental FlashCopy feature is not supported on this version of AIX: <v1>. A generic FlashCopy is performed instead.

Explanation:

Incremental FlashCopy is only supported on AIX versions 5.1.0 or later. Because this version of AIX is earlier than 5.1.0, an incremental FlashCopy cannot be performed.

User response:

Upgrade to AIX version 5.1.0 or later in order to take advantage of the Incremental FlashCopy feature.

EEO0070E Some of the volumes belonging to this database have Incremental Change Recording enabled while others do not.

Explanation:

To perform an incremental FlashCopy, all the volumes belonging to the database must have Incremental Change Recording enabled.

User response:

Withdraw the FlashCopy relationships for those volumes that have Incremental Change Recording enabled and then retry the command. For the monitor command (background monitoring process), withdraw the FlashCopy relationships and retry both the backup and monitor (background monitoring process) commands. In an SAP environment, you only need to retry the backup, because the background monitoring process is started automatically.

EEO0071I Source volume: <v1> Target volume: <v2> Pending Sectors: <v3>

Explanation:

This message displays the number of sectors that are still to be copied either from source volumes to target volumes for a backup, or from target volumes to source volumes for restore.

User response:

None.

EEO0120E A null logical volume has been detected.

Explanation:

Data Protection for Snapshot Devices could not determine a logical volume name from the list of database files.

User response:

Verify that the calling program has passed the list of database files. Check for preceding errors.

EEO0121E A null volume group has been detected.

Explanation:

Data Protection for Snapshot Devices could not determine a volume group name from the list of database files.

User response:

Verify that the calling program has passed the list of database files. Check for preceding errors.

EEO0122E An error was detected in volume group: vg1.

Explanation:

An error was returned from the specified volume group.

User response:

Verify that the target database information is specified correctly in the profile. Verify that the AIX volume manager is running. If the problem persists, gather information from the trace file and log file and contact your IBM service representative.

EEO0123E The physical volumes of the volume group <v1> were not found.

Explanation:

Data Protection for Snapshot Devices issues the command 'lsvg -M <vgname>' in an LVM mirror environment to determine the physical and logical volumes that the production database is located on. This command failed.

User response:

Check the return code of lsvg. Consult the AIX system documentation.

EEO0124I Mounting file system: fs1.

Explanation:

Data Protection for Snapshot Devices is currently attempting to mount the file system.

User response:

None.

EEO0125E The serial number for the device 'logdev' could not be found.

Explanation:

Data Protection for Snapshot Devices determines the volume serial numbers from the list of database files that is passed. To do this, several system commands are used, such as `lscfg -pvl devname` or `lsvpcfg`.

One of these commands has failed or the specified device was not displayed.

User response:

Check the specific error message. Issue the commands above from the command line and check that the specified device is displayed in the list. Consult the AIX system documentation.

EEO0126I Trying to find new devices to match the source device. This process will take some time...

Explanation:

Data Protection for Snapshot Devices is currently trying to find a target device to match the source device.

User response:

None.

EEO0127I Removing device: devname

Explanation:

Data Protection for Snapshot Devices removes the logical devices from the Device Configuration database (ODM) on the backup system after the backup has ended and before withdrawing the relationships of the volumes.

User response:

None.

EEO0128E Configuring the target volume would cause a duplicate physical volume ID: pvid1

Explanation:

A different set of target volumes that was previously associated with the same source volumes was detected.

User response:

Perform one of the following:

- Delete the disk on the backup system only:
  1. Find the disk using the AIX lspv command
  2. Run smitty and choose the following from the menu: devices- fixed disk- remove a disk- select the disk to be removed
  3. Press return
- Clear the `pvid` of each physical volume hdisk by issuing the AIX chdev command with the following arguments: `chdev -1 (hdisk#) -a pv=clear`

EEO0129E Removing device parm1 failed.

Explanation:

Data Protection for Snapshot Devices removes the logical devices from the Device Configuration database (ODM) on the backup system after the backup ended and before withdrawing the relationships of the volumes. The `rmdev` command failed.

User response:

Check the specific error message. Consult the AIX system documentation. Check whether the device is a member of an active volume group. Check for preceding errors.

EEO0130W Removing the mount point directory <mntpt1> failed with rc: <rc1>

Explanation:

An error occurred while trying to remove a mount point. Processing continues.

User response:

None.

EEO0131E The physical volume ID <pvid1> is duplicated on the production machine.

Explanation:

The output of the command lspv shows that two logical devices (hdisk/vpath) have the same physical volume ID.

User response:

Perform one of the following:

- If the hdisks with the same pvid belong to the same multipath, convert the hdisk device volume group to a Subsystem Device Driver vpath device volume group.
- If the problem is the result of a corrupt ODM, consult the AIX Troubleshooting documentation.
- If the physical volume involved neither belongs to a volume group nor contains file systems to be imported in the future, you can clear the pvid by issuing the AIX chdev command with the following arguments: `chdev -l hdisk# -a pv=clear`

EEO0132W The umount command failed with rc <rc> for mount point <mntpt>

Explanation:

An error occurred while trying to remove a mount point. Processing continues.

User response:

None.

EEO0138I The FlashCopy type is set to NOCOPY. Removing disk meta data for all target disks. This backup is NOT valid for a FlashCopy Restore. Restore from TSM Server.

Explanation:

Target PVIDs are cleared. This process removes disk metadata for all target disks. These target volumes can now be used as targets for source volumes from multiple databases. However, this backup is not valid for a FlashCopy Restore. You can only restore from a Tivoli Storage Manager server.

User response:

None.

EEO0139W Removing the file system on the mount point <mntpt1> failed with rc: <rc1>

Explanation:

An error occurred while trying to remove a file system during the snapshot restore. Processing continues. The restore will resolve this problem.

User response:

None.

EEO0140I The FlashCopy type is set to COPY or INCR. Leaving disk meta data intact for all target disks. This backup is valid for a FlashCopy Restore.

Explanation:

The target PVIDs are not cleared. This process leaves disk meta data intact for all target disks. This backup can be used for a snapshot restore.

User response:

None.

EEO0141E The command lslv failed for the logical volume *volume*

Explanation:

The LVM command lslv failed with the specified logical volume.

User response:

Check that the file system /tmp contains enough space. Try to run the same command from the command line on the host and verify that it works correctly.

EEO0143E An unsupported volume group <v1> has been detected.

Explanation:

The volume group that the database has been allocated to is an unsupported type.

User response:

Make sure that volume group is not rootvg.

EEO0146E A physical disk from the volume group ’vgname’ was not found.

Explanation:

A physical disk from the specified database volume group was not found in the Device Configuration database.

User response:

Check the specific error message. Consult the AIX system documentation. Check whether this device is a member of one active volume group. Check for preceding errors.

EEO0147I Exporting volume group ’vgname’ failed.

Explanation:

Data Protection for Snapshot Devices issues the command `exportvg` before withdrawing the FlashCopy relationships to remove the volume group from the Device Configuration database. This command has failed.

User response:

Check the specific error message. Consult the AIX system documentation. Check for preceding errors during the unmount of the file systems.

EEO0148I Importing volume groups now...

Explanation:

Data Protection for Snapshot Devices is processing a comand to import volume groups.

User response:

None.

EEO0149I Newly imported volume group: ’vgname’

Explanation:

Data Protection for Snapshot Devices has successfully imported this new volume group on the backup system after the FlashCopy.

User response:

None.

EEO0150E The Logical Volume cannot be found for the file fnm1.

Explanation:

An error has occurred in determining the logical volume of a file in the list of database files.

User response:

Check the specific error message. Consult the AIX system documentation.

EEO0151E Varying off volume group ’vgname’ failed.

Explanation:

Before withdrawing the FlashCopy relationships, Data Protection for Snapshot Devices varies off the database volume group on the backup system. The command varyoffvg has failed.

User response:

Check the specific error message. Consult the AIX system documentation. Check for preceding errors during the unmount process.

EEO0152I Removing volume group fnm1...

Explanation:

Data Protection for Snapshot Devices is attempting to remove the volume groups.

User response:

None.

EEO0153I Varied off and exported volume group: ’vgname’

Explanation:

The specified volume group was varied off and exported successfully.

User response:

None.

EEO0154I **<lvname> <copy> <pv> <serialno> <status>**

Explanation:

When finding the source volumes of the production database in an LVM mirror environment, Data Protection for Snapshot Devices displays a list of all the logical volumes with the number of copies, the physical volumes, the serial numbers, and the status. The status is only displayed for stale partitions.

User response:

None.

EEO0156I **Finding the serial numbers...**

Explanation:

Data Protection for Snapshot Devices receives a list of database files to be backed up as input and from it determines the logical volumes, volume groups, and serial numbers of the physical volumes where the production database is located.

User response:

None.

EEO0161E **No volume group was found.**

Explanation:

The AIX command lsvg failed on the backup system, and the volume groups that were added after the FlashCopy could not be determined.

User response:

Check the operating system error issued by lsvg. Consult the AIX documentation.

EEO0162E **The volume group <vg1> cannot be found.**

Explanation:

The AIX command lsvg failed on the production system and the source volumes of the production database could not be determined.

User response:

Check the operating system error issued by lsvg. Consult the AIX documentation.

EEO0164E **The quorum of the volume group ’vgname’ must be off.**

Explanation:

In a high-availability LVM mirror environment, Data Protection for Snapshot Devices requires the quorum of the volume group to be set to off. If a mirror is inactive due to a failure, the database should continue working properly.

User response:

Set the quorum of the volume group off.

EEO0166E **The logical volume ’vgname’ must have at least 2 copies.**

Explanation:

If the parameter for working with LVM mirrors is active, Data Protection for Snapshot Devices requires that two copies of each logical volume exist.

User response:

Create a copy of each logical volume on separate machines. Ensure that you have a target volume for the FlashCopy in the same hardware unit for each source volume.

EEO0168E **The logical volume ’lvname’ must have the parallel scheduling policy.**

Explanation:

Data Protection for Snapshot Devices requires the parallel scheduling policy. With the parallel scheduling policy there is no primary or secondary mirror. All copies in a mirror set are referred to as copies, regardless of which one was created first.

User response:

Set the scheduling policy of this logical volume to ’parallel’.

EEO0170W **The logical volume ’lvname’ has ’number’ stale partitions.**

Explanation:

Data Protection for Snapshot Devices first checks all the logical volumes for stale partitions and initially issues only a warning if it finds any. The mirror set in the hardware unit that was chosen for the FlashCopy on this specific run must be free of stale partitions.

User response:

Check why you have stale partitions. If necessary, synchronize the logical volumes of the production database.

EEO0172E **The logical volume ’lvname’ must have mirror write consistency on.**

Explanation:

Mirror write consistency ensures data consistency among mirrored copies of a logical volume during normal I/O processing. If a system or volume group is not shut down properly, mwc identifies which logical partitions may be inconsistent. Data Protection for Snapshot Devices requires this capability to be set for the logical volumes of the production database.

User response:

Set mirror write consistency on.

EEO0174E **None of the mirror copies of the logical volume ′lvname′ resides completely on the specified hardware unit ′identifier′**

Explanation:

Data Protection for Snapshot Devices requires all the partitions of one mirror set to be on the physical volumes of one hardware unit.

User response:

Reconfigure the allocation on the production system.

EEO0176E **Some of the partitions of ′lvname′ are stale on the specified hardware unit ′identifier′**

Explanation:

Data Protection for Snapshot Devices first checks all the logical volumes for stale partitions and initially issues only a warning if it finds any. The mirror set that is in the hardware unit that was chosen for the FlashCopy on this specific run must be free of stale partitions.

User response:

Check why you have stale partitions. Synchronize the logical volumes of the production database.

EEO0178I **Could not determine the number of paths to target volumes. Using the default value of 1.**

Explanation:

Data Protection for Snapshot Devices supports SDD (Subsystem Device Driver). SDD is a pseudo-device driver that is designed to support the multipath configuration environments in the storage system and is used to enhance data availability. Data Protection for Snapshot Devices determines the number of multiple paths by querying the Device Configuration database (ODM).

User response:

To take advantage of SDD, check the Subsystem Device Driver User’s Guide for the correct configuration.

EEO0180E **Failure in changing the mount point ′mp′, return code ′rc′ from command chfs**

Explanation:

In a high-availability LVM mirror environment, Data Protection for Snapshot Devices uses the recreatevg command to create the volume groups after the FlashCopy on the backup system. Because recreatevg inserts the prefix ″/fs″ at the start of the mount point, Data Protection for Snapshot Devices must remove it by calling the command ″chfs″ for the original names.

User response:

Check the specific error message. Consult the AIX system documentation. Check for preceding errors.

EEO0182E **The same hdisk ′devname′ cannot be associated with two different vpaths (serial numbers ′serial#1′ and ′serial#2′).**

Explanation:

Data Protection for Snapshot Devices has encountered a corrupted configuration in the system.

User response:

Issue the command `lsvpcfg` to identify this error. Check the Subsystem Device Driver User’s Guide for a correct configuration.

EEO0184E **The lsvg command failed.**

Explanation:

Data Protection for Snapshot Devices uses the command lsvg to determine the physical and logical volume of the volume group. This command has failed.

User response:

Check the specific error message. Consult the AIX system documentation. Check for preceding errors.

EEO0186I **Recreating the new volume groups...**

Explanation:

In a high-availability LVM mirror environment, Data Protection for Snapshot Devices uses the `recreatevg` command to create the volume groups after the FlashCopy on the backup system.

User response:

None.

EEO0188E **the lvm queryvg failed.**

Explanation:

Data Protection for Snapshot Devices uses the system routine `lvm_queryvg` to read information of the VGDA of the volumes.

User response:

Check the specific error message. Consult the AIX system documentation. Check for preceding errors.

EEO0190E **The number of new volume groups is limited to 256.**

Explanation:

Data Protection for Snapshot Devices can support a database with a maximum of 256 volume groups.

User response:

Reconfigure the production database.

EEO0191I **Varying on volume group ’vgname’ failed.**

Explanation:

After the `importvg` or `recreatevg`, Data Protection for Snapshot Devices varies on the database volume group on the backup system. The command `varyonvg` has failed.

User response:

Check the specific error message. Consult the AIX system documentation. Check for preceding errors.

EEO0272I **Flushing the buffers to disk...**

Explanation:

Data Protection for Snapshot Devices is currently synchronizing to force the buffers to disk.

User response:

None.

EEO0273I **Unmounting the file system mntpt1...**

Explanation:

Data Protection for Snapshot Devices is currently attempting to unmount the file system from the mount point.

User response:

None.

EEO0274I **Bringing up the volume groups...**

Explanation:

The new resources are available after the FlashCopy.

User response:

None.

EEO0275I **There are too many file systems.**

Explanation:

The number of file systems exceeds the compiled limit of 4096.

User response:

Reconfigure the production database.

EEO0290E **The source volume with serial number ’serial_#’ is no longer attached to the production system.**

Explanation:

The specified physical volume was found during the FlashCopy backup as part of the database volumes on the production system. It could no longer be found on the production system during the snapshot restore.

User response:

Log on with the user root and issue the command `lsvpcfg`. Check whether the volume is displayed. Use the storage-system user interface to find out which host this volume is attached to. You can restart the snapshot restore at any time, as long as you have a valid disk backup on the target volumes.

EEO0291E **The source volume with serial number ’serial_#’ belongs to another volume group.**

Explanation:

The specified physical volume was found during the FlashCopy backup as part of the database volumes on the production system. During the snapshot restore, Data Protection for Snapshot Devices found it as a member of another volume group and cannot proceed with the restore.

User response:

You must remove this volume from the volume group if you want to use the specified FlashCopy backup for the snapshot restore. You can restart the snapshot restore at any time, as long as you have a valid disk backup on the target volumes.

EEO0292W **The logical volume ’lvname’ on the mount point ’mp’ was renamed or newly added.**

Explanation:

Data Protection for Snapshot Devices found a difference between the names of the logical volumes that were on the production database at the time of FlashCopy backup and the current logical volumes at the time of the snapshot restore.

User response:

Before all the file systems and logical volumes are removed, Data Protection for Snapshot Devices asks you during the snapshot restore if you are sure you want to continue. Data Protection for Snapshot Devices then reconstructs only the file systems that were backed up with FlashCopy. You must manually add all the additional system changes that were made after the FlashCopy backup.

EEO0293I List of the current file systems on the backed up volume groups:

Explanation:

Before starting the snapshot restore, Data Protection for Snapshot Devices displays a list of all the file systems that are currently on the production database system.

User response:

None.

EEO0294I List of file systems that will be restored:

Explanation:

Before starting the snapshot restore, Data Protection for Snapshot Devices displays a list of all the file systems that were on the production database system at the time of the FlashCopy backup.

User response:

None.

EEO0297W The newly-added volume ’logdev’ will be deleted from the database volume group ’vgname’

Explanation:

The `reducevg` command removes physical volumes from a volume group. Data Protection for Snapshot Devices calls this command during the snapshot restore to remove the physical volumes that were added to the database volume groups after the FlashCopy backup.

User response:

None.

EEO0299I To synchronize the LVM copies the following commands should be run after the FlashCopy process in the background has finished.

Explanation:

Data Protection for Snapshot Devices does not automatically synchronize the copies after the reconstruction of the LVM mirror. A basic command is created and displayed.

User response:

You must start the synchronization of the LVM mirror manually after the FlashCopy process in the background has finished.

If necessary, add additional parameters to the commands to improve the performance of the synchronization.

EEO0300E Error converting the hdisk device volume group ’vgname’ to a Subsystem Device Driver vpath device volume group.

Explanation:

For the function FlashCopy backup, Data Protection for Snapshot Devices uses the hd2vp command to convert the hdisk device volume group to a Subsystem Device Driver vpath volume group. This takes effect after the importvg and before the mount of the file systems on the backup system.

User response:

Check the return code and the error message of the `hd2vp` command. Consult the AIX system documentation.

EEO0301W The rmlv command ’lv’ ended with return code ’rc’

Explanation:

For the function snapshot restore, Data Protection for Snapshot Devices uses the `rmlv` command to remove the logical volumes that the production database should be restored to. This takes effect after the `unmount` and before the `exportvg` and the actual FlashCopy reverse.

User response:

Check the return code and the error message of the rmlv command. Consult the AIX system documentation. You can restart the snapshot restore at any time, as long as you have a valid disk backup on the target volumes.

EEO0302E Data Protection for Snapshot Devices encountered a problem when using the FlashCopy function of Copy Services.

Explanation:

Data Protection for Snapshot Devices requesteda FlashCopy to be done by the Copy Services for a set of source/target volume pairs. If the request fails in the storage system with a non-zero return code for one or more pairs, Data Protection for Snapshot Devices provides the return code and then terminates.

User response:

To identify the volumes that were the cause of the problem, view the Copy Services status log for failures. This lists the failing volumes along with details about possible causes of the problem.

EEO0303E The file system ’fs’ already has an entry in /etc/filesystems.

Explanation:

Data Protection for Snapshot Devices found that the specified file system still exists in `/etc/filesystems` on the backup system after the FlashCopy.

User response:

Normally the `exportvg` command removes the corresponding file systems from `/etc/filesystems`. Check for errors during the unmount and withdrawal process.

EEO0304W The reducevg command ’cmd’ ended with return code ’rc’

Explanation:

The reducevg command removes physical volumes from a volume group. Data Protection for Snapshot Devices calls it on:

1. Snapshot restore to remove the physical volumes added after the FlashCopy backup
2. Snapshot restore with LVM mirroring to remove the physical volumes that are located in the hardware unit that is not yet involved in the snapshot restore
3. FlashCopy backup with LVM mirroring if the environment variable IMPORTVG is set, to remove the physical volumes that are located in the hardware unit that is not yet involved in the FlashCopy

User response:

Check the return code and the error message of the `reducevg` command. Consult the AIX system documentation.

EEO0305W The extendvg command ’cmd’ ended with return code ’rc’

Explanation:

The `extendvg` command adds physical volumes to a volume group. Data Protection for Snapshot Devices calls it to add the volumes that are located in the hardware unit and are not yet involved in the snapshot restore to the database volume groups.

User response:

Check the return code and the error message of the extendvg command. Consult the AIX system documentation.

EEO0306W The mklvcopy command ’cmd’ ended with return code ’rc’

Explanation:

Data Protection for Snapshot Devices calls the `mklvcopy` command to add a copy of a logical volume to the physical volumes that are located in the second hardware unit. This call only takes effect in an LVM mirroring environment after the snapshot restore has been initiated. The snapshot restore and the recovery continue, but the second copy of the logical volumes will be missing.

User response:

Check the return code and the error message of the mklvcopy command. Consult the AIX system documentation. Check for errors during the disabling process (`unmount, rmfs, rmlv, varyoffvg, exportvg`). You can restart the snapshot restore at any time, as long as you have a valid disk backup on the target volumes.

EEO0307I Removing copies from the logical volumes...

Explanation:

Data Protection for Snapshot Devices uses the rmlvcopy command for the function snapshot restore to remove the copies of the logical volumes that are located in the second hardware unit. This takes effect after the unmount and before the exportvg and the actual FlashCopy reverse.

User response:

None.

EEO0308I Removing physical volumes from the volume groups...

Explanation:

Data Protection for Snapshot Devices uses the reducevg command for the function snapshot restore to remove the physical volumes that are located in the second hardware unit. This takes effect after the rmlvcopy and before the exportvg and the actual FlashCopy reverse.

User response:

None.

EEO0309I Adding physical volumes to the volume groups...

Explanation:

On the function snapshot restore, Data Protection for Snapshot Devices adds the physical volumes that are located in the second hardware unit to the database volume groups. This takes place after the FlashCopy reverse and the import of the volume groups.

User response:

None.

EEO0310I Adding copies to the logical volumes...

Explanation:

On the function snapshot restore, Data Protection for Snapshot Devices uses the mklvcopy command to add the copies of the logical volumes on the second hardware unit. This takes effect after the `importvg` and the `extendvg`.

User response:

None.

EEO0311W The command 'cmd' ended with return code 'rc'

Explanation:

The execution of the system command ended with the displayed return code.

User response:

Check the return code and the error message of the specified command. Consult the AIX system documentation.

EEO0312E Importing the volume group from hdisk 'logdev' failed.

Explanation:

Data Protection for Snapshot Devices uses the command `importvg` on the function FlashCopy backup. This command is issued on the backup system after the actual FlashCopy and the run of the configuration manager (cfgmgr). It takes a volume from each volume group that makes up the production database, reads its VGDA and makes this information available to the operating system.

User response:

Check the return code and the error message of the importvg command. Consult the AIX system documentation.

EEO0313E Recreating the volume group from the hdisks 'hdisks' failed.

Explanation:

Data Protection for Snapshot Devices uses the command `recreatevg` for the function FlashCopy backup if the production database is located in a high-availability LVM mirror environment. This command is issued on the backup system after the actual FlashCopy and the run of the configuration manager (cfgmgr).

The difference to the command `importvg` is that `recreatevg` creates the volume group with only the specified volumes. These form exactly the one copy on the hardware unit where the FlashCopy was issued.

User response:

Check the return code and the error message of the `recreatevg` command. Consult the AIX system documentation.

EEO0314W Removing the logical device 'logdev' with the same PVID 'pvid' in the ODM.

Explanation:

There is still a logical device (hdisk or vpath) in the state defined with the same PVID as one of the source volumes.

User response:

None.

EEO0315I Could not mount all the file systems that were originally present.

Explanation:

This message appears if, when running the function snapshot restore, a file system was found that was added after the FlashCopy backup.

User response:

You are responsible for creating the new file system after the FlashCopy reverse, but before the recovery, if this file system was already used from the production database.

EEO0316W The database volume groups do not currently contain a file system.

Explanation:

This message appears if, when running the function snapshot restore, no file system was found on the original database volume group. Following this, Data Protection for Snapshot Devices displays a list of the file systems on the FlashCopy target volumes. These are restored with snapshot restore.

User response:

None.

EEO0317W One or more errors were found disabling the production system resources. However, the FlashCopy Restore will continue.

Explanation:

This message appears if, when running the function snapshot restore, an error occurs unmounting the existing file systems and removing the volume groups. However, Data Protection for Snapshot Devices continues with the snapshot restore.

User response:

None.

EEO0320E Although the pvid <pvid> is contained in the descriptor area of the volume group <vgname>, no logical device (hdisk/vpath) has this on the production system.

Explanation:

The output of the command lspv shows that no physical volume hdisk/vpath exists with this pvid, although the pvid was found in the descriptor area of the volume group.

User response:

You very likely have an ODM corruption for the affected volume group. Check this volume group with the command lsvg -l <vgname> and lsvg -p <vgname>. Depending on the error, you have to take different actions. Consult the AIX troubleshooting documentation to repair the ODM.

EEO0321E Physical volume <hdisk> is in the descriptor area of the volume group <vgname> but does not belong to this volume group.

Explanation:

The output of the command lsvg -p <vgname> does not show that the hdisk/vpath belongs to this volumegroup, but its pvid is registered in the descriptor area of the volume group.

User response:

If the hdisks with the same pvid belong to the same multipath, convert the hdisk device volume group to a Subsystem Device Driver vpath device volume group.

If you have ODM corruption, check the affected volume group with the command lsvg -l <vgname> and lsvg -p <vgname>. Depending on the error, you have to take different actions. Consult the AIX troubleshooting documentation to repair the ODM.

EEO0322W The major number of the volume group <vgname> could not be determined.

Explanation:

The command ′getlvodm′, which is used to determine the major number of the specified volume group, failed. The option `-V` of the command ′importvg′ is not used on a snapshot restore of this backup.

User response:

Check for error messages issued by ′getlvodm′.

EEO0323W Major number *major* already exists on the production machine. The system will assign the next available major number to the volume group *vgname*

Explanation:

Data Protection for Snapshot Devices found that the major number of the given volume group is being used by another device. The importvg command is issued without the option -V <major number>. The system then generates the next available major number automatically.

User response:

Check the major numbers on the system with the command ″ls -al /dev″.

EEO0324E The production database is not in an LVM mirror environment.

Explanation:

The LVM mirroring capability of Data Protection for Snapshot Devices is on, but the database logical volumes do not have a mirror copy.

User response:

Set the parameter for LVM mirroring off, or set up the system in a high-availability LVM mirror environment.

EEO0325E Error reading the status information of the file system *fsname* : *txtmsg*

Explanation:

The system call stat failed. Check the specific error message appended to this message. In some cases you need administrator rights to execute this command.

User response:

Check the specified error message. Ensure that you have sufficient rights.

EEO0326W The file system *fsname* is not of type jfs2. The freeze/thaw function is applied only on file systems of type jfs2.

Explanation:

The freeze/thaw function is applied only on file systems of type jfs2.

User response:

None.

EEO0327E Error freezing the file system *fsname*: *txtmsg*

Explanation:

The function FREEZE failed for this file system.

User response:

Check the specific error reported by the operating system, which is appended to this message.

EEO0328E Error thawing the file system ***fsname*****:** ***txtmsg***

Explanation:

The function THAW failed for this file system.

User response:

Check the specific error reported by the operating system, which is appended to this message.

EEO0329I Freezing file system: ***fs1***

Explanation:

Currently attempting to freeze the file system.

User response:

None.

EEO0330I Thawing file system: ***fs1***

Explanation:

Currently attempting to thaw the file system.

User response:

None.

EEO0331I Performing snapshot restore of the source volume ***srcvol*** **to the snapshot** ***snapid*** **(LUN** ***lunpath*****).**

Explanation:

The snapshot restore function causes the source volume to revert to the version represented by the specified snapshot name. This message appears for each LUN that is involved in the restore process. The snap restore is performed based on the volume.

User response:

None.

EEO0332I Performing snapshot of the source volume ***srcvol*** **(LUN** ***lunpath*****).**

Explanation:

A snapshot is taken of this volume. This message appears for each LUN that is involved in the snapshot process. However, when several LUNs belong to the same volume, only one snapshot of this volume is taken.

User response:

None.

EEO0333I The snapshot ***snapid*** **was generated for the source volume** ***srcvol*** **(LUN** ***lunpath*****).**

Explanation:

A snapshot with the name displayed was taken from this volume. In a SAN environment, this message appears for each LUN thhat is involved in the snapshot process. However, when several LUNs belong to the same volume, only one snapshot of this volume is taken.

User response:

None.

EEO0350E Error obtaining the size of the target volume src1 with return code rc1.

Explanation:

The storage system query command cannot determine the size of the target volume.

User response:

Issue a `query` command from the Copy Services Web Interface to verify that the disk exists. If the problem persists, save the diagnostic information and contact IBM service.

EEO0351E The sizes of source volume src1 and target volume tgt1 are different.

Explanation:

The source volume and target volume must be the same size and be in the same hardware unit.

User response:

Issue a query command from the Copy Services Web Interface to verify that the disk exists. If the problem persists, save the diagnostic information and contact IBM service.

EEO0352E The wrong volume size for the target volume tgt1 is specified in the profile.

Explanation:

The `TARGET_VOLUME` parameter specifies an incorrect size for the target volume.

User response:

Make sure the parameter in the profile specifies a correct size for the target volume. If you do not know the exact size of the target volume, specify a dash (-) for both the source value and size value. The size of the target volume is determined automatically.

EEO0353E **Unable to open file** ***file1***

Explanation:

An error was detected when trying to open the file. The file may not exist.

User response:

Make sure that the file exists.

EEO0354I **Performing <fctype> FlashCopy of source volume <src1> to target volume <tgt1>**

Explanation:

A FlashCopy from the source volume to the target volume was requested.

User response:

None.

EEO0355E **The FlashCopy command failed.**

Explanation:

The FlashCopy command failed. This could be due to various reasons:
1. Some library or jar files may be missing from the Copy Services command line interface package.
2. The source volumes or target volumes are in another FlashCopy relationship.
3. The Copy Services command line interface package and Copy Services microcode are not in sync.

User response:
1. If there are files missing from the command line interface package, install it again.
2. If the source volumes or target volumes are in another FlashCopy relationship, wait until the concerned volumes exit the relationship or use other target volumes.
3. If the command line interface package and Copy Services microcode are not in sync, check with the storage system administrator to obtain the appropriate level of Copy Services command line interface and microcode.

EEO0356E **Cannot find a target volume to match the source volume parm1.**

Explanation:

A target volume could not be found.

User response:

Make sure that the target volumes are available to the backup system and that the syntax is correct for the following parameters:
- TARGET_VOLUME
- COPYSERVICES_PRIMARY_SERVERNAME
- COPYSERVICES_USERNAME

EEO0357I **Performing FlashCopy withdrawal of source volume <src1> from target volume <tgt1>**

Explanation:

A FlashCopy withdrawal of the source volume from the target volume was requested.

User response:

None.

EEO0358E **No target volume is available. Terminating...**

Explanation:

No target volume was found.

User response:

Make sure that the target volumes are available to the backup system and that the syntax is correct for the following parameters:
- TARGET_VOLUME
- COPYSERVICES_PRIMARY_SERVERNAME
- COPYSERVICES_USERNAME

EEO0359I **Incremental Change Recording: <val1>**

Explanation:

This message displays the value of Incremental Change Recording.

User response:

None.

EEO0360I **Querying the storage system for the size of volume volser1...**

Explanation:

A query of the target volume was requested.

User response:

None.

EEO0361I **A NOCOPY FlashCopy was performed. Withdrawing the NOCOPY FlashCopy relationship...**

Explanation:

The FlashCopy relationship between the source and target volumes terminates after the NOCOPY FlashCopy is performed.

User response:

None.

EEO0362I Checking the status of the primary Copy Services server...

Explanation:

Currently verifying the primary Copy Services server status.

User response:

None.

EEO0363I Primary Copy Services server is ready.

Explanation:

The primary Copy Services server is ready.

User response:

None.

EEO0365I Checking the status of the backup Copy Services server...

Explanation:

Currently verifying the backup Copy Services server status.

User response:

None.

EEO0366I FlashCopy was performed with <parm1> option.

Explanation:

This is the type of FlashCopy that was actually performed. It may be different from the value specified by the user, because Data Protection for Snapshot Devices overrides this value under certain conditions.

User response:

None.

EEO0367I Source and target volumes have been switched due to a previous incremental FlashCopy Restore operation. Previous target volume: <parm1> is now the source volume. Previous source volume: <parm2> is now the target volume.

Explanation:

Whenever you perform an incremental snapshot restore operation, the source and target volumes are reversed.

User response:

None.

EEO0368I The backup Copy Services server is ready.

Explanation:

The backup Copy Services server is ready.

User response:

None.

EEO0369E ERROR! Both the primary and backup Copy Services servers are not available.

Explanation:

The primary and backup Copy Services servers are not available.

User response:

Use the ESS Copy Service Web Interface to verify that the TCP/IP connection is valid for both the Copy Services servers. Also verify that the ESS is configured correctly.

EEO0370E ERROR! A Copy Services backup server has not been specified. Exiting...

Explanation:

The backup Copy Services server is not specified in the Setup File.

User response:

Use the Storage Subsystem Copy Service Web Interface to verify that the TCP/IP connection is valid for the backup Copy Services server. Also verify that the Storage Subsystem is configured correctly on the backup Copy Services server.

EEO0371I Value of FlashCopy type is: <parm1>

Explanation:

None.

User response:

None.

EEO0372I A primary Copy Services server has not been specified.

Explanation:

The primary Copy Services server is not defined in the profile. Data Protection for Snapshot Devices attempts to use the backup Copy Services server.

User response:

None.

EEO0376E Error: Target volume v1 involved in the previous backup does not exist in the profile.

Explanation:

The list of target volumes specified in the profile for restoring a specified database using snapshot restore needs to be the same as those specified in the profile at the time of FlashCopy Backup. This is necessary to ensure that a complete image of the database is available to the restore process.

User response:

Ensure that the target volumes specified in the profile are accurate.

EEO0380E An invalid value, <parm1>, has been specified for the FlashCopy type.

Explanation:

FlashCopy type can only be NOCOPY, COPY, or INCR.

User response:

Specify NOCOPY, COPY, or INCR for the FlashCopy type and retry the command.

EEO0381I Querying storage system for pending sectors for volume: <volser1>

Explanation:

A query of all the source and target volumes was requested to ensure that a background copy is not in progress between them.

User response:

None.

EEO0400E Error on running command: parm1

Explanation:

An error was detected while running a system command.

User response:

Gather log file information and contact your IBM service representative.

EEO0630E A memory allocation error has occurred.

Explanation:

Not enough memory was available to continue processing.

User response:

Ensure that the system has sufficient real and virtual memory. Close unnecessary applications.

EEO0640E Could not open trace file <v1>

Explanation:

There were some problems opening the trace file. Make sure you can open the trace file that was specified in the profile.

User response:

None.

EEO0641E Could not create the trace object.

Explanation:

There was a problem creating the trace class object.

User response:

None.

EEO1625I Number of volumes to be processed by FlashCopy: *v1*

Explanation:

The number of volumes to be processed by FlashCopy.

User response:

None.

EEO1626E An unexpected error was encountered processing a Tivoli Storage Manager for Advanced Copy Services function.
TDP function name: *function-name*
TDP function: *function-desc*
TDP return code: *TSM-rc*
TDP file: *filename* **(***line-number***)**

Explanation:

None.

User response:

Contact the TDP administrator with the information provided in this message.

EEO1627E SVC virtual disk *v1* **is not valid.**

Explanation:

The specified virtual disk was not found in the list of virtual disks provided by the connected SVC cluster.

User response:

Ensure that this virtual disk exists in the SVC cluster.

EEO1628E The source *v1* **and target** *v2* **virtual disks are in different SVC clusters.**

Explanation:

The SVC source and target virtual disks must be assigned to the same SVC cluster.

User response:

Ensure that the source and target virtual disks are in the same SVC cluster.

EEO1629E **The source** *v1* **and target** *v2* **virtual disks are of different size.**

Explanation:

The SVC source and target virtual disks must be of the same size.

User response:

Ensure that the source and target virtual disks have the same size.

EEO1630E **An error was returned calling an operation of the Common Information Model (CIM).**
TDP function name: *function-name*
TDP function: *function-desc*
TDP CIM return code: 0x*CIM-rc*
TDP file: *filename* **(***line-number***)**

Explanation:

An error occurred calling a CIM operation of the disk subsystem.

User response:

See the documentation for possible values of *CIM-rc*.

EEO1631E **A memory allocation error has occurred in file** *filename***, line number** *linenumber*

Explanation:

Not enough memory was available to continue processing.

User response:

Ensure that the system has sufficient real and virtual memory. Close unnecessary applications.

EEO1650E **The execution of command ’lscfg’ failed. Verify that the command ’tset -I -Q’ is not set in the user’s environment files .profile, .login, .dbenv_<hostname>.sh, .dbenv_<hostname>.csh, and .sapenv_<hostname>.sh, sapenv_<hostname>.csh.**

Explanation:

If the command ’tset -I -Q’ is set in the user’s environment files .profile, .dbenv_<hostname>.sh, and .sapenv_<hostname>.sh, the command ’lscfg’ fails with the output `Not a terminal` and does not return any configuration. This causes the Data Protection for Snapshot Devices script ’hdwmap.sh’ to fail.

User response:

Ensure that the command ’tset -I -Q’ is not set in the user’s environment files .profile, .dbenv_<hostname>.sh, and .sapenv_<hostname>.sh.

EEO1651I **The ONTAP filer version on this appliance is:** *n*

Explanation:

None.

User response:

None.

EEO1652W **The option fractional reserve on volume** *vol_name* **was reduced to less than 100 percent.**

Explanation:

When using N Series devices, it is strongly recommended that when the fractional reserve is set to less than 100%, you actively monitor space consumption and the rate of change of data on the volume to ensure you do not run out of space reserved for overwrites. In this case, if you run out of overwrite reserve space, writes to the active file system fail and the host application or operating system might crash.

User response:

Ensure that you monitor the space consumption. Consult the NetApp vendor for tools to monitor available space on the volume.

EEO1653I **Removing the snapshot** *namesrc1* **of source volume** *src_vol* **(LUN** *lunpath***)**

Explanation:

Removal of the specified snapshot of the source volume was requested.

User response:

None.

EEO1654E **The snap restore for volume** *volname* **with snapshot name** *snapname* **would destroy later snapshots that are required for other applications or for volume clones.**

Explanation:

N Series systems delete newer snapshots of a volume when a specific snapshot is used for snap restore. However, if one or more of the newer snapshots is currently in a ’busy’ state (that is, in use by another application or as a volume clone), they cannot be deleted until the association has terminated and the ’busy’ state is reset.

User response:

Before a snap restore, ensure that newer snapshots are not being used in other applications or as volume clones. Refer to the *Installation and User's Guide* for the procedure to determine which snapshots are affected. These must be closed before a previous snapshot can be restored.

EEO1655W DP for Snapshot Devices did not find any snapshots for volume *volname* on the N Series filer.

Explanation:

No snapshots were found for this volume in the N Series filer.

User response:

None.

EEO1656W DP for Snapshot Devices did not find any information about the N Series volume *volname*

Explanation:

An attempt to obtain information about this volume did not return any data.

User response:

None.

EEO1657E The snapshot name *snapname* for volume *volname* was not found in the snapshot list on the N Series filer.

Explanation:

Th esnapshot that is identified by this name does not exist.

User response:

None.

EEO2051W The local snapshot repository was not found on *location*

Explanation:

The specified directory for the local snapshot location does not exist.

User response:

A new local snapshot repository is built in the specified directory.

EEO2052E Information about the disk subsystem is missing.

Explanation:

The local snapshot repository could not be initialized due to missing information about the disk subsystem.

User response:

The application ensures that the disk subsystem is initialized properly. Check for preceding error messages.

EEO2053E A memory allocation error has occurred in file *filename*, line number *linenumber*

Explanation:

Not enough memory was available to continue processing.

User response:

Ensure that the system has sufficient real and virtual memory. Close unnecessary applications.

EEO2054E Operating system error *errno*: *messagetext*

Explanation:

The application encountered an unexpected-message error during the execution of a system function. The associated operating system error and message text are displayed.

User response:

Check the specific error message.

EEO2055I The local snapshot manager could not be locked.

Explanation:

The local repository has been locked by another application. This process proceeds when the other application unlocks the local repository.

User response:

None.

EEO2056I Waiting maximum of *timeout* seconds until the lock is released by the other application.

Explanation:

While the local repository is locked by another application, the program waits a specific period of time to proceed. In the SAP environment, this period is 1 hour.

User response:

None.

EEO2057E The local snapshot manager is not initialized.

Explanation:

The local snapshot repository was used without previous initialization.

User response:

The system normally ensures that the local repository is initialized. Check for preceding error messages.

EEO2058E The data container with the ID *dcID* could not be updated in the local repository.

Explanation:

During a FlashCopy backup the target set record in the local repository is updated with the corresponding properties. A failure occurred during that process.

User response:

Check for preceding error messages such as memory allocation error or other system error.

EEO2059W Cannot find a target data container that matches the source data container.

Explanation:

During a FlashCopy backup, TSM for Advanced Copy Services attempts to find a target data container that matches the source data container to satisfy the FlashCopy backup. A matching target data container could not be found.

User response:

See the rules for selecting one of multiple target data containers. For example, this message is displayed if you are trying to start a FlashCopy backup of type 'INCR' and all the target sets are being used for the FlashCopy type 'COPY'. Also make sure that the target volumes are available to the backup system and the syntax is correct for the following parameters:
- TARGET_VOLUME
- COPYSERVICES_PRIMARY_SERVERNAME
- COPYSERVICES_USERNAME

EEO2060W Cannot find a volume in the target data container *dcID* to match the source *srcvol*

Explanation:

This message indicates that a target volume could not be found in this target data container that matches a FlashCopy operation for the specified source. If multiple target data containers are being used, the processing continues checking the volumes of the next target data container.

User response:

None.

EEO2061W The target data container with ID *dcid* was not found in the local repository.

Explanation:

An inquiry of the data container with the specified ID could not be satisfied because that target set does not exist in the local repository.

User response:

Check for succeeding messages.

EEO2062W Could not find a target data container in the state *state* to fulfill the requested criteria.

Explanation:

A data container in the specified state was not found in the local repository to satisfy specific criteria requested by the application.

User response:

The criteria that have been passed is application-specific. Check for succeeding messages.

EEO2063W The local snapshot repository already exists in the directory *location*

Explanation:

An application tried to create the local repository in a directory that already exists.

User response:

Check for succeeding messages.

EEO2064I The local snapshot repository is created on the directory *location*

Explanation:

The local snapshot repository containing information about the state of the data containers is being created.

User response:

None.

EEO2065I The local snapshot repository could not be created on the directory *location*

Explanation:

A failure occurred in creating the local snapshot repository.

User response:

Look for an operating system error message.

EEO2066E Cannot read the .fct file ***filename***

Explanation:

The .fct file tha contains the target data containers was not found or is not accessible.

User response:

Check the name, path and permissions for the file.

EEO2067E The exception CLsmException was thrown. Reason: ***txt***

Explanation:

An unexpected error occurred while processing a function of the local snapshot repository.

User response:

Check the specified reason.

EEO2068E No target LUNs were found for the data container ***dcID*** **in the .fct file** ***filename***

Explanation:

The program searches in the .fct file of each specified data container for a list of entries with the label TARGET_VOLUME. Either you have an incorrect label for the target volumes of the specified data container or this data container in the .fct file does not have any target LUNs.

User response:

This error can only occur if the application does not have a GUI where you provide the input of the target data containers and the format is automatically checked. If so, check the format of the .fct file.

EEO2069E Cannot read the file ***filename*** **of the local snapshot repository.**

Explanation:

The system keeps some information about the state of the data containers locally in a file. This file was not found or is not accessible.

User response:

Check the name, the path and the permissions of the file.

EEO2070E The repository state file ***filename*** **is empty or has an incorrect format.**

Explanation:

The system keeps some information about the state of the data containers locally in a file. This file was found but the expected format of the data in not correct.

User response:

Normally the system ensures that the format of this file is correct. Check for a preceding error.

EEO2071E The data container ***dcID*** **could not be inserted in the local snapshot repository.**

Explanation:

The system keeps some information about the state of the data containers locally in a file. Inserting an entry for a new data container caused an error.

User response:

This is an unexpected error. Check for a preceding error. If no other error is indicated, collect the logs and traces and contact your IBM Support representative.

EEO2072E An unexpected error was encountered processing a TSM for Advanced Copy Services function.
TDP function name: *function-name*
TDP function: *function-desc*
TDP return code *TSM-rc*
TDP file: *filename* **(***line-number***)**

Explanation:

None.

User response:

Contact the TDP administrator with the information that is provided in this message.

EEO2073E The file ***filename*** **of the local snapshot repository could not be opened for writing.**

Explanation:

The system keeps some information about the state of the data containers in the local snapshot repository. Opening a file of this repository generated an error.

User response:

Check the permissions of the file.

EEO2727E The LUN ID ***v1*** **is not valid.**

Explanation:

The LUN ID must be 8 characters long.

User response:

Make sure the length of the LUN ID is 8 characters.

EEO2729E The operating system command '*command*' failed; rc=*rc*

Explanation:

None.

User response:

Check the return code from the operating system for more information about the failure. Issue the failing command manually to see if the same failure occurs.

EEO2730E The primary and secondary Copy Services servers are down.

Explanation:

None.

User response:

Start at least one of the Copy Services servers.

EEO2731E Cannot open the command output file *v1* for writing.

Explanation:

The file cannot be opened for writing.

User response:

Make sure you have enough space on the system and write permissions for the file.

EEO2732E The LUNs are already in use.

Explanation:

None.

User response:

Release the LUNs in order to reuse them.

EEO5250E An unexpected error was encountered. TDP function name: *function-name* **TDP function:** *function-desc* **TDP return code:** *TSM-rc* **TDP file:** *file-name* **(***line-number***)**

Explanation:

None.

User response:

If the message output contains “CIM Error”, collect the CIM Agent logs and send them to CIM support. If the indicated CIM error is “Connection Timed Out”, increase profile parameter COPYSERVICES_TIMEOUT to 12 (the default value is 6), for example, to allow for more time to check the source/target relations.

Otherwise, contact the TDP administrator with the information that is provided in this message.

EEO5297E Error while querying volume properties of volume <volume name>. Verify that the volume specified in the target volumes file exists.

Explanation:

The volume information of <volume name> cannot be found in the copy services configuration. This can be the result of a typographical error for the specified volume in the target volumes file (.fct). This error can also occur if the specified storage hardware unit cannot be found in the current copy services configuration.

User response:

Verify that the volume <volume name> specified in the target volumes file exists. In the case of ESS 800, DS6000 or DS8000, verify the CIM Agent configuration with the command

```
/opt/IBM/cimagent/verifyconfig -u <CIM user>
-p <CIM user password>
```

If the specified storage hardware unit is not found in the CIM Agent configuration, contact CIM Agent support.

EEO5298E A FlashCopy background copy is in progress between source volume: *source volume* **and target volume:** *target volume*

Explanation:

A FlashCopy background copy from a previous operation is not complete for the given source and target volumes.

User response:

Wait until the background copy is complete and retry the command.

EEO5299E A FlashCopy association exists between source volume: *source volume* **and a different target volume:** *target volume*

Explanation:

A FlashCopy association exists between the source volume and a target other than the designated target volume.

User response:

Withdraw the FlashCopy association between the source and target volumes and retry the restore command.

EEO6010T Tivoli Storage Manager for Advanced Copy Services Version @1%u, Release @2%u, Level @3%u.@4%u Data Protection for Snapshot Devices (C) Copyright IBM Corporation 2000, 2005. All rights reserved.

Explanation:

User response:

EEO7366E Unable to close trace output file *filename*

Explanation:

An error occurred during the closing of a trace output *filename* (for example, not enough disk space).

User response:

Check the specific operating system error message.

EEO7367E Unable to write to trace file ***tracefile*****. Tracing disabled.**

Explanation:

An error occurred when writing to the specified *tracefile*.

User response:

Ensure that the device for the *tracefile* is available and has sufficient space for the file. Retry the command.

EEO7826E Unable to open trace output file <filename>.

Explanation:

The Data Protection for Snapshot Devices user does not have permission to open the specified trace file.

User response:

Check the access rights for the directory of the specified trace file.

IDS Messages

IDS0064E The parameter <parameter_name> in the topic <topic_name> of the profile <.fcs filename> is not known.

Explanation:

In the section <topic_name> of the profile .fcs, a parameter was found that is not supported by Data Protection for Snapshot Devices.

User response:

Remove the cited parameter from the .fcs file.

IDS1000E Profile not specified

Explanation:

Data Protection for Snapshot Devices cannot locate the profile.

User response:

Ensure that a profile is available. Note that the `splitint` call must have the following form: <path>/splitint -p <path>/init<SID>.fcs -f <function>....

IDS1001E Function not defined

Explanation:

An invalid argument has been specified for the -f option of Data Protection for Snapshot Devices.

User response:

Ensure that you pass a valid function name with the option -f. Valid functions are: withdraw, flashcopy, password, unmount, inquire, ts_inquire, and query.

IDS1004E Subfunction not defined.

Explanation:

An invalid argument has been specified for the -s option of Data Protection for Snapshot Devices. This option has been designed for internal `splitint` use only and should not be used externally.

User response:

Do not use the -s option with the `splitint` call.

IDS1005I Start of splitint program at: ***time*****.**

Explanation:

Data Protection for Snapshot Devices started at *time*.

User response:

None.

IDS1007I End of splitint program at: ***time*****.**

Explanation:

Data Protection for Snapshot Devices ended at *time*. Control is returned to either the shell or to tsm4acs when `splitint` was called by tsm4acs.

User response:

None.

IDS1008E Parameter <keyword> in the profile file required.

Explanation:

The parameter <keyword> in the profile for Data Protection for Snapshot Devices could not be found. It must be defined.

User response:

Set the parameter <keyword> and its value in the profile for Data Protection for Snapshot Devices.

IDS1009E Directory path <path> for the IDS control file does not exist.

Explanation:

Either the entry for the parameter IDS_CONTROL_FILE is incorrect or the path does not exist.

User response:

Ensure that the parameter IDS_CONTROL_FILE in the profile has a valid path. If the path does not exist, you must create it.

IDS1010E Option -i <backup_list> not specified.

Explanation:

The function -f getresources requires the specification of the option -i <backup_list> too.

User response:

Ensure that you transfer the list of the files to back up when you call the function -f getresources. Note that in this case the `splitint` call must have the following form: <path>/splitint -p <path>/init<SID>.fcs -f getresources -i <backup_list>...

IDS1011E Option -f <function> not specified.

Explanation:

`splitint` always requires the option -f <function> with a valid function.

User response:

Ensure that the `splitint` call has the following form: <path>/splitint -p <path>/init<SID>.fcs -f <function>....

IDS1014I <subsystem message>

Explanation:

Data Protection for Snapshot Devices received an information message from the IDS subsystem.

User response:

None.

IDS1015I Start of splitint program at <timestamp>

Explanation:

Reports the activation of splitint.

User response:

None.

IDS1015W <subsystem message>

Explanation:

Data Protection for Snapshot Devices received a warning message from the IDS subsystem.

User response:

None.

IDS1016E <subsystem message>

Explanation:

Data Protection for Snapshot Devices received an error message from its IDS control part.

User response:

See the subsystem error messages for more information and perform required action.

IDS1020I The Snapshot Restore ended successfully.

Explanation:

The high-performance restore issued with the FlashCopy from the target volumes to the source volumes was completed successfully.

User response:

None.

IDS1023I Exiting with return code <rc>.

Explanation:

The `splitint` program issues this message on terminating. The program returns the value 0 if successful, or nonzero if the execution of the called function failed.

User response:

If the called function has failed, check for previous error messages.

IDS1024I Exiting with return code <rc>.

Explanation:

The `splitint` program issues this message on terminating. The program returns the value 0 if successful, or nonzero if the execution of the called function failed.

User response:

If the called function has failed, check for previous error messages.

IDS1025I Time stamp: <current_time>

Explanation:

Data Protection for Snapshot Devices performs several tasks in sequence (for example, initiate the FlashCopy of source volumes on the production system and mount file systems on the backup system). Tracking the various time stamps allows analysis of how long each task took.

User response:

None.

IDS1026I Start of splitint on the production system...

Explanation:

Data Protection for Snapshot Devices has issued a call to the production system and is waiting for the end of the execution.

User response:

None.

IDS1027I splitint ended on the production system successfully.

Explanation:

Data Protection for Snapshot Devices has ended the call to the production system successfully.

User response:

None.

IDS1028E splitint ended with errors on the production system.

Explanation:

The remote exec call to the production system has ended with errors.

User response:

Check the specific error message.

IDS1030I Snapshot started...

Explanation:

The command with the ′flashcopy′ function has been issued on the production system, and the program `splitint` waits until this action has finished.

User response:

None.

IDS1031I Snapshot successful.

Explanation:

The command for the snapshot-based copy of the volume pairs has completed successfully on the production system.

User response:

None.

IDS1032W Information from Tivoli Storage Manager for ERP was not found.

Explanation:

The exchange data between Data Protection for Snapshot Devices and Tivoli Storage Manager for ERP was not found. The information is exchanged through the call of the Data Protection for Snapshot Devices′s function ″set_bki_info″ by backint before the Tivoli Storage Manager backup. For older versions, the information is first exchanged after the Tivoli Storage Manager backup during the execution of the unmount function. Either the Tivoli Storage Manager for ERP you have installed does not support Data Protection for Snapshot Devices, or Tivoli Storage Manager for ERP has failed after a successful FlashCopy and mount.

User response:

Check the run logs of tsm4acs. This error could have various reasons and should be resolved depending on the specific situation:

Case 1: tsm4acs has finished successfully.

Result: The backup on disk (FlashCopy target volumes) as well as the one done to the Tivoli Storage Manager server are valid. However, Data Protection for Snapshot Devices cannot show the backup ID in its report when using the function ′inquire′.

Reason for warning: It is very likely that Tivoli Storage Manager for ERP (AIX version) does not have Data Protection for Snapshot Devices support (prior to version 3.1.0.3).

Action: Install the appropriate Tivoli Storage Manager for ERP version.

Case 2: tsm4acs has terminated abnormally.

Result: Carefully check the run log of tsm4acs for any BKI, ANS or ANR error messages. Most likely, the backup on disk (FlashCopy target volumes) is valid (check with `splitint -f inquire` whether PSI is PSI_MOUNT_DONE or PSI_UNMOUNT_DONE), but the backup to the Tivoli Storage Manager server is invalid.

Cause: Problems with the network or on the Tivoli Storage Manager server caused Tivoli Storage Manager for ERP to fail when running a backup.

Action: Depending on the error message, eliminate the reason for not getting a successful backup to the Tivoli Storage Manager server.

IDS1033I Information from Tivoli Storage Manager for ERP has been found with BACKUPID <backupid>.

Explanation:

The exchange data between Tivoli Storage Manager for ERP and Data Protection for Snapshot Devices has been found during the execution of the function unmount. The backups on disk (FlashCopy target volumes) as well as to the Tivoli Storage Manager server are valid. The list of files has been saved in the Tivoli Storage Manager with the backup ID <backupid>.

User response:

None.

IDS1034E Entry <field_name> in the current backup cycle of the IDS control file is missing.

Explanation:

The field with the name <field_name> in the current backup cycle was unexpectedly empty.

User response:

Check for preceding errors.

IDS1035I The IDS control file exists and a new backup cycle entry has been created.

Explanation:

At the start of the function -f getresources, Data Protection for Snapshot Devices inserts a record in the IDS control file for the new backup cycle. This record is updated as the status of the new backup cycle changes (such as FlashCopy target volumes/file systems being mounted or unmounted).

User response:

None.

IDS1036E The backup ID was not passed by Tivoli Storage Manager for ERP. This snapshot backup cannot be used for snapshot restore.

Explanation:

Before this error, the warning IDS1041W is displayed. The backup ID is mandatory for using a snapshot backup for the restore.

User response:

To use snapshot restore, ensure that you have installed DP for SAP (backint) version 3.3.10 or higher.

IDS1038I The IDS control file <ids_control_file> does not exist. It will be created.

Explanation:

Data Protection for Snapshot Devices writes the first record to the IDS control file specified in the entry IDS_CONTROL_FILE of the profile.

User response:

None.

IDS1039E The IDS control file has no entry.

Explanation:

Data Protection for Snapshot Devices has found the IDS control file, but it has no records. This error occurs when you start one of the functions inquire, withdraw or unmount before you have run the ’flashcopy’ function for the first time.

User response:

The problem is resolved after you run at least one `tsm4acs` with a successful FlashCopy.

IDS1040E The IDS control file must be read or inserted before update.

Explanation:

Data Protection for Snapshot Devices has detected a logical error when processing the IDS control file.

User response:

Contact Tivoli Storage Manager for ERP support.

IDS1041W The value of the field ’field_name’ in the file ’file_name’ is empty.

Explanation:

The program tsm4acs updates the IDS repository after the Tivoli Storage Manager backup but also in case of a disk-only backup. A temporary file is created with the following format:

```
>>> backint_data BID <backup id> UTL <name
of the application profile used> INF <DPF
backup ID> EBC <log directory> EBB <backup
type> EBR <first active log>
<<< backint_data   >>> input_file
<file list> <<< input_file
```

If one of the fields of the topic "backint_data" is empty (that is, missing), this message is displayed. If the backup ID is empty, the process terminates with error IDS1036E.

User response:

None.

IDS1042W Info data from Tivoli Storage Manager for ERP /tmp/bki<SID>.ids cannot be read.

Explanation:

Before the unmount process, Data Protection for Snapshot Devices reads /tmp/bki<SID>.ids, which contains information about the backup that was done by Tivoli Storage Manager for ERP. Among the information read is:

- Backup ID
- Util file used for the backup

- A list of the files used for the backup
- The backup type

This message is issued if Tivoli Storage Manager for ERP terminated unsuccessfully for some reason.

User response:

Ensure that Tivoli Storage Manager for ERP runs successfully.

IDS1043I The maximum number of backup cycles in the IDS control file has been reached.

Explanation:

The maximum number of backups controlled via the parameter BACKUP_MAX will be exceeded with the new inserted record. If the parameter is not set, the program uses the default value of 30.

User response:

None.

IDS1044I Delete backup cycle with BSEQ_N = <bseq_n> and all associated files...

Explanation:

The program deletes the oldest record with the backup sequence number <bseq_n> because the maximum number of records has been reached. In addition, the oldest reports and traces associated with that backup cycle are deleted.

User response:

None.

IDS1045W Directory path <directory> for the report files does not exist. Using the current directory.

Explanation:

The directory entry of the parameter LOG_TRACE_DIR in the profile could not be found. The current directory is used for the log and trace files.

User response:

To avoid directories cluttered with reports and traces, the parameter LOG_TRACE_DIR should be used, or the directory it specifies must be created if necessary.

IDS1046I Start of listing of importing volume groups/mounting file systems ...

Explanation:

After initiating the FlashCopy source/target volumes on the production system, Data Protection for Snapshot Devices makes the corresponding target volumes available to the backup host. A list of mount points or volume groups is shown.

User response:

None.

IDS1047I End of listing.

Explanation:

This message marks the end of the list of mount points or volume groups.

User response:

None.

IDS1048I The unmount process is skipped because the progress status indicator (PSI) has a value of ’psi’

Explanation:

When the ’withdraw’ function is started, the unmount process is performed only if the PSI has a value of PSI_MOUNT_STARTED or PSI_MOUNT_DONE.

User response:

The documentation shows the permissible functions depending on the backup progress status indicator.

IDS1050E The version of the splitint program must be the same on the backup and production systems.

Explanation:

The version of Data Protection for Snapshot Devices on the production system is different from the version on the backup system.

User response:

Ensure that you install the same version of Data Protection for Snapshot Devices on the production and backup systems. You obtain the version number when you start `splitint` without parameters.

IDS1051I Enter the password for the user <user ID>

Explanation:

The password for the user ID <user ID> has to be entered. It is encoded and stored in a file specified in the parameter CONFIG_FILE. Note that this user ID and password must be the same on the production and backup systems. The Data Protection for Snapshot Devices program `splitint` uses the user ID to execute a remote shell on the production system.

User response:

Enter the password for the corresponding user ID.

IDS1052I Enter the password for the user <user ID> again

Explanation:

To avoid typing errors, you must enter the password twice.

User response:

Enter the password again.

IDS1053I The password entry does not match, try again

Explanation:

The two entered passwords are not identical. You must enter the password again.

User response:

Enter the password again. You are permitted three attempts before the program terminates.

IDS1054E No password stored.

Explanation:

The two entered passwords are not identical. You have tried three times, and the passwords were different in each case.

User response:

You must start the `splitint` program with the function -f password again. If no password is stored, or it is invalid, `splitint` fails when the ’flashcopy’ function is used.

IDS1055E The config file named <config_file> could not be opened. Call splitint with the password function to create that file.

Explanation:

Data Protection for Snapshot Devices is unable to read the configuration file <config_file>.

User response:

This error could have various reasons. Try the following:

1. Call `splitint` with the ’password’ function to create the file.
2. Check the path of the configuration file. The path must be specified in the profile (parameter CONFIG_FILE).
3. Make sure that the file access permissions are set correctly.

IDS1056E The information of Tivoli Storage Manager for ERP could not be set in the IDS repository.

Explanation:

After the mount of the file systems on the backup system was finished, the call of Tivoli Storage Manager for ERP (backint) takes place. Backint then calls Data Protection for Snapshot Devices with the function ″-f set_bki_info″ to set the Tivoli Storage Manager backup ID and other information. This information is mandatory for using a FlashCopy backup for restore. This information could not now be set.

User response:

Ensure that you have a version of backint that is compatible for snapshot restore.

IDS1057E No target set entries were found in the IDS repository.

Explanation:

The target set entries in the IDS repository are generated automatically from the entries configured in the .fct file (set of target volumes). This happens during the FlashCopy backup.

User response:

Check the .fct file (set of target volumes). Check the parameters IDS_CONTROL_FILE (IDS repository) and VOLUMES_DIR (.fct file).

IDS1060I Start of listing of exported volume groups/unmounting file systems ...

Explanation:

A list of unmount points or exported disk groups is shown. Due to the use of the unmount function on the backup host, Data Protection for Snapshot Devices unmounts the file systems and export volume groups on the backup host that had been imported or mounted when the Data Protection for Snapshot Devices ’flashcopy’ function was executed.

User response:

None.

IDS1061I Start the withdrawal of the target-source pairs...

Explanation:

The command with a withdraw has been issued from the backup system to the primary Copy Services server for the storage system.

User response:

None.

IDS1062I **The progress status indicator (PSI) is already PSI_UNMOUNT_DONE.**

Explanation:

Data Protection for Snapshot Devices has been called with the function unmount, but the PSI value of the latest backup cycle was already updated to PSI_UNMOUNT_DONE in a previous `splitint` call.

User response:

None.

IDS1063E **Parameters LOGON_HOST_PROD/ LOGON_HOST_BACK in profile wrong or missing.**

Explanation:

Either Data Protection for Snapshot Devices is unable to read one of the parameters LOGON_HOST_PROD or LOGON_HOST_BACK from the profile, or the parameter values are incorrect. Note that these parameters must have the following format:

LOGON_HOST_PROD <hostname/TCP name> <user ID>
LOGON_HOST_BACK <hostname>

The host names must match the respective host names of the production and backup systems. The TCP/IP address is used for the communication between the two systems. The user ID specified must match the DB2 user ID ('db2<sid>').

User response:

Ensure that the profile contains valid entries for LOGON_HOST_PROD and LOGON_HOST_BACK.

IDS1064E **The parameter <keyword> in the profile is not known.**

Explanation:

An unknown parameter <keyword> has been found in the profile.

User response:

Check the specified parameter in the profile and try again.

IDS1065E **You cannot run the function 'function' if the progress status indicator (PSI) has a value of 'psi'**

Explanation:

The backup cycle was left in a state that does not allow Data Protection for Snapshot Devices to start the specified function.

User response:

The documentation shows the permissible functions depending on the backup progress status indicator.

IDS1066E **The option -f flashcopy can only be used on the backup system.**

Explanation:

You cannot start the flashcopy function on the production system.

User response:

Make sure you start `splitint` with the function -f flashcopy on the backup system only. Ensure that the profile contains a valid entry for LOGON_HOST_BACK.

IDS1067E **The options -f flashcopy -s performsplit can only be used on the production system.**

Explanation:

The option -s is designed for internal `splitint` use only and should not be used externally.

User response:

Make sure you issue `splitint -f flashcopy` on the backup system only. Ensure that the profile contains valid entries for LOGON_HOST_PROD and LOGON_HOST_BACK. Do not use the -s option with the `splitint` call.

IDS1068E **The option -f withdraw can only be used on the backup system.**

Explanation:

You cannot start the function withdraw on the production system.

User response:

Make sure you start `splitint` with the function -f withdraw on the backup system only. Ensure that the profile contains a valid entry for LOGON_HOST_BACK.

IDS1069E **The option -f unmount can only be used on the backup system.**

Explanation:

You cannot start the function unmount on the production system.

User response:

Make sure you start `splitint` with the function -f unmount on the backup system only. Ensure that the profile contains a valid entry for LOGON_HOST_BACK.

IDS1071E Topic named <topicname> could not be found in the file <filename>.

Explanation:

Data Protection for Snapshot Devices was able to read the file <filename> but the expected entry for the topic <topicname> was not found.

User response:

If the affected file is in the directory denoted by the parameter VOLUMES_DIR, check whether the topic name has the format:

```
>>> volumes_set_#
```

Where # is a placeholder for the volume set number (1, 2, etc.)

If the affected file is another file, you likely have another error prior to this one. Otherwise, contact Tivoli Storage Manager for ERP support.

IDS1072E The source volume <serial number> cannot be specified as a target volume in the .fct file.

Explanation:

Data Protection for Snapshot Devices found one of the source volumes in the list of target volumes in the `init<SID>.fct` file.

User response:

Ensure that the target volumes list in `init<SID>.fct` does not contain any of the source volumes.

IDS1073E No target volumes were specified for the set <volumes_set_#> in file <filename>.

Explanation:

Data Protection for Snapshot Devices has read file <filename> in the directory specified by VOLUMES_DIR. The format of the file is correct, but the list of target volumes is missing.

User response:

See the description of the target volumes file in the documentation.

IDS1074E The backup ID (timestamp) is empty. This snapshot backup cannot be used for a snapshot restore.

Explanation:

Before this error, the warning IDS1041W is displayed. The backup ID (timestamp) is mandatory for using a FlashCopy backup for the restore. The program tsm4acs was not able to generate a timestamp.

User response:

Check for preceding errors. Check whether the backup to Tivoli Storage Manager ended successfully.

IDS1075I Creating a semaphore for the critical part of importing/exporting ...

Explanation:

When multiple production systems run a backup via a single backup system at the same time, Data Protection for Snapshot Devices ensures that the critical parts of the code run for a single instance of the program at a time. These phases are:

1. When the FlashCopy has been done and resources (volume groups and file systems) are being enabled
2. Before the FlashCopy relationship is withdrawn and resources (volume groups and file systems) are being disabled.

For this synchronization process, a semaphore with the fixed key 0x88886666 is created.

User response:

None.

IDS1076I Trying to set the semaphore for the critical part of importing/exporting ...

Explanation:

If the Data Protection for Snapshot Devices semaphore is already allocated, the program waits until it is released. Otherwise, the program sets it and pass into the critical part of the run. Another instance arriving at this point now has to wait for the release of the semaphore.

User response:

None.

IDS1077I Semaphore released.

Explanation:

After the program has passed the critical part of the run, the semaphore is released.

User response:

None.

IDS1078W The semaphore could not be created. System error <sys_errno>: <sys_message>.

Explanation:

If Data Protection for Snapshot Devices could not create the semaphore, the system error number and message are issued as a warning. The concurrent run of multiple production systems with a single backup system will not work properly.

User response:

Check the system error number and message with the system administrator.

IDS1079W **The semaphore could not be initialized. System error <sys_errno>: <sys_message>.**

Explanation:

If Data Protection for Snapshot Devices could not initialize the semaphore, the system error number and message are issued as a warning. The concurrent run of multiple production systems with a single backup system will not work properly.

User response:

Check the system error number and message with the system administrator.

IDS1080W **The semaphore could not be allocated. System error <sys_errno>: <sys_message>.**

Explanation:

If Data Protection for Snapshot Devices could not allocate the semaphore, the system error number and message are issued as a warning. The concurrent run of multiple production systems with a single backup system will not work properly.

User response:

Check the system error number and message with the system administrator.

IDS1081W **The semaphore could not be released. System error <sys_error>: <sys_message>.**

Explanation:

If Data Protection for Snapshot Devices could not allocate the semaphore, the system error number and message are issued as a warning. The concurrent run of multiple production systems with a single backup system will not work properly.

User response:

Check the system error number and message with the system administrator.

IDS1082E **Duplicate target volume ’serial number’ was found in the target list.**

Explanation:

Data Protection for Snapshot Devices found a duplicate serial number for a target volume in a file residing in the directory specified in the VOLUMES_DIR parameter.

User response:

Ensure that the serial numbers of the target volumes in a file residing in the directory specified by the VOLUMES_DIR parameter are unique.

IDS1084I **This is your last chance to stop the Snapshot Restore. Enter ’c[ont]’ to continue or ’s[top]’ to cancel.**

Explanation:

Data Protection for Snapshot Devices asks the user a last time before the program begins with the restore process. The original data is overwritten with the data of the snapshot backup.

User response:

Be sure that you want to restore from the FlashCopy backup.

IDS1085E **You cannot restore from a snapshot backup of the type NOCOPY.**

Explanation:

Only the snapshot backups made with the parameter FLASHCOPY_TYPE set to COPY or INCR can be used for the snapshot restore.

User response:

Normally the calling program must make sure to determine one backup sequence number that contains a FlashCopy backup of type COPY or INCR. Check for preceding errors.

IDS1086E **You cannot run the function ’flashback’ if the backup status indicator (BSI) has a value of ’bsi_value’**

Explanation:

The ’flashcopy’ function can only be called with a backup sequence number that has a backup status of BSI_DISKONLY or BSI_DISKANDTAPE. All other values, such as BSI_START, BSI_TAPEONLY or BSI_INVALID, are not allowed.

User response:

Normally the calling program must determine one backup sequence number that contains a FlashCopy backup with one of the allowed values for the backup status indicator. Check for preceding errors.

IDS1088W **One or more errors were found disabling the production system resources.**

Explanation:

Before the actual snapshot restore to the database volume occurs, Data Protection for Snapshot Devices does the following:

1. Unmounts the database file systems
2. For LVM mirroring:
   - Remove the mirror copies from the logical volumes
   - Remove the mirror physical volumes from the volume groups
3. Remove the volume group from the AIX ODM

One or more of these operations have ended with errors. Data Protection for Snapshot Devices issues a warning but the snapshot restore continues.

User response:

None.

IDS1089E The Snapshot Restore was already started using the target set *id*

Explanation:

The background process of a snapshot restore is still in progress for the specified target set ID, and the RESTORE_FORCE parameter (in the devices section of the Data Protection for Snapshot Devices profile) is not set to YES.

User response:

There are two options:
1. Wait until the background process is finished.
2. Start a new snapshot restore with the RESTORE_FORCE parameter set to YES.

   Note: If the snapshot is of type INCR, this option breaks the INCR relations and, as a result, the snapshot restore starts a full copy of the data from the target to the source LUNs. The next snapshot backup is also a full copy.

IDS1090E The NLS catalog could not be loaded. Make sure that the catalog - *fully_qualified_catalog_name*- exists.

Explanation:

DP for Snapshot Devices uses an English NLS catalog for the LVM and storage-system parts of the product. The installation process copies the catalog to the displayed path.

User response:

Check for errors during the installation procedure.

IDS1091E You cannot run the function *function* if the restore status indicator (RSI) on target set *id* has a value of RSI_START.

Explanation:

If the restore status RSI of the target set has a value of RSI_START, then a snapshot restore is still running in the background. You cannot start a FlashCopy backup again until the background copy to the database volume is finished. In this case the RSI value is either RSI_DISKONLY or in case of LVM mirroring RSI_DISKANDLVM.

User response:

Wait until the FlashCopy background process is finished.

IDS1092E Snapshot failed.

Explanation:

The procedure for establishing the FlashCopy relationship between the source and target volumes in the storage subsystem failed.

User response:

This is a significant error because the source/target pair could be left in a different state. Check for preceding errors, and check the connection to the CIM agent and to the storage subsystem.

For a FlashCopy backup, start the ’withdraw’ function of ’splitint’ to clean up the relationships.

For a snapshot restore, restart the restore. The software detects the state and asks you for the withdraw.

IDS1093E The target set ID was not found.

Explanation:

For the handling of 2 different LVM mirror sets, you must now specify 2 different target sets in the .fct file. The parameter HARDWARE_ID_LVM_MIRROR, which determines what hardware unit should be taken as the source, is specified here under the corresponding target set as well.

Internally Data Protection for Snapshot Devices keeps the status of each target set (progress status, backup status, restore status, backup sequence number, etc) in the housekeeping directory. After the FlashCopy, Data Protection for Snapshot Devices rereads the target set information. This message is only displayed if this information was destroyed, is corrupt or something unexpected occured.

User response:

Check for preceding errors.

IDS1097E The option -f set_bki_info can only be used on the backup system.

Explanation:

Tivoli Storage Manager for ERP (backint) calls Data Protection for Snapshot Devices with the function -f set_bki_info for a FlashCopy backup on the backup machine after the mount of the file systems. This call is not allowed on the production machine.

User response:

Consult the documentation to understand the flow of the FlashCopy backup in an SAP environment.

IDS1100E The parameter ’HARDWARE_ID_LVM_MIRROR’ has to be moved from the profile ’filename.fcs’ to the corresponding target set in ’filename.fct’

Explanation:

For AIX LVM mirroring, the parameter ’HARDWARE_ID_LVM_MIRROR’ indicates the identifier of the hardware unit to be selected for the mirror copy that should be used for the FlashCopy. This parameter is now contained in the target set topics in the .fct file.

User response:

Move the parameter from the .fcs to the .fct file.

IDS1102E The target set ID ’target_set_id’ could not be read or inserted.

Explanation:

For the handling of 2 different LVM mirror sets, you must now specify 2 different target sets in the .fct file. The parameter HARDWARE_ID_LVM_MIRROR, which determines what hardware unit should be selected for the FlashCopy, is specified under the corresponding target set as well.

Internally Data Protection for Snapshot Devices keeps the status of each target set (progress status, backup status, restore status, backup sequence number, etc) in the housekeeping directory. The file containing the information of the target set could not be read or written.

User response:

Check for preceding errors.

IDS1103W The restore status indicator (RSI) has a value of RSI_INVALID on target set ***id***

Explanation:

If the restore status RSI of the target set has a value of RSI_INVALID, this means that a snapshot restore was initiated but did not terminate. Nevertheless, Data Protection for Snapshot Devices issues this warning and continue with the FlashCopy backup.

User response:

Check whether the FlashCopy backup ended successfully.

IDS1104E No target set assigned to the last backup cycle. Specify the option -n *target_set_ID*

Explanation:

When called without the ’-n’ option, the functions ’unmount’ and ’withdraw’ are applied to the last backup cycle. However, one requirement for this is that a target set was assigned to the last backup cycle. The system ensures that a target set ID is always assigned to the backup cycle during the FlashCopy backup. This error can only occur as a consequence of other very severe errors.

User response:

Call the functions -f unmount or -f withdraw together with the option -n ’target_set_ID’. To see the correlation of backup ID to target set ID call the function -f ts_inquire. Check also for preceding errors during the FlashCopy backup.

IDS1121I Getting the source volumes...

Explanation:

The first step of Data Protection for Snapshot Devices in a FlashCopy backup is to determine the source volumes from the list of files passed by the corresponding calling UI backup tool.

User response:

None.

IDS1122I FlashCopying the sources to the target volumes...

Explanation:

After finding the pairs of volumes to be copied, Data Protection for Snapshot Devices signals to the calling program to set the database into backup mode or shut down the database. Then the actual FlashCopy can be requested to the Copy Services server.

User response:

None.

IDS1123I Enabling the volumes and file systems...

Explanation:

After the FlashCopy, the target volumes attached to the backup machine are imported in the operating system and the file systems are mounted

User response:

None.

IDS1125I **Checking AIX LVM mirroring...**

Explanation:

In a high-availability LVM mirror environment, Data Protection for Snapshot Devices ensures that the LVM mirror setup complies with the requirements listed below before and after the actual FlashCopy:

1. The quorum of each involved volume group must be off. This means that if a mirror set is inactive due to a failure, the database can continue working properly (see EEO0164E).
2. Each logical volume must have at least two copies (see EEO0166E).
3. Each logical volume must have the parallel scheduling policy (see EEO0168E).
4. The mirror set that is located in the hardware unit that was chosen for the FlashCopy must be free of stale partitions (see EEO0176E).
5. All the partitions of each logical volume copy must reside on the physical volumes of the same hardware unit (see EEO0174E).
6. Each logical volume must have the mirror write consistency on (see EEO0172E). This ensures that the mirror set used for the FlashCopy is consistent from the point of view of the file system level.

User response:

None.

IDS1128I **The parameter ’CLEAR_TARGET_PVID’ in the profile ’filename’.fcs is obsolete and is ignored.**

Explanation:

This parameter is no longer needed because the clearing of the physical volume IDs now depends directly on the value of the parameter FLASHCOPY_TYPE and whether the backup is a disk-only backup.

User response:

Delete the parameter ’CLEAR_TARGET_PVID’ from the .fcs file.

IDS1129E **You cannot run an incremental FlashCopy until all the changed tracks are copied.**

Explanation:

If you set the parameter FLASHCOPY_TYPE of the .fcs file to the value INCR, then an incremental FlashCopy is issued. This means that only the data that has changed since the last time-zero (first incremental) or subsequent incremental FlashCopy is copied. This helps reduce background copy completion time when only a subset of the data has changed.

User response:

If you want to start a new time-zero FlashCopy backup in any case, you must withdraw the FlashCopy relations.

IDS1130E **The list of files passed by Tivoli Storage Manager for ERP in the file ’temp_file’ is empty.**

Explanation:

Tivoli Storage Manager for ERP calls Data Protection for Snapshot Devices with the function set_bki_info to pass, among other things, the backup ID and the list of files used by backint. This list of files was now found to be empty.

User response:

Check that you are using a compatible version of backint for snapshot restore. The version of backint must be v3.3.10 or higher.

IDS1131E **Data Protection for Snapshot Devices cannot be used for partial restores. The following database files are in the restore list but were not on the backup list.**

Explanation:

Unlike other backup techniques, Data Protection for Snapshot Devices moves the complete data on a physical volume instead of individual files. Two requirements are necessary to build a backup of a database:

1. The complete set of physical volumes making up a volume group must be moved.
2. Furthermore, all the volume groups that the database is in must also be completely moved. The operating system allows access to the data on each physical volume only if all the volumes are represented as a consistent group to the system. Also, you can only start up a database if all the volume groups containing the database files are available.

User response:

Restore the data using Tivoli Storage Manager from tape.

IDS1132E **You cannot run a snapshot backup again until all the tracks on the storage disk subsystem have been copied.**

Explanation:

This message is valid only for FlashCopy devices. If you set the parameter FLASHCOPY_TYPE to the value COPY, then a full copy FlashCopy is issued. This means that all the data from the source to the target LUNs is copied, regardless of whether it has changed since the last time-zero FlashCopy.

User response:

f you want to reduce the amount of data copied, you should consider using copy type INCR instead of COPY.

IDS1133E Some of the production logical volumes are mirrored. You have to set the hardware unit ID in the parameter HARDWARE_ID_LVM_MIRROR for the corresponding target set in the .fct file <filename>.

Explanation:

Data Protection for Snapshot Devices found that some of the logical volumes that the production database is located in are mirrored using the mirror capability of the Logical Volume Manager. However, the parameter HARDWARE_ID_LVM_MIRROR was not specified in the .fct file. This parameter causes Data Protection for Snapshot Devices to make all the necessary checks to get a consistent copy via the FlashCopy on the target volumes in an LVM mirror environment.

User response:

Set the parameter HARDWARE_ID_LVM_MIRROR with the hardware unit ID that is used for the FlashCopy.

IDS1134I Disabling the volumes and file systems...

Explanation:

Before the snapshot restore from the backup to the production volumes, the production volumes and file systems are disabled. The following actions are started:

- Unmount
- Remove devices
- Remove logical volumes
- Vary off the volume group
- Export volume groups.

User response:

None.

IDS1135I FlashCopying the target to the source volumes...

Explanation:

This message is displayed during the FlashCopy restore process to the production volumes.

User response:

None.

IDS1136I The parameter *parameter_name* was not specified in the profile.

Explanation:

The specified parameter was not found in the .fcs profile. However, this does not impact the program, and processing continues with the default value. If the parameter is FLASHCOPY_TYPE, the default value is used as the FLASHCOPY_TYPE.

User response:

Add the specified parameter to the profile if necessary.

IDS1137I The option ’-C *copy_type* determines the copy type. The parameter FLASHCOPY_TYPE was not specified in the profile.

Explanation:

The argument of the command line option -C specifies the FlashCopy type that should be used. It overrides the default value of the parameter FLASHCOPY_TYPE.

User response:

None.

IDS1138E The parameter HARDWARE_ID_LVM_MIRROR for the target set ’target_set_id’ is set in the .fct-file ’file_name’, but the production logical volumes are not mirrored.

Explanation:

The HARDWARE_ID_LVM_MIRROR parameter should only used in an LVM mirror environment.

User response:

If you want to use this feature you need to mirror the production logical volumes on source volumes residing on different hardware units. Otherwise, remove the parameter HARDWARE_ID_LVM_MIRROR parameter from the .fct file.

IDS1142I The progress status indicator (PSI) is already PSI_WITHDRAW_DONE.

Explanation:

A rerun of the ’withdraw’ function detects that the progress status of the specified (option -n) or last FlashCopy backup is already PSI_WITHDRAW_DONE.

User response:

If for some reason the status PSI_WITHDRAW_DONE is not in sync with the status of the source/target relationships, the ’withdraw_force’ function can be used.

IDS1143E **The function withdraw_force requires src/tgt pairs to be specified in the .fct file ’file_name’. The matching list of src/tgt volumes could not be set.**

Explanation:

In contrast to the normal ’withdraw’ function, where the source/target volumes are taken from the local repository, the ’withdraw_force’ function needs to get this information from the .fct file. The reason for that is that the ’withdraw’ function removes the matching list from the local repository, because a restore after a withdraw is not allowed.

User response:

Check the .fct file.

IDS1147I **Reconciling the local snapshot directory with the storage system....**

Explanation:

In the case of N Series, Tivoli Storage Manager for ACS checks that, for each snapshot kept in its Local Snapshot Manager, a valid snapshot exists on the N Series storage system.

User response:

None.

IDS1148I **Deleting the snapshot ’snap id’ of the volumes in the data container ’dc id’**

Explanation:

The specified snapshot is deleted.

User response:

None.

IDS1149E **The snapshot on the storage subsystem SAN N Series requires you to freeze the file systems.**

Explanation:

The parameters LVM_FREEZE_THAW and TARGET_DATABASE_SUSPEND are set in a combination that at the end the file system will be not frozen, however snapshots on SAN N Series requires you to freeze the file systems.

User response:

Check the interdependency between the two parameters LVM_FREEZE_THAW and TARGET_DATABASE_SUSPEND and ensure that they are set up in a way that the file systems will then be frozen.

IDS1174E **The option -b ’backup ID’ or -b ’backup sequence number’ must be specified.**

Explanation:

The call of splitint with the function -f flashback requires a backup sequence number (also called backup cycle number) or timestamp that is a unique identifier for the backup to be restored. With this identifier Data Protection for Snapshot Devices will find the volumes target set containing the disk backup to be restored.

User response:

Normally the calling program must determine one valid backup ID or backup sequence number to be passed. Check for preceding errors.

IDS1175E **The backup ID or the backup sequence number ’identifier’ was not found.**

Explanation:

Data Protection for Snapshot Devices did not find any entry in the IDSSAVE for the specified backup ID or backup sequence number.

User response:

Normally the calling program must determine one valid backup ID or backup sequence number to be passed. Check for preceding errors.

IDS1176I **The target set ’target_number’ does not contain a valid snapshot backup. (backup ID ’identifier’).**

Explanation:

This message can be displayed when Tivoli Storage Manager for ERP calls Data Protection for Snapshot Devices to inquire about disk backups on the target sets. The target sets are numbered, starting with 1.

User response:

None.

IDS1177E **The snapshot run ’backup sequence number’ was not a valid disk backup.**

Explanation:

To do a snapshot restore, a valid disk backup must exist on one of the target sets. The backup status indicator (BSI) must have the value BSI_DISKONLY or BSI_DISKANDTAPE.

User response:

Check the backup status indicator (BSI) of the target volumes calling the tsm4acs executable file: tsm4acs -p ’initSID.fcs’ -f ts_inquire -n ’target set ID’

IDS1178E The backup status indicator (BSI) for the FlashCopy run ’backup sequence number’ is not valid.

Explanation:

The backup status indicator can accept one of the following values in the IDSSAVE:

- BSI_START: a disk backup as background copy was started and is still running
- BSI_TAPEONLY: only a backup on TSM is available
- BSI_DISKONLY: only a backup on disk is available
- BSI_DISKANDTAPE: both disk and TSM backups are available
- BSI_INVALID: invalid entry for disk backup

Any other value is not allowed and makes the backup cycle unusable.

User response:

Check the backup status indicator (BSI) of IDSSAVE calling the tsm4acs executable file with the option -f inquire : tsm4acs -p ’initSID.fcs’ -f inquire -b ’backup sequence number’ Check for preceding errors.

IDS1179E The backup status indicator (BSI) for target set ’number’ is not valid.

Explanation:

The backup status indicator can accept one of the following values for one specific target set:

- BSI_START: a disk backup as background copy was started and is still running
- BSI_TAPEONLY: only a backup on TSM is available
- BSI_DISKONLY: only a backup on disk is available
- BSI_DISKANDTAPE: both disk and TSM backups are available
- BSI_INVALID: invalid entry for disk backup

Any other value is not allowed and makes the backup cycle unusable.

User response:

Check the backup status indicator (BSI) of the target volumes calling the tsm4acs executable file with the option -f ts_inquire (target set inquire): tsm4acs -p ’initSID.fcs’ -f ts_inquire -n ’target set ID’ Check for preceding errors.

IDS1180E The snapshot run ’backup sequence number’ is a valid disk backup.

Explanation:

Data Protection for Snapshot Devices has found that the selected backup to be restored has a valid disk backup with an entry in the IDSSAVE.

User response:

None.

IDS1181E The snapshot run ’backup sequence number’ is not the last backup of target set ’number’

Explanation:

The specified backup sequence number cannot be used for snapshot restore because on the target volumes a newer snapshot-type run was already entered.

User response:

Check the backup status indicator (BSI) of the target volumes calling the tsm4acs executable file with the option -f ts_inquire (target set inquire): tsm4acs -p ’initSID.fcs’ -f ts_inquire -n ’target set ID’ Select another backup Id for snapshot restore.

IDS1182E No target set ID could be assigned to the backup run *backup_sequence_number*

Explanation:

During a FlashCopy backup, TSM for Advanced Copy Services tries to find a target set (data container) that matches the source data container to satisfy the FlashCopy backup. It can be a target set in the state AVAILABLE or the state IN_USE (in which case it is re-used). A matching target data container could not be found, however.

User response:

See the rules for selecting one of multiple target data containers. For example, this message is displayed if you are trying to start a FlashCopy backup of type ’INCR’ and all the target sets are being used for the FlashCopy type ’COPY’. Also make sure that the target volumes are available to the backup system and the syntax is correct for the following parameters:

- TARGET_VOLUME
- COPYSERVICES_PRIMARY_SERVERNAME
- COPYSERVICES_USERNAME

IDS1183I A disk-only backup (option -d) was invoked, forcing the parameter ’FLASHCOPY_TYPE’ of the .fcs-file to ’COPY’

Explanation:

If you specified a disk-only backup via the parameter -d and the parameter ’FLASHCOPY_TYPE’ of the .fcs file has the value of NOCOPY, Data Protection for Snapshot Devices sets the value to COPY.

User response:

None.

IDS1184I Checking the backup status on Tivoli Storage Manager and on disk...

Explanation:

This message is displayed by Data Protection for Snapshot Devices during the inquiry of the backups on Tivoli Storage Manager and on disk.

User response:

None.

IDS1185I Reading the SAP backup log ’<PATH>/back<SID>.log’...

Explanation:

This message is displayed by Data Protection for Snapshot Devices while reading the backup of the SAP system ID <SID>.

User response:

None.

IDS1186E The parameter ’param’ in the profile <.sap file name> or the environment variable ’env_var’ is required.

Explanation:

This error is issued by Data Protection for Snapshot Devices if the specified parameter of the .sap file passed by the option -p could not be read.

User response:

Check that the passed .sap file is a valid profile for the SAP environment.

IDS1189E The option ’-C *copy_type*’ overrides the value *value* of the parameter FLASHCOPY_TYPE in the profile.

Explanation:

The value of the copy type parameter in the option -C *copy_type*, if specified in the command line, overrides the value found in the Data Protection for Snapshot Devices profile (.fcs)

User response:

None.

IDS1190E The information of the source/target volumes could not be found.

Explanation:

The executable file ’splitint’ is started automatically as a daemon (sometimes referred as the background monitoring process) to monitor the background copy. An attempt to obtain the status of the copy process has failed.

User response:

Check the error log file `splitint_[p|b]_runagent_jjjjmmddHHMMSS.log` in the directory specified in the parameter LOG_TRACE_DIR of the .fcs file. Check the availability of the storage system using the applicable tool (STORWATCH Specialist, DS Storage Manager, or SVC console).

Check the parameters in the .fcs file:
- COPYSERVICES_PRIMARY_SERVERNAME
- COPYSERVICES_SERVERPORT
- COPYSERVICES_USERNAME

Also verify the availability of the CIM agent and its connection to the storage system as described in the storage-system documentation.

IDS1191I The target volumes set ’number’ does not contain a valid disk backup.

Explanation:

This informational message is displayed during the call of the function get_disk_backups of Data Protection for Snapshot Devices (which is issued by the calling UI backint or Data Protection for Snapshot Devices) if one of the target sets contains an invalid disk backup.

User response:

None.

IDS1192I No disk backups were found on the target volumes.

Explanation:

This informational message is displayed during the call of the function get_disk_backups of Data Protection for Snapshot Devices (which is issued by the calling UI backint or Data Protection for Snapshot Devices) if none of the target sets contains a valid backup.

User response:

Select a backup from Tivoli Storage Manager.

IDS1193I The snapshot run with backup ID ’id’ was of type NOCOPY.

Explanation:

This informational message is displayed during the call of the function get_disk_backups of Data Protection for Snapshot Devices (which is issued by the calling UI backint or Data Protection for Snapshot Devices) if one of the target sets contains a snapshot backup of type NOCOPY.

User response:

None.

IDS1194I **The snapshot run ’backup_sequence_number’ has a backup status indicator (BSI) of ’status’ and is therefore not valid for snapshot restore.**

Explanation:

This informational message is displayed during the call of the function get_disk_backups of Data Protection for Snapshot Devices (which is issued by the calling UI backint or Data Protection for Snapshot Devices).

The values of the backup status (BSI) BSI_DISKONLY and BSI_DISKANDTAPE are valid values for a snapshot restore. The values BSI_START and BSI_TAPEONLY could be valid values at a later point in time. Any other value is invalid.

User response:

None.

IDS1196E **The list of files to be restored does not exist for the specified backup ID ’identifier’**

Explanation:

A FlashCopy disk backup can only be restored in coordination with Tivoli Storage Manager for ERP. At restore time, Data Protection for Snapshot Devices has to know about the corresponding list that was passed at backup time.

User response:

Check that you have the version of Tivoli Storage Manager for ERP that supports snapshot restore. Otherwise, restore from Tivoli Storage Manager.

IDS1197I **The list of files to be restored does not exist for the snapshot run ’backup_cycle_number’.**"

Explanation:

This informational message is displayed during the call of the function get_disk_backups of Data Protection for Snapshot Devices (which is issued by the calling UI backint or Data Protection for Snapshot Devices) if the list of files was not found for one of the target sets.

User response:

None.

IDS1200E **The exception ’CIdsException’ was thrown. Reason: <reason text>**

Explanation:

At present, the only reason text is: Not enough memory space. Allocation error in file <file name>, line <line number>.

User response:

Ensure that db2<sid> and the root user have the right setting for memory allocation. The output of ulimit shows these values. Check the SAP documentation for the respective release installed. Perform the following steps as recommended by SAP:

Checking Created Users
Check, as root, all existing users. To do this:

1. Enter the command smitty.
2. Select: Security & Users .Users .Change/Show Characteristics of a User
3. Press F4 to get a list of users.
4. For user root and each created user <user>:
   a. Select <user>.
   b. Change field Soft CPU time to -1 (this is the default value).
   c. Change field Soft CORE file size to 2097151 (this is the default value).
   d. Change field Soft FILE size to 4194302.
   e. Change field Soft DATA segment to -1.
   f. Change field Soft STACK size to -1.

You must make sure that the system-wide default HARD values are not explicitly defined to be lower than the number indicated above. Check the file /etc/security/limits under the ’default:’ stanza. If they are not explicitly set, then the values are as shown in the table at the top of the file.

IDS1212W **One or more errors were found checking the FlashCopy relations.**

Explanation:

This message can appear during the snapshot restore if the check of the source/target relations ended with any error that originated in the storage subsystem. This check takes part before any resource is removed.

User response:

Examine the preceding message output.

IDS1257E **A LUN with the serial number ’serial_number’ was not found in the storage subsystem.**

Explanation:

For the storage systems SAN Volume Controller and N Series, the names of the volumes managed by the storage interface and the serial number on the host are different. Data Protection for Snapshot Devices creates a mapping list and converts from one to the other automatically. This serial number was now not found in the mapping list.

User response:

Check using an operating system command that the serial number exists and has a valid correspondence to a physical disk on the storage system.

IDS1300E Cannot read file: <filename>.

Explanation:

Data Protection for Snapshot Devices is unable to read the data file <filename>.

User response:

Check the access permissions of the affected file and try again.

IDS1301E Cannot write file: <filename>.

Explanation:

Data Protection for Snapshot Devices is unable to write to the data file filename. The affected files could be:
- <LOG_TRACE_DIR>/splitint_b_<date_time_stamp>.log
- <LOG_TRACE_DIR>/splitint_p_<date_time_stamp>.log
- <LOG_TRACE_DIR>/splitint_b_<date_time_stamp>.trace
- <LOG_TRACE_DIR>/splitint_p_<date_time_stamp>.trace
- <config_file>
- <ids_control_file>
- the field value EXCHANGE_FILE in a backup cycle record.

User response:

Check the access permissions of the affected file and try again.

IDS1302E The environment variable <env_var> must be set.

Explanation:

The environment variable <env_var> is required. The following environment variables must be set when running Data Protection for Snapshot Devices:
- DB2 instance directory: to the home directory of the DB2 user
- DB2INSTANCE: to the DB2 instance
- DB2DBDFT: to the DB2 default database

User response:

Set the missing environment variable and try again.

IDS1303E The environment variable <env_var> is not correct.

Explanation:

This error can occur when the environment variable is set but contains a non-existent directory path.

User response:

Check the value of the environment variable and try again.

IDS1304E File not found or not accessible: <filename>.

Explanation:

The file <filename> was not found or is not accessible to Data Protection for Snapshot Devices.

User response:

Check path, name and the permissions of the file and try again.

IDS1305E The effective user ID of the process could not be set to the user <userid>.

Explanation:

One of the following cases can cause this error:
- The access rights for `splitint` are not set to 4750. Because the s-bit is not set, Data Protection for Snapshot Devices cannot switch between the users ’db2<sid>’ and ’root’ during the execution of the program.
- The file system that `splitint` is installed in was mounted with the NOSUID option.

User response:
- Check the `splitint` file in the directory /usr/tivoli/tsm/acssap/db2/x.y.z, and set the access rights for `splitint` with `chmod 4750 splitint`. After the installation, the command `ls -l splitint....` outputs a line such as: `-rwsr-x--- 1 root dba 1918611 Apr 11 17:09 splitint` (This is what setup.sh would do if you had used it.)
- If the file system that `splitint` is installed in was mounted with the NOSUID option, mount the file system with SUID allowed.

IDS1306I Issuing command ’command_string’...

Explanation:

Data Protection for Snapshot Devices is running the specified system command with the parameter as shown.

User response:

None.

IDS1308W Warning: File <file name> still exists on the backup system.

Explanation:

Data Protection for Snapshot Devices checks at the start of the function flashcopy if any of the files passed in the file list still exist on the backup system. If so, this warning is issued. Normally, none of the files should exist because the withdraw function, which should run before the FlashCopy, unmounts the files systems, varies them offline, exports the volume groups, and removes the devices.

User response:

Always run the function withdraw before starting the FlashCopy again.

IDS1310W The free space in the file system containing the directory ’path’ is only ’amount’ MB.

Explanation:

The existing free space of the file systems containing the following directories is checked:
- The database home directory and
- The directory specified by the parameter LOG_TRACE_DIR in the .fcs file and
- The directory containing the idssave file specified by the parameter IDS_CONTROL_FILE in the .fcs file.

Data Protection for Snapshot Devices warns you if the free space of these file systems falls below 50 MB. If it is under 5 MB an error is issued and the program fails, throwing an exception.

User response:

Ensure that the free space on these file systems is large enough.

IDS1311W splitint requires free space of at least 5 MB in the file system containing the directory ’path’

Explanation:

If the free space of the checked file systems (see the explanation for IDS1310W) is under 5 MB this error message is issued and the program fails throwing an exception.

User response:

Ensure that the free space on the database file system is large enough.

IDS1318E Operating system error <error_no>: <message text>.

Explanation:

Data Protection for Snapshot Devices encountered an unexpected-message error during the execution of a system function. The corresponding operating system error and message text are displayed. The message appears, for example, as a result of
- An incorrect user ID on the parameter LOGON_HOST_PROD in the .fcs file
- An incorrect password given for the user ID on the parameter LOGON_HOST_PROD in the .fcs file
- An incorrect TCP/IP name on the parameter LOGON_HOST_PROD in the .fcs file (for example: connection timeout)
- A failure allocating memory using the function malloc, and the operating system cannot satisfy the request

User response:

Check the specified error message.

IDS1322I The file ’filename’ is locked, waiting one second and retrying.

Explanation:

Data Protection for Snapshot Devices saves control information for the FlashCopy process in an internal repository that consists of several files. Some of these files may need to be written concurrently by several processes. To ensure consistency, Data Protection for Snapshot Devices uses a lock mechanism.

User response:

None.

IDS1325I Check the messages above. Enter ’r[etry]’ to retry or any other key to stop the process.

Explanation:

This message is asking you to retry an operation that previously failed.

User response:

Check the specific message and decide whether to retry or stop the process. In the case of critical restore runs, it is recommended to retry the operation after the reason for the failure has been identified and remedied.

IDS1326E Password input file ’<input file>’ not found.

Explanation:

The input file specified by the -i <input file> option was not found.

User response:

Specify a valid filename with full path for the input file for the password/configure function.

IDS1327I Topic named ’<topic name>’ could not be found in the file ’<input file>’. The password of user ’<username>’ is not changed.

Explanation:

The input file specified by the -i <input file> option does not have the topic <topic name> specified. The user <username> is not changed. There are two topic names (DBUSER, CSUSER). If none of these topics are found in the <input file>, then no password is changed.

User response:

None.

IDS1328W Parameter named ′<parameter name>′ could not be found in the file ′<input file>′. The password of user ′<username>′ is not changed.

Explanation:

The input file specified by the -i <input file> option does not have a valid format. The parameter <parameter name> is not found in it. The password of the user <username> is not changed.

User response:

Check for the valid format of the <input file>. Parameter <parameter name> is required in the topics DBUSER and CSUSER.

IDS1329I The password of user ′<username>′ is changed.

Explanation:

The input file specified by the -i <input file> option has a valid format and the password of the user <username> of either the DBUSER or the CSUSER topic is changed.

User response:

None.

IDS1330E The file ′<diskmapper filename>′ could not be found. Check that the parameter DISKMAPPER_SCRIPT is specified as a fullyqualified path/filename.

Explanation:

The script <diskmapper filename> specified by the parameter DISKMAPPER_SCRIPT in the DP for Snapshot Devices profile is not valid.

User response:

Specify a valid filename with full path for the DISKMAPPER_SCRIPT parameter.

IDS1331E The file ′<filename>′ could not be found. Check that this file exists or that the symbolic link points to an existing file.

Explanation:

The file <filename> is not valid.

User response:

Check that the file <filename> exists or that the symbolic link points to an existing file.

IDS1332E The update of the IDS repository failed.

Explanation:

Data Protection for Snapshot Devices failed to update the backup or restore status indicator (BSI/RSI) during the monitoring of the background copy process.

User response:

Check the traces for details about this failure. One possible cause is a full file system.

IDS1400E The backup status on target set *targetSetID* **must be BSI_DISKONLY or BSI_DISKANDTAPE for re-use with incremental copy type.**

Explanation:

A FlashCopy backup of type INCR in a non-AIX LVM mirror environment will re-use the already existing target set with FlashCopy type INCR only if the background process is already finished.

User response:

Check the background process by starting the program splitint with the function ″inquire″ or ″ts_inquire″.

IDS1401E The target set *targetSetID* **does not match the source volumes.**

Explanation:

Data Protection for Snapshot Devices checks whether the target set for the FlashCopy backup contains a target volume for each source volume, located in the same hardware unit and with the same size.

User response:

Check the volume list of this target set and ensure that the volumes are in the same hardware unit and have the same size as the source.

IDS1402E A background copy process of type *CopyType* **is still running on target set** *targetSetID*

Explanation:

Data Protection for Snapshot Devices fails if a background copy is still running for the same logical FlashCopy group (see the documentation). However, any target set (state AVAILABLE) that does not yet belong to a logical FlashCopy group (state AVAILABLE) can be selected.

User response:

Check the backup status of the FlashCopy backups that may be running.

IDS1404I The target set with ID *targetSetID* is selected for this run.

Explanation:

Data Protection for Snapshot Devices use two procedures for the selection of a target set.

User response:

None.

IDS1405E No target set found to accept a backup of type ’copy_type’.

Explanation:

If all the target sets are being used with the same type of logical FlashCopy group (either INCR or COPY), you will not find a target set to make a FlashCopy with a different copy type.

User response:

To make a target set AVAILABLE, start the function withdraw on the specific target set using the option -n.

IDS1408E The copy type argument *copy_type* is not valid.

Explanation:

The argument (FLASHCOPY_TYPE) of the command line option -C <FLASHCOPY_TYPE> can have the following values: COPY, NOCOPY and INCR. Any other value is not valid. Furthermore, INCR is only valid for an SVC configuration with version 4.2.1 of the SVC master console.

User response:

Specify one valid value.

IDS1410E You cannot run a snapshot restore from target set *targetSetID* if the sources are involved in a relationship of type *copytype* with the target set *targetSetID*

Explanation:

Data Protection for Snapshot Devices exploits the feature ″Multiple Relationship FlashCopy″ of the storage system. This means that for Data Protection for Snapshot Devices the source set of volumes can participate in multiple snapshot relationships with several target sets of volumes. However, there are some limitations:

- A source can have up to 12 targets
- A target can only have one source
- A target cannot be a source at the same time

User response:

To start a snapshot restore (in reverse, from the target to the source volumes) you have to withdraw the relationship with the specified target set.

IDS1411E The intended FlashCopy type has a value of *copy_type*

Explanation:

Data Protection for Snapshot Devices has detected a discrepancy in the FlashCopy specification.

User response:

None.

IDS1413E An invalid value *copy_type* has been specified for the FlashCopy type in the profile ’.fcs file’.

Explanation:

The parameter FLASHCOPY_TYPE of the Data Protection for Snapshot Devices profile (.fcs file) can have the following values: COPY, NOCOPY and INCR. Any other value is not valid. INCR is only valid for an SVC configuration starting with version 4.2.1 of the SVC master console.

User response:

Specify one valid value.

IDS1418E The target set *targetSetID* is already using incremental FlashCopy.

Explanation:

Using the procedure of specific target set selection, it is not allowed to select more the one target set for incremental FlashCopy on the same storage device.

User response:

Re-use the same target set or withdraw the existing relationship.

IDS1436E The value of the parameter ’*parameter_name*’ in the device section of the profile is invalid.

Explanation:

This message is displayed when an invalid value is found for one of the parameters of the device section of the profile.

User response:

Change the value according to the values explained in the section “Parameters of the DP for Snapshot Devices Profile”.

IDS1441I Checking the FlashCopy relations, please wait...

Explanation:

Data Protection for Snapshot Devices is reading the source/target FlashCopy relations from the storage system.

User response:

None.

IDS1444E A background copy process on target set '*target-set_id*' is still running from the last restore.

Explanation:

During the start of a new snapshot backup, Data Protection for Snapshot Devices detected that the selected target set is still in use by a previous snapshot backup.

User response:

Wait until the background copy process is finished before starting a new backup with Data Protection for Snapshot Devices.

IDS1445E Parameter ID '*number*' is not a valid one in the exchange file '*file_name*' of the IDS Repository.

Explanation:

In reusing a target set for a snapshot backup, Data Protection for Snapshot Devices was not able the find the data of the preceding backup in the IDS Repository.

User response:

This error is not expected unless the data repository is corrupt. Collect the log, traces and the ACS repository and send them to IBM Tivoli support.

IDS1446E No entries were found for the field '*field_name*' in the exchange file '*file_name*' of the IDS repository.

Explanation:

This error is not expected unless the data repository is corrupt.

User response:

Collect the log, traces and the ACS repository and send them to IBM Tivoli support.

IDS1452E This version of Data Protection for Snapshot Devices has expired.

Explanation:

This is a test version that has expired.

User response:

Order a release version of Data Protection for Snapshot Devices or contact your IBM/Tivoli marketing representative.

IDS1453W This version of Data Protection for Snapshot Devices expires in 'number' days.

Explanation:

This is a test version with a time limit.

User response:

Order a release version of Data Protection for Snapshot Devices or contact your IBM/Tivoli marketing representative before the version expires.

IDS1454I * This copy is NOT FOR RESALE. *****

Explanation:

This version is not for resale.

User response:

None.

IDS1455E License file 'filename' does not exist.

Explanation:

The license file 'agentess.lic' was not found where expected.

User response:

Make sure that the 'agentess.lic' file is located in the same directory as the init<SID>.fcs profile.

IDS1456E Unable to access license file 'file name'

Explanation:

Unable to access license file.

User response:

Make sure the access permissions allow read/write access.

IDS1457E License file 'file name' contains invalid data/checksum.

Explanation:

The license file is invalid.

User response:

Make sure you have the right agentess.lic file installed.

IDS1458E This license does not allow use of LVM mirrors.

Explanation:

The use of DB2 ACS or Data Protection for Snapshot Devices in an LVM mirror environment requires the extended license of Data Protection for Snapshot Devices.

Starting with V5.5, the DB2 version of Data Protection for Snapshot Devices (DP for Snapshot Devices) is a licensed, functionally enhanced version of the DB2 Advanced Copy Services (DB2 ACS) product initially provided with DB2 Enterprise V9.5. Conversely, DB2 Advanced Copy Services can be regarded as a functionally restricted version of Data Protection for Snapshot Devices.

User response:

Contact IBM Tivoli support to acquire the required license.

IDS1459E This license does not allow to use JFS file systems.

Explanation:

During a snapshot backup run, Data Protection for Snapshot Devices detected that at least one file system is of type JFS. Because JFS file systems need to be verified on the offload system by the Data Protection for Snapshot Devices device agent running with the -force mount- (-F) option, the Data Protection for Snapshot Devices product must be installed and licensed. The current snapshot backup run is deleted.

User response:

Install and license Data Protection for Snapshot Devices or change all file systems to type JFS2 and restart the snapshot backup.

IDS1460E You cannot freeze file systems of type JFS.

Explanation:

This message may indicate, for example, that profile parameter LVM_FREEZE_THAW is set to YES but at least one of the file systems involved is a JFS file system. The freeze/thaw feature is only available for JFS2 file systems. It is used to suspend all I/O on the file systems while taking a snapshot of them. JFS file systems do not support the freeze/thaw feature. Therefore, the parameter LVM_FREEZE_THAW is not allowed to be YES if any JFS file systems are used.

User response:

There are two options to resolve this problem:

1. If you need to use JFS file systems, you must explicitly set the profile parameter LVM_FREEZE_THAW to NO in the CLIENT section of the profile.
2. Move the data from the JFS file systems to JFS2 file systems. The profile parameter LVM_FREEZE_THAW can then be set to YES.

IDS1520E The FlashCopy agent can only be started if the last FlashCopy run was of type COPY or INCR.

Explanation:

Data Protection for Snapshot Devices automatically starts a daemon called the background monitoring process (FlashCopy agent) to monitor the background copy, provided the parameter FLASHCOPY_TYPE of the .fcs file was set to COPY or INCR.

User response:

Normally, the calling program controls this process. Check for preceding errors.

IDS1531E Timestamp ’string’ cannot be converted.

Explanation:

The status of the background copy is written by the background monitoring process daemon to a file named `fc_exchange.'bseq_number'` in the directory that contains the IDSAVE specified by the parameter IDS_CONTROL_FILE.

The file `fc_exchange.'bseq_number'` has, for each volume pair, the entry ’volume_pair: target source size state YYYY-MM-DD-HH.MM.SS YYYY-MM-DD-HH.MM.SS rate’, where:
- target is the serial number of the target volume
- source is the serial number of the source volume
- state can be ’active’ if the background copy is running or ’ none’ if the background copy is finished
- YYYY-MM-DD-HH.MM.SS represents approximate times for the start and end of the background process (in seconds since 00:00:00 GMT, January 1, 1970, which is the time standard the operating system uses)
- rate is the transfer rate within the storage system

To calculate the transfer rate some conversion is needed. When doing this conversion, an error occurred. The rate value is invalid.

User response:

Check the date and time setting of the machine.

IDS1540I Start of the FlashCopy agent on .the backup system.

Explanation:

Data Protection for Snapshot Devices automatically starts a daemon (called the FlashCopy agent) to monitor the background copy after the start of a FlashCopy backup of type COPY or INCR on the backup system.

User response:

None.

IDS1541I Removing the FlashCopy agent on the backup system.

Explanation:

Data Protection for Snapshot Devices automatically stops the FlashCopy agent daemon after the background copy has finished on the backup system.

User response:

None.

IDS1545I Start of the FlashCopy agent on the production system

Explanation:

Data Protection for Snapshot Devices automatically starts a daemon (called the FlashCopy agent or background monitoring process) to monitor the background copy after the start of a snapshot restore on the production system.

User response:

None.

IDS1546I Removing the FlashCopy agent on the production system.

Explanation:

Data Protection for Snapshot Devices automatically stops the FlashCopy agent daemon after the background copy has finished the restore on the production system.

User response:

None.

IDS1550E The FlashCopy agent could not be added to /etc/inittab.

Explanation:

Data Protection for Snapshot Devices automatically starts a daemon (called the FlashCopy agent) to monitor the background copy after the start of a FlashCopy backup of type COPY or INCR on the backup system and after the start of the snapshot restore on the production system. An entry in `/etc/inittab` allows the daemon to be started periodically. However, Data Protection for Snapshot Devices was unable to add an entry to /etc/inittab.

User response:

Check the rights of the Data Protection for Snapshot Devices executable file (splitint or tsm4acs).

IDS1551W The FlashCopy agent already exists in /etc/inittab.

Explanation:

Data Protection for Snapshot Devices automatically starts a daemon (called the FlashCopy agent) to monitor the background copy after the start of a FlashCopy backup of type COPY or INCR on the backup system and after the start of the snapshot restore on the production system. An entry in /etc/inittab allows the daemon to be started periodically. In an attempt to add such an entry, Data Protection for Snapshot Devices detected that an entry already existed.

User response:

None.

IDS1552E The FlashCopy agent could not be removed from /etc/inittab.

Explanation:

Data Protection for Snapshot Devices automatically stops the FlashCopy agent daemon after the background copy has finished on the backup system or, in the case of snapshot restore, on the production system. The entry in /etc/inittab is removed. However, Data Protection for Snapshot Devices was unable to remove the entry.

User response:

Check the rights of the Data Protection for Snapshot Devices executable file (splitint or tsm4acs).

IDS1553W The FlashCopy agent has already been removed from /etc/inittab.

Explanation:

Data Protection for Snapshot Devices automatically stops the FlashCopy agent daemon after the background copy has finished on the backup system or, in the case of snapshot restore, on the production system. The entry in /etc/inittab is removed. However, Data Protection for Snapshot Devices detected that the entry no longer exists in the table.

User response:

None.

IDS1602I Waiting for SyncPoint 'number' on all DPF nodes...

Explanation:

Data Protection for Snapshot Devices is waiting for all running tsm4acs processes to reach the specified SyncPoint.

User response:

None.

IDS1603E Timeout of ’number’ seconds on waiting for SyncPoint ’number’ on all DPF nodes reached.

Explanation:

While Data Protection for Snapshot Devices is waiting for all running tsm4acs processes to reach the specified SyncPoint, a time out condition occurs. This error can have the following reasons:

1. The Data Protection for Snapshot Devices parameter DB2_DPF_SYNCTIMEOUT is set too low. Check the Data Protection for Snapshot Devices parameter DB2_DPF_SYNCTIMEOUT in the Data Protection for Snapshot Devices configuration file.
2. Data Protection for Snapshot Devices is not started for each production server.
3. One or more Data Protection for Snapshot Devices processes running for the production servers were terminated.

User response:

1. Check the Data Protection for Snapshot Devices parameter DB2_DPF_SYNCTIMEOUT in the Data Protection for Snapshot Devices configuration file.
2. Check that Data Protection for Snapshot Devices is running on the backup system for all production servers.
3. Check for error messages in the Data Protection for Snapshot Devices log files for each process.

IDS1605I The last socket synchronization is still active.

Explanation:

The last Data Protection for Snapshot Devices socket synchronization was not stopped.

User response:

None.

IDS1606E Socket synchronization could not be started.

Explanation:

The last Data Protection for Snapshot Devices socket synchronization was not stopped. Data Protection for Snapshot Devices failed in trying to stop and restart the socket synchronization.

User response:

Restart the socket server on the production server that holds the DPF coordination partition. Use the function ’stopsocket’. After stopping the socket server, it is automatically restarted because of the entry in the `/etc/inittab` file.

IDS1607I Socket server was not running.

Explanation:

`tsm4acs` was called with function `stopsocket` to stop the socket server, but the socket server was not running.

User response:

None.

IDS1610E Invalid user name or password.

Explanation:

While `tsm4acs` is sending a socket request from the socket client to the socket server, the user and the encrypted password are checked on the socket server. Either the user or the password (or both) sent to the socket server are incorrect.

User response:

If the password for the user db2<sid> or the Copy Services user ID is changed, the socket server has to be restarted. The password for the users has to be changed by calling the `tsm4acs` function ’configure’.

IDS1620E The TCPIP service port ’number’ could not be found in /etc/services.

Explanation:

This error occurs, if the TCP/IP port for the socket server communication is not configured in the file `/etc/services`.

User response:

Make sure, that the socket service configuration is done by calling `tsm4acs` with function ’configure’ on the production system and that the backup system is configured with the script setupDB2BS. If the DB2 DPF configuration is changed (for example, a new DPF partition is added), you have to reconfigure the socket server.

IDS6901I Response to Init request.

Explanation:

This message indicates the progress of the flow within the device agent.

User response:

None.

IDS6902I Response to Partition request.

Explanation:

This message indicates the progress of the flow within the device agent.

User response:

None.

IDS6903I Response to Prepare Flash request.

Explanation:

This message indicates the progress of the flow within the device agent.

User response:

None.

IDS6904I Response to Restore request.

Explanation:

This message indicates the progress of the flow within the device agent.

User response:

None.

IDS6905I Response to Flash request.

Explanation:

This message indicates the progress of the flow within the device agent.

User response:

None.

IDS6906I Response to Verify request.

Explanation:

This message indicates the progress of the flow within the device agent.

User response:

None.

IDS6907I Response to Complete Restore request.

Explanation:

This message indicates the progress of the flow within the device agent.

User response:

None.

IDS6908I Response to Expiration request.

Explanation:

This message indicates the progress of the flow within the device agent.

User response:

None.

IDS6909I Response to Monitor request.

Explanation:

This message indicates the progress of the flow within the device agent.

User response:

None.

IDS6910E Could not set user ID to *number***. Error** *error_code - error_text*

Explanation:

The user ID could not be changed as required. This might be due to a missing s-bit for the executable file, indicating that the components were not set up correctly.

User response:

Check whether the installation process set the s-bit for the executable file in question. If it is missing, consult the user documentation for the appropriate installation and setup procedures.

IDS6911E The effective user ID *number1* **of the process could not be set to the user** *number2***. Error** *error_code - error_text* **. Check that the device agent executable file has the s-bit set.**

Explanation:

The effective user ID could not be changed as required. This might be due to a missing s-bit for the executable file, indicating that the components were not set up correctly.

User response:

Check whether the installation process set the s-bit for the executable file in question. If it is missing, consult the user documentation for the appropriate installation and set-up procedures.

IDS6912E Background operation shutting down in order to give precedence to a concurrent operation.

Explanation:

A background operation is ending because some interactive operation using the same resources was started. Once the operation taking precedence has ended, the background operation is resumed.

User response:

None.

IDS6913E Wrong parameter provided with option <option>.

Explanation:

A program was called with an unsupported parameter value.

User response:

If the program was called from the command line or from a script, correct the call. Otherwise, contact your IBM support personnel.

IDS6914E Invalid option '-K' specified.

Explanation:

A program was called with an unsupported parameter value for the internal option '-K'.

User response:

If the program was called from the command line or from a script, correct the call. Otherwise, contact your IBM support representative.

IDS6915E Could not change directory to *path*

Explanation:

An executable file needs to change to the named working directory, however, changing to the directory did not succeed.

User response:

Make sure authorization is set correctly for the executable file to access the required path.

IDS6917E Failed to find volume group for file: *path*

Explanation:

The file named could not be located. Its file system or volume group could not be determined.

User response:

Make sure that the database meets the requirement for snapshot backups. Make sure that the data is located on a file system under the control of the storage device.

IDS6918E Error when reading the correlation list or during the FlashCopy of the volume pairs.

Explanation:

A problem occurred either while reading the correlation list or while flashing the volume pairs.

User response:

Check the relations of the (source/target) volume pairs.

IDS6919E Failed to cancel the copy relationship of volume pairs: rc= *return_code*

Explanation:

Withdrawing the copy relations of the determined volume pairs failed.

User response:

Check the log and trace files for details.

IDS6920E After 'withdraw done' was finished the update of the IDS repository failed: rc=*return_code*

Explanation:

The IDS repository could not be updated.

User response:

Check the log and trace files for details.

IDS6921E Failed to monitor the FlashCopy.

Explanation:

The task for monitoring the progress of the background copy process of the volume pairs failed.

User response:

Check the log and trace files for details.

IDS6922E Failed to allocate memory.

Explanation:

Not enough memory was available to continue processing.

User response:

Ensure that the system has sufficient real and virtual memory. Close unnecessary applications.

IDS6923I *Object_name* **control object already initialized.**

Explanation:

The internal control object is already initialized and is used for the following process flow.

User response:

None.

IDS6924E Failed to initialize *object_name* control object.

Explanation:

The internal control object could not be initialized.

User response:

Check the log and trace files for details.

IDS6925E Function call '*function_name*' failed.

Explanation:

A call to the named internal function failed.

User response:

Check the log and trace files for details.

IDS6926I Adding '*path*' to the Disk Mapper input list.

Explanation:

The named file is added to the Disk Mapper input list.

User response:

None.

IDS6927E Failed to find N Series volume for file '*path*'. Error: *error_information*

Explanation:

The matching N Series volume for a specified file could not be found due to an error.

User response:

Check the log and trace files for details.

IDS6928E File system not found. Failed to find NFS mount point for file: '*path*'

Explanation:

The file system base for a mount point of a specified file could not be found.

User response:

Check the log and trace files for details.

IDS6929E Not a file system of type NFS. Failed to find N Series volume for file: '*path*'

Explanation:

The named file is not located on an NFS mounted file system.

User response:

Make sure that the database meets the requirement for snapshot backups. Make sure that the data is located on a file system under the control of the N Series storage device.

IDS6930E Volume information missing. Failed to find N Series volume for file: '*path*'

Explanation:

The volume information could not be collected for the named file.

User response:

Check the log and trace files for details.

IDS6931E Function call '*function_name*' failed. Error: *error_information*

Explanation:

A call to an internal function failed due to the specified error.

User response:

Check the log and trace files for details.

IDS6932E Function call ' *function_name* ' failed with rc=*return_code* **. Error:** *error_information*

Explanation:

A call to an internal function failed with the specified return code due to the stated error.

User response:

Check the log and trace files for details.

IDS6933I Volume '*volume_id*', snap ID = *snapshot_id*

Explanation:

The snap ID is associated with the specified volume.

User response:

None.

IDS6934I The snapshot '*snapid*' was generated for the source volume '*volname*'

Explanation:

A snapshot with the name displayed was taken from this volume. In a SAN environment, this message appears for each LUN thhat is involved in the snapshot process. However, when several LUNs belong to the same volume, only one snapshot of this volume is taken.

User response:

None.

IDS6935I Unmounting '*mount_point*'

Explanation:

Unmounting the specified mount point.

User response:

None.

IDS6936E Failed to unmount '*mount_point*'

Explanation:

Failed to unmount the specified mount point.

User response:

Check the log and trace files for details.

IDS6937I Mounting '*mount_point*'

Explanation:

Mounting the specified mount point.

User response:

None.

IDS6938E Failed to mount '*mount_point*'

Explanation:

Failed to mount the specified mount point.

User response:

Check the log and trace files for details.

IDS6939I Prepare for snap restore, volume '*volume_id*', snap ID = *snapshot_id*

Explanation:

Preparation for a snap restore of the specified volume with the associated snap ID is being performed.

User response:

None.

IDS6940I Prepare flash of group 'group_id'

Explanation:

Preparation for a snapshot copy of a group of the specified volumes is being performed.

User response:

None.

IDS6941I *Parameters_of_storage_device*

Explanation:

A list of storage device parameters.

User response:

None.

IDS6942E The storage device '*number*' is not handled by this device agent.

Explanation:

The specified storage device cannot be handled with this device agent.

User response:

Contact your IBM support.

IDS6943I Hardware version installed: version_information

Explanation:

The specified version of the installed hardware is indicated.

User response:

None.

IDS6944I NLS and tracing are already initialized.

Explanation:

The logging and tracing facilities are already initialized and are used further internally.

User response:

None.

IDS6945I File system '*path*' was already unmounted.

Explanation:

The specified file system was already unmounted.

User response:

None.

IDS6946E The environment variable 'ODMDIR' is not specified. Verify that the DB2 registry parameter DB2ENVLIST contains the value 'ODMDIR'. To set the DB2ENVLIST issue the command: db2set -i <DB2 instance name> DB2ENVLIST='<current envlist> ODMDIR'

Explanation:

The environment variable 'ODMDIR' must set in the user's environment where the snapshot backup or restore is started. In general, this is the case for default operating system installations.

User response:

Check the trace files where the runtime environment is written. If an entry for the ODMDIR environment variable cannot be found, set it manually as described in the message text.

IDS6947E File system '*mount_point*' is already mounted.

Explanation:

During the call of the function mount, Data Protection for Snapshot Devices found that the specified file system is already mounted on the backup system.

User response:

IDS6950W The output file '*path*' is not valid.

Explanation:

The device agent's log file could not be created. The messages will be logged to STDOUT as well as to the acsd log file.

User response:

Check the permissions of the directories and that there is enough free space in the file system. Check the acsd log and trace files for details.

IDS6951E Version mismatch error. Check setup (*version-information*).

Explanation:

The versions of acsd and the device agent are different.

User response:

Check the log and trace files for details. If the problem cannot be resolved, contact your IBM support.

IDS6952E Error in connection to DB2 ACS management agent.

Explanation:

The DB2 ACS management agent (acsd) could not be reached from within the device agent.

User response:

Check the log and trace files for details.

IDS6953E Error while parsing *path* script. The keyword '*keyword* ' is not supported during *function_name*

Explanation:

The script could not be parsed successfully due to an incorrect keyword for the given action.

User response:

Check the indicated script.

IDS6954E Error while parsing script. The keyword '*keyword*' is not supported.

Explanation:

The script could not be parsed successfully due to an incorrect keyword.

User response:

Check the indicated keyword.

IDS6955E To define a data container, '#GROUP <gid>' needs to be preceded by '#CREATE <cid>'.

Explanation:

The #CREATE clause must be specified before specifying a #GROUP clause.

User response:

Correct the appropriate script.

IDS6956E Error replacing standard input.

Explanation:

The standard input could not be replaced.

User response:

Check the log and trace files for details.

IDS6957E Script has continued without waiting.

Explanation:

The script should wait before continuing execution.

User response:

Check the log and trace files for details.

IDS6958I Output from script:

Explanation:

The output of the script.

User response:

None.

IDS6959I Script '*path*' returned with code *return_code*

Explanation:

The indicated script returned with the specified return code.

User response:

None.

IDS6960E **Non-zero return code from script '*path*'**

Explanation:

The script returned with a non-zero return code, which could indicate a warning or an error.

User response:

Check the log and trace files for details.

IDS6961E **Specify a script for removing data.**

Explanation:

To remove data, you must specify a script.

User response:

Create and specify an appropriate script.

IDS6962I **Response to File System Service request (*request*).**

Explanation:

A file system service request (*request*) is handled by the device agent and a response message is sent back to the management agent.

User response:

None.

IDS6964I **Number of volumes to be processed by snapshot: '*number*'.**

Explanation:

The number of volumes to be processed by FlashCopy.

User response:

None.

IDS6965I **Snapshot started...**

Explanation:

The command with the 'flashcopy' function has been issued on the production system, and the program `splitint` waits until this action has finished.

User response:

None.

IDS6966I **Snapshot successful**

Explanation:

The command for the snapshot-based copy of the volume pairs has completed successfully on the production system.

User response:

None.

IDSI696I **Performing snapshot of the source volume '*volname*'.**

Explanation:

A snapshot is taken of this volume. This message appears for each LUN that is involved in the snapshot process. However, when several LUNs belong to the same volume, only one snapshot of this volume is taken.

User response:

None.

Appendix G. Accessibility features for Tivoli Storage Manager

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features of Tivoli Storage Manager are described in this topic.

Accessibility features

The following list includes the major accessibility features in Tivoli Storage Manager:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices
- User documentation provided in HTML and PDF format. Descriptive text is provided for all documentation images.

The Tivoli Storage Manager Information Center, and its related publications, are accessibility-enabled.

Keyboard navigation

The Tivoli Storage Manager for Windows Console follows Microsoft conventions for all keyboard navigation and access. Drag and Drop support is managed using the Microsoft Windows Accessibility option known as MouseKeys. For more information about MouseKeys and other Windows accessibility options, please refer to the Windows Online Help (keyword: MouseKeys).

Tivoli Storage Manager follows AIX operating system conventions for keyboard navigation and access.

Tivoli Storage Manager follows HP-UX operating-system conventions for keyboard navigation and access.

Tivoli Storage Manager follows Linux operating-system conventions for keyboard navigation and access.

Tivoli Storage Manager follows Sun Solaris operating-system conventions for keyboard navigation and access.

Vendor software

Tivoli Storage Manager includes certain vendor software that is not covered under the IBM license agreement. IBM makes no representation about the accessibility features of these products. Contact the vendor for the accessibility information about its products.

Related accessibility information

You can view the publications for Tivoli Storage Manager in Adobe® Portable Document Format (PDF) using the Adobe Acrobat Reader. You can access these or any of the other documentation PDFs at the IBM Publications Center at http://www.ibm.com/shop/publications/order/.

IBM and accessibility

For more information about the commitment that IBM has to accessibility, see the IBM Human Ability and Accessibility Center at http://www.ibm.com/able.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Glossary

This glossary defines terms specific to Tivoli Storage Manager for Advanced Copy Services.

A comprehensive glossary for Tivoli Storage Manager is located in the Tivoli Storage Manager Version 6.1 information center: http://publib.boulder.ibm.com/infocenter/tsminfo/v6.

To view glossaries for other IBM products, go to http://www.ibm.com/software/globalization/terminology/.

acsd The name of the executable file for the DB2 ACS Management Agent.

Administration Assistant
A Web-browser-based graphical interface to support and assist the customization of Tivoli Storage Manager for ERP (System Configuration) and the analysis of SAP database backup and restore operations (Operations Monitor, Performance Monitor).

administrative client
A program that runs on a file server, workstation, or mainframe. This program lets administrators monitor and control Tivoli Storage Manager servers using Tivoli Storage Manager administrator commands. See also backup-archive client.

administrator (TSM)
A user who is registered to the server as an administrator. Administrators can be assigned one or more privilege classes. Administrators can use the administrative client to enter Tivoli Storage Manager server commands and queries according to their privileges.

Application Client
The component of Data Protection for Snapshot Devices that is responsible for communicating with the Management Agent. In the case of DB2, the client is implemented as a separate library (see snapshot backup library).

BackOM
See Backup Object Manager (BackOM).

backup
A function permitting users to copy one or more files to another location, such as a snapshot target set or TSM storage pool, in order to protect against data loss. See also restore.

backup-archive client
A component of Tivoli Storage Manager that runs on a workstation or file server and provides a means for Tivoli Storage Manager users to back up, archive, restore, and retrieve files to or from the TSM server. See also administrative client.
.

Backup Object Manager (BackOM)
A utility provided with Tivoli Storage Manager for Enterprise Resource Planning for backing up databases and for querying, creating, restoring, and deleting backup objects on the TSM server.

backup system
The secondary server environment that performs backup procedures.

backup usability state
An attribute assigned to a snapshot backup to indicate a specific status of the backup with respect to a particular function.

BRARCHIVE

1. An SAP database utility to perform backups of offline redo log files in an SAP Oracle database environment.

2. An SAP DB2 administration tools utility to perform backups of offline log files in an SAP DB2 database environment.

BRBACKUP
An SAP database utility to perform online or offline backups of SAP Oracle databases. BRBACKUP can be used to back up data files, control files and online redo log files.

BRCONNECT
An SAP database utility that ensures that the database status required for the online or offline backup of an SAP Oracle

database remains unchanged during the backup. BRCONNECT is started internally by BRBACKUP and BRARCHIVE

BRRESTORE

1. An SAP database utility to restore an entire Oracle database backup or parts of it, previously backed up with BRBACKUP or BRARCHIVE. Any non-database files and directories that were saved can also be restored. Subdirectories within the sapdata directories are created automatically, if necessary.

2. An SAP DB2 Administration Tools utility to perform a restore of previously backed up offline log files in an SAP DB2 database environment.

BR*Tools
Utilities provided by SAP to simplify the administration of a database system within an SAP environment.

central scheduling
A function permitting an administrator to schedule backup and archive operations from a central location. The operations can be scheduled on a periodic basis or on an explicit date.

client A program running on a file server, PC, workstation, or terminal that requests services of another program called the server. See also server and host.

client options file
A configuration file of the TSM client containing a set of processing options that identify the server, communication method, and options for backup, archive, hierarchical storage management, and scheduling. Its default name is dsm.opt on UNIX or Linux systems and `<servername>.opt` on Windows.

client-server
A communications network architecture in which one or more programs (clients) request computing or data services from another program (the server).

client system options file
A configuration file of the TSM client on UNIX or Linux systems, containing a set of processing options that identify the Tivoli Storage Manager servers to be contacted for services. This file also specifies communication methods and options for backup, archive, hierarchical storage management, and scheduling. Its name is dsm.sys.

clone With respect to N Series, a point-in-time, unsynchronized, independent copy of a source element. Clones are generated on request from an internal snapshot. They are equivalent to target volumes for FlashCopy devices. Copies of type ″clone″ are associated with FlashCopy types COPY, NOCOPY, and INCR.

cluster
A collection of servers that provide a set of resources to a client.

Command Line Processor (CLP)
A character based interface of DB2 for entering SQL statements and database manager commands (for example, backup or restore).

Common Information Model (CIM)
An implementation-neutral, object-oriented schema for describing network management information. The Distributed Management Task Force (DMTF) develops and maintains CIM specifications.

concurrent copy
A Copy Services function that produces a backup copy and allows concurrent access to data during the copy.

consistency group
An association of SVC virtual disks that are treated as a unit for FlashCopy backup and restore purposes.

consistent copy
A copy of a data entity (for example, a logical volume) that contains the entire data entity at a single instant in time.

Control Center
A graphical interface of DB2 that shows database objects (such as databases and tables) and their relationship to each other. The Control Center allows administrative tasks (for example database backup) provided by the DBA utility to be performed and provides visual explanation and performance monitor tools.

control file
A file associated with a database that

maintains the physical structure and time stamps of all files within that database. The control file is updated continuously during database use and must be available for writing, if the database is mounted or opened.

Copy Services
An optional feature of the IBM ESS and DS storage systems that provides replication and mirroring.

Database Partitioning Feature (DPF)
A feature that can be used to improve the management of a large database by dividing it into multiple database partitions that are physically placed on one or more servers.

data container
Alternative term for a set of source or target volumes.

data file
A physical operating system file on disk containing data structures of a database, such as tables and indexes. A data file belongs to a specific tablespace in a database.

Data Protection (DP)
A storage management software application that performs backup and recovery functions across a wide variety of client and server platforms.

Data Protection for ESS (DP for ESS)
Former name of the current product up to and including version 5.3.0.

destructive restore
A restore that renders other backups invalid due to their chronological relationships.

device agent
A Data Protection for Snapshot Devices software component that communicates with the operating system and the hardware device to perform the file system and snapshot operations.

Distributed Management Task Force (DMTF)
The group responsible for developing the Common Information Model (CIM). See also Common Information Model (CIM).

DPF See Data Partitioning Feature.

fast restore
A synonym for snapshot restore or FlashCopy restore. See also snapshot restore and FlashCopy.

File Manager
See Tivoli Storage Manager for Enterprise Resource Planning File Manager.

FlashCopy
A Copy Services function that can quickly provide an image copy from a source location to a target location.

freeze The function of disabling access to a file system for the duration of a point-in-time copy.

hdisk A logical disk volume on an AIX platform.

host A computer that is connected to a network and provides an access point to that network. The host can be a client, a server, or both a client and a server simultaneously. See also client and server.

Incremental Change Recording (ICR)
A facility of the ESS and DS storage systems and the SAN Volume Controller that records changes (at the track level) and copies only these tracks to the target volumes.

Incremental FlashCopy
A mode of FlashCopy for the ESS and DS storage systems and the SAN Volume Controller in which changes are recorded at the track level and only these tracks are copied to the target volumes.

input/output (I/O)
Pertaining to a device, process, channel, or communication path involved in data input, data output, or both.

I/O group
A set of two SVC nodes defined by the configuration process. Each SVC node is associated with one I/O group. The nodes in the I/O group provide access to the vDisks in the group. See also virtual disk.

Licensed Internal Code (LIC)
Microcode that IBM does not sell as part of a machine but licenses to the customer. LIC is implemented in a part of storage that is not addressable by user programs. Some IBM products use it to implement functions as an alternative to hard-wired circuitry.

local area network (LAN)
A variable-size communications network placed in one location. A LAN connects servers, PCs, workstations, a network operating system, access methods, and communications software and links.

Local Snapshot Manager (LSM)
The Local Snapshot Manager (LSM) is a generic component of Tivoli Storage Manager that is responsible for managing any data containers. For Data Protection for Snapshot Devices, it is the LUN manager that administers a *universe of LUNs* grouped into target sets (also referred to as data containers) in a local repository and tracks the state of the backups contained in them. The key functions of LSM include not only the identification of a target set in the state AVAILABLE, which can therefore accept a new FlashCopy backup, but also the decision as to when to re-use a target set in the state IN_USE. The local backup is referred to in generic terms as a snapshot backup. In the context of Data Protection for Snapshot Devices, it is referred to as a FlashCopy backup.

logical unit number (LUN)
A volume identifier number for a storage subsystem logical disk drive.

logical volume
The storage medium associated with a logical disk drive. A logical volume is typically located on one or more storage devices. A logical volume is referred to on an AIX platform as an *hdisk*, an AIX term for storage space. A host system sees a logical volume as a physical volume.

management agent
The software component in Data Protection for Snapshot Devices and DB2 ACS that controls the snapshot backup repository and performs support functions such as the profile wizard.

master console (SVC)
See SVC master console

Media Management API
An interface provided by Oracle to which vendors are able to write compatible software libraries. This software integrates with Oracle. Thus, an Oracle server process is able to issue commands to the media manager to write backup files out to sequential storage (for example, Tivoli Storage Manager) and read files from sequential storage.

mirroring
The process of writing the same data to multiple disks at the same time. The mirroring of data protects it against data loss within the database or within the recovery log.

negative list
(SAP term) A list of files that are explicitly permitted to be backed up, although they would normally not be included.

Network Appliance, Inc. (NetApp)
The vendor of the embedded technology within an N Series device that supports snapshot functions.

Network File System (NFS)
A facility in UNIX and Linux systems for accessing files on a remote system.

node

1. An individual server in an SVC cluster on which the SVC software runs.
2. In TSM, a unique name that is used to identify a Tivoli Storage Manager client to the TSM server.
3. In SMP, a single machine in a Symmetrical Multiprocessor (SMP) environment.

See also partition.

node name
A unique name used to identify a workstation, file server, or PC to the server.

null trust provider mode
A communication mode of the CIM Agent in which the CIM Agent does not verify that the certificate passed by the client matches a known certificate. Rather, it accepts any certificate from the client (including a null string for the filename). To enable this mode, the value of COPYSERVICES_CERTIFICATEFILE must be set to NO_CERTIFICATE, which is the default setting. However, it is recommended to use this mode only if the production and backup systems, as well as the storage system, are protected by a firewall.

offline log file
A log file that is no longer needed by the

DB database for rollback or crash recovery. However, it may be required for a roll-forward recovery. DB2 may call the userexit to copy an offline log file to the log_archive path.

offline redo log
If the database is in ARCHIVELOG mode and an online redo log is filled, it is copied to one (or more) archive log destinations, which is typically the saparch directory in an SAP environment. This copy is the offline redo log (also called archived redo log).

Offload Agent (tsm4acs)
The component of DP for Snapshot Devices that is responsible for sending a snapshot backup to TSM for tape backup.

online redo log
The online redo log is a set of two or more files that record all changes made to Oracle data files and control files.

online active log file
The log file that is currently being used by DB2 to log transactions. It is needed for rollback operations and crash recovery.

online retained log file
A DB2 log file that is no longer being used to log transactions, but contains transactions with data pages that have not yet been written from the buffer pool to disk. The DB2 logging user exit is called by DB2 (if configured) to copy a filled or closed online retained log file to the log_archive directory. Online retained log files may be deleted or reused by DB2 if they are no longer needed because all referenced transactions are committed and all changed pages have been written to disk, and the userexit has successfully copied them to the log_archive directory.

options file
A file that contains processing options.

partition
In DB2, a part of a database that consists of its own data, indexes, configuration files, and transaction logs. A database partition is sometimes called a node or a database node.

path A connection between a Tivoli Storage Manager node and a Tivoli Storage Manager server interface. On the client side, a path is defined by a logical server name listed in the client option file dsm.sys (UNIX or Linux systems) or `<servername>.opt` (Windows systems). On the server side, the possible paths are defined by the network addresses of the Tivoli Storage Manager server.

Pegasus
An open-source implementation of the DMTF CIM and WBEM standards. It is designed to be portable and highly modular. It is coded in C++ so that it effectively translates the object concepts of the CIM objects into a programming model but still retains the speed and efficiency of a compiled language. Pegasus is designed to be inherently portable and builds and runs today on most versions of UNIX, Linux, and Microsoft Windows.

production system
The active production environment that remains online during Data Protection for Snapshot Devices backup processing.

progress state
An attribute assigned to a snapshot backup indicating what point in the processing the backup has attained.

ProLE The background process (UNIX or Linux) or service (Windows) that controls backup and restore operations of Tivoli Storage Manager for Enterprise Resource Planning.

quorum disk
In an SVC environment, a disk that serves as a tie-breaker if exactly half the nodes in a cluster fail at the same time or the cluster is divided so that exactly half the nodes in the cluster cannot communicate with the other half.

Recovery Manager (RMAN)
A tool that is used to back up, restore and recover Oracle databases. It can be used with or without a Recovery Catalog, If a Recovery Catalog is not used, Recovery Manager decides how to back up, restore and recover the database using the control file of the database. Incremental backups of Oracle databases can only be done with RMAN.

recovery history file
A recovery history file is created with

each DB2 database and is automatically updated, for example, whenever one of the following operations is performed:

- Backup of a database or tablespace
- Restore of a database or tablespace
- Rollforward of a database or tablespace
- Alter of a tablespace
- Load of a table
- Drop of a table
- Reorganization of a table
- Update of table statistics

Every DB2 backup operation includes a copy of the recovery history file.

replica
A synonym for target volume.

restore
A function that permits users to copy a version of a backup file from snapshot media or the TSM storage pool to a workstation or file server. The backup copy on the snapshot media or in the TSM storage pool is not affected. See also backup.

retention
The amount of time, in days, that inactive files that have been backed up or archived to a TSM server are kept by the backup server before they are deleted. Copy group attributes and default retention grace periods for the domain define retention.

SAN Volume Controller (SVC, also SAN VC)
A virtualization layer that allows addressing a heterogeneous configuration of IBM and non-IBM open-system storage devices through one interface to an open-systems host.

SAP BACKINT interface
An interface that is provided by BR*Tools utilities that can be used to access external backup programs, for example, Tivoli Storage Manager for Enterprise Resource Planning or Data Protection for Snapshot Devices.

SAP Note
A document that contains service information provided by SAP. SAP Notes can be accessed (with an SAP user ID and password) at the SAP Service Marketplace: http://service.sap.com/notes

SCSI address
The hexadecimal value that defines a physical I/O device on a SCSI channel path. A SCSI address consists of a target ID and a logical unit number (LUN).

server
A program running on a mainframe, workstation, or file server that provides shared services such as backup and archive to other various (often remote) programs (called clients).

shared library
In DB2, the shared library (UNIX) or dynamic link library (DLL, Windows) implementing the vendor API of DB2 for backup and restore solutions. Tivoli Storage Manager for Enterprise Resource Planning functionality is partly implemented as a shared library.

SID
A unique identifier for a system defined within the database configuration.

sid
The lowercase version of SID.

snapshot
Generically, a point-in-time disk copy. In N Series, an internal structure representing a copy of a data entity at a particular point in time.

snapshot backup library
A dynamically loadable library that implements the Application Client component of Data Protection for Snapshot Devices for the DB2 environment.

snapshot backup repository
The set of data describing snapshot backups taken using Data Protection for Snapshot Devices or DB2 ACS

snapshot restore
A restore analogous to a snapshot backup, in which the target volumes (copies) are copied back to the source volumes.

stale partition
In AIX LVM mirroring, a physical partition (that belongs to a logical partition and, in turn, a logical volume) that could not be updated at some point and is therefore different from the other mirror copies of that partition.

storage area network (SAN)
A high-speed special-purpose network (or subnetwork) that interconnects different kinds of data storage devices with

associated data servers on behalf of a larger network of users.

Subsystem Device Driver (SDD)
A pseudo device driver that resides in the host server with the native disk device driver for the storage system. It uses redundant connections between the host server and disk storage to provide enhanced performance and data availability. These connections comprise many different components through which data flows during input and output processes. Redundancy and the ability to switch between these components provides different paths for the data to travel. In the event of failure in one input-output path (such as a cable or controller failure), the SDD automatically switches to another input-output path. I/O operations sent to the Subsystem Device Driver are passed to the AIX disk driver after path selection.

SVC master console
The platform on which the software runs that is used to manage the SAN Volume Controller. It includes a Web interface and the CIM Agent for SVC.

table space
A logical unit of storage in a database. In DB2 Database for Linux, UNIX, and Windows, a table space is a collection of containers, and the data, index, long field, and LOB portions of a table can be stored in the same table space or in separate table spaces. See also table space container.

table space container
A generic term for an allocation of space to a table space. Depending on the table space type, the container can be a directory, device, or file.

table space definition information (TDI)
Data describing the physical layout of a database required by the Backup Object Manager redirected restore function. The data includes information about all the table spaces and their associated table space containers. The TDI can be created at the end of a full database backup.

target set
The target volumes that are copied from a set of source volumes that are subjected to a FlashCopy backup.

TDI See table space definition information.

thaw The function to enable access to a file system that was frozen prior to performing a point-in-time copy.

Tivoli Data Protection (TDP)
The former name of the various software components currently designated as Data Protection within Tivoli Storage Manager.

Tivoli Storage Manager (TSM)
A client/server product that provides storage management and data access services in a heterogeneous environment. Tivoli Storage Manager supports various communication methods, provides administrative facilities to manage the backup and storage of files, and provides facilities for scheduling backups.

Tivoli Storage Manager API
A set of functions that applications running on a client platform can call to store, query, and retrieve objects from Tivoli Storage Manager storage.

Tivoli Storage Manager for Enterprise Resource Planning (TSM for ERP)
The interface program between Tivoli Storage Manager and Data Protection for Snapshot Devices in an SAP environment.

Tivoli Storage Manager for Enterprise Resource Planning configuration file
A binary file that contains persistent information used by Tivoli Storage Manager for Enterprise Resource Planning, such as the TSM client password or the current backup version number. Its default file name is init.<SID>.bki.

Tivoli Storage Manager for Enterprise Resource Planning File Manager
A utility that simplifies the Tivoli Storage Manager for Enterprise Resource Planning inquire, restore and delete operations. It can be seen as an add-on to Tivoli Storage Manager for Enterprise Resource Planning.

Tivoli Storage Manager for Enterprise Resource Planning profile
An ASCII file that contains option keywords for configuring Tivoli Storage Manager for Enterprise Resource Planning. Its default file name is init.<SID>.utl.

usability state
See backup usability state.

user exit
The DB2 database manager can call a user exit program to store and retrieve log files and manage the location of archived log files, if the database configuration parameter ’userexit’ is activated. Using a user exit program to archive and retrieve log files enables the database for roll-forward recovery.

util_file_online
A (data file) backup using an external backup program addressed by the BACKINT interface. If an online backup is running, the backup status is set and completed dynamically for the table spaces that are being backed up. Thus, the volume of offline redo log files during an online backup can be reduced significantly.

validate
In Tivoli Storage Manager, the process of ensuring that the active policy set contains a default management class and reports on copy group definition errors.

vendor API
An interface provided by DB2 to which vendors are able to write compatible software libraries, which should be shared libraries. Thus, the DB2 process is able to issue commands to the Vendor API to write backup data to sequential storage (for example, Tivoli Storage Manager) and read files from sequential storage.

vendor environment file
A file that is used to communicate environment settings to DB2 to be passed on to the shared library. The name of the vendor environment file is passed to DB2 as a parameter of the DB2 ’backup database’ and ’restore database’ commands.

virtual disk (vDisk)
An SVC device that appears to host systems attached to the SAN as a SCSI disk. Each vDisk is associated with one I/O group.

volume

1. A general term referring to a single device visible to the host. For an SVC configuration, it is used in this document synonymously with virtual disk.
2. The basic unit of storage for the Tivoli Storage Manager database, recovery log, and storage pools. A volume can be an LVM logical volume, a standard file system file, a tape cartridge, or an optical cartridge. Each volume is identified by a unique volume identifier.

volume copy
(SAP term) A snapshot-based copy procedure.

withdraw
A storage system function that dissolves the relationship of source and target volumes initiated by a FlashCopy function.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at ″Copyright and trademark information″ at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

SAP, SAP NetWeaver, and mySAP are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Index

A

accessibility features 363
acscim 6, 141
acsd 6, 138
acsnnas 6, 143
acsnsan 6, 143
acsora
  default location 105
acsxiv 145
AIX
  information sources xvi
augmentation of Tivoli Storage Manager for ERP functions 5

B

background monitoring (FlashCopy) 215
backup
  backup status indicator (BSI) 217
  cycles 213
  methods 33
  monitoring progress 34
  multiple generations on disk 37
  partial 120
  progress status indicator (PSI) 216
  restore of snapshot backups in busy state 125, 126
  restore status indicator (RSI) 218
  scheduling of 13
  snapshot backup with SVC 79
  starting 125
  to Tivoli Storage Manager server 119
  usability states 35
  using snapshot disks 34
  without snapshot disks 120
backup node 111, 113
backup overview 16
backup procedure
  fully automated backup 124
  manual backup 123
  strategy requirements 122
backup_dev_type 193
backup_type 193

C

CIM Agent for DS Open API
  installing 100
  introduction 30
CIM Agent for SAN Volume Controller
  installing 100
  introduction 31
commands 133
Common Information Model (CIM)
  components 96
  information sources xvi
  logs and traces 230
  SSL setup 97
commtimeout option 105
Concurrent I/O (CIO) 77
configuration file relationships 75
configuration files 159
control files
  password file 188
  profile 160
  target volumes file (.fct) 189
customer support
  contact xix

D

Data Protection for Oracle
  and RMAN 16
  configuring with Data Protection for Snapshot Devices 108
  options files
    setting values 112
  understanding 16
Data Protection for Snapshot Devices 136
  augmentation of Tivoli Storage Manager for Enterprise Resource Planning functions 12
  backup methods 33
  backup procedure
    strategy requirements 122
  backups without snapshot disks 120
  commands 133
  compared to DB2 ACS 3
  components shared with DB2 ACS 6
  configuration files 159
  configuring with Data Protection for Oracle 108
  enhanced functions 5, 10
  environment variables
    DSM_CONFIG 114
    DSM_DIR 114
    DSM_LOG 114
  fully automated backup 124
  functions 12, 13
  functions shared with DB2 Advanced Copy Services 4
  installation in console mode 93
  installation in silent mode 93
  installation requirements
    environment 89
    hardware 80
    LVM mirroring 90
    software 82
    volume groups 90
  installed files 105
  installing 61
  installing and customizing 66, 91
  installing on a new instance 95
  integrated Tivoli Storage Manager backup 11
  integrated TSM backup 5
  LVM 48
  manual backup 123
  manual setup 134
  messages 233
Data Protection for Snapshot Devices *(continued)*
  Offload Agent (tsm4acs) 154
  operating environment 8
  options files 221
    configuring multiple server stanzas 222
    configuring to same server 221
    setting values 110
  overview 1
  password file 188
  preparations for installing 67
  profile 160
  restore methods 43
  restore procedure
    Restore Method One (Entire Database) 130
    Restore Method Two (Datafile Only) 131
  RMAN backup script
    creating 115
    example 115
  server script
    editing 222
  setup script 134
  snapshot backups 34
  snapshot restore
    limitations 47
    procedure 128
  software environment 8, 15, 24
  starting backups automatically 125
  target volumes file 189
  understanding 3, 13
  uninstalling 100
  version/maintenance levels 61
database instances
  setup script 61
DB2
  backup history file 127
  information sources xvii
  installing Data Protection for Snapshot Devices on new instance 95
  LIST HISTORY command 127
  reference information xv
DB2 Advanced Copy Services
  compared to Data Protection for Snapshot Devices 3
  functions shared with Data Protection for Snapshot Devices 4
DB2 Advanced Copy Services (DB2 ACS)
  components shared with DP for Snapshot Devices 6
DB2 vendor options for DB2 Advanced Copy Services 136
definitions 367
device agent
  for CIM devices (acscim) 141
  for IBM XIV Storage System devices (acsxiv) 145
  for N Series devices (acsnsan, acsnnas) 143

Device Agent for CIM Devices (acscim) 6
Device Agent for N Series Devices (acsnnas, acsnsan) 6
disk layout
  installation 68, 70
  sample 203
Disk Mapper script 147
Disk Storage (DS) system
  description 25
  source/target volumes 116
DPF
  backup modes 120
dsierror.log 114
DSM_CONFIG
  setting 114
DSM_DIR
  setting 114
DSM_LOG
  and scheduler 122
  setting 114
dsm.opt
  and Data Protection for Oracle 112
  and Data Protection for Snapshot Devices 110
  example 221
  requirements 114
dsm.sys
  and Data Protection for Oracle 112
  and Data Protection for Snapshot Devices 110
  and management class 105
  example 221
  multiple server stanzas 114
  requirements 114
  two separate files 114
dsmerror.log 114, 122
DSMI_CONFIG
  setting 114
DSMI_DIR
  setting 114
DSMI_LOG
  setting 114

E

education
  see Tivoli technical training xviii
enhancements in v6.1 xxii
Enterprise Storage Server (ESS)
  description 25
  source/target volumes 116
environment
  installation requirements 89
environment variables
  DSM_CONFIG 114
  DSM_DIR 114
  DSM_LOG 114, 122
  DSMI_CONFIG 114
  DSMI_DIR 114
  DSMI_LOG 114
error messages 233
examples
  disk layout 199
  options files
    dsm.opt 221
    dsm.sys 221
examples *(continued)*
  RMAN backup script 115

F

file systems
  JFS and JFS2 76
files 114
  agent_hdw.lic 105
  dsierror.log 114
  dsm.opt 112
    and Data Protection for Snapshot Devices 110
  dsm.sys 112
    and Data Protection for Snapshot Devices 110
  dsmerror.log 114, 122
  installed by Data Protection for Snapshot Devices 105
  README 105
  serverscript.smp.oracle 105
  setupfile.smp.oracle 105
fixes, obtaining xix
FlashCopy
  overview 17
FlashCopy background monitoring 215
FlashCopy backup
  with LVM mirrors 49
fully automated backup 124
functions 5

G

glossary 367

H

HACMP 52
hardware
  installation requirements 80
help 226

I

IBM N Series storage system 78
IBM Software Support
  submitting a problem xxi
IBM storage systems
  information sources xvi
IBM Support Assistant xviii
IBM System Storage N Series 27
IBM Tivoli Storage Manager for Advanced Copy Services
  information sources xv
IBM Tivoli Storage Manager for Enterprise Resource Planning
  information sources xv
include option 105
include-exclude
  and management class 105
incremental backup and restore 5, 12
incremental feature 17
installation
  CIM Agent for DS Open API 100
installation *(continued)*
  CIM Agent for SAN Volume Controller 100
  CIM Client 98
  CIM Server (Pegasus) 98
  customization requirements 74
  Data Protection for Snapshot Devices 95
  Data Protection for Snapshot Devices in console mode 93
  Data Protection for Snapshot Devices in silent mode 93
  disk layout 68, 70
  NFS file systems 116
  of Data Protection for Snapshot Devices 61, 66, 91
  Open SSL 96
  prerequisite products 90
installation requirements
  environment 89
  hardware 80
  LVM mirroring 90
  software 82
  volume groups 90
Internet, search for problem resolution xviii
Internet, searching for problem resolution xix
IPv6 231

J

JFS file system 76
JFS2 file system 76

K

knowledge bases, searching xviii

L

license 105
Linux 8
log files 114
  CIM 230
  Data Protection for Snapshot Devices 228
  DB2 Advanced Copy Services 228
  dsierror.log 114
  dsmerror.log 114, 122
  storage system 229
  summary 225, 228
  Tivoli Storage Manager for ERP 230
Logical Volume Manager (LVM)
  advantages 48
  asymmetrical environments 53
  configuration 54
  functions 49
  requirements 80
  symmetrical environments 53
  utilizing for FlashCopy backup 48
logical volume names 76
LVM mirroring
  installation requirements 90

M

- Management Agent (acsd) 6
  - description 138
- management class
  - specifying 105
- manual backup 123
- maxnummp option 105
- mirror environment
  - target volumes file 57
- mount
  - function of tsm4acs 157
- multiple server stanzas
  - configuration procedure 222
  - discussed 114
- multiple target sets
  - in LVM mirrored environment 49

N

- N Series storage system
  - introduction 27
  - restore considerations 46
- network attached storage (NAS) 78
- NFS
  - considerations for N Series 78
  - setting up 116
- NOCOPY backup and restore 5, 12

O

- Offload Agent (tsm4acs) 6, 154
- Open SSL
  - installation 96
- options
  - commtimeout 106
  - include 105
  - maxnummp 105
  - passwordaccess 112
    - and Data Protection for Snapshot Devices 110
  - schedmode
    - and Data Protection for Snapshot Devices 110
  - servername 112
    - and Data Protection for Snapshot Devices 110
  - tcpserveraddress 112
    - and Data Protection for Snapshot Devices 110
- options files
  - configuring multiple server stanzas 222
  - configuring to same server 221
  - dsm.opt
    - requirements 114
  - dsm.sys
    - and management class 105
    - requirements 114
  - example
    - dsm.opt 221
    - dsm.sys 221
  - include-exclude 105
    - and management class 105
  - requirements 114
  - setting values 112
- options files *(continued)*
    - Data Protection for Snapshot Devices 110
- Oracle
  - information sources xvii

P

- password file 188
- passwordaccess option 110, 112
- Pegasus CIM Server
  - installing 98
- problem determination
  - describing problem for IBM Software Support xx
  - determining business impact for IBM Software Support xx
  - submitting a problem to IBM Software xxi
- production node 111, 113
- profile 160
  - overriding 163
  - parameter descriptions 164
  - structure 160
  - updating 164
- profile keywords 192
- progress status indicator (PSI) 216
- publications
  - download xii
  - order xii
  - search xii
  - Tivoli Storage Manager xii

R

- raw logical volumes 76
- README.TDPHDW.ORACLE 105
- registering workstations 105
- restore
  - backup status indicator (BSI) 217
  - cycles 213
  - methods 43
  - progress status indicator (PSI) 216
  - restore status indicator (RSI) 218
- restore overview 17
- restore procedure
  - Restore Method One (Entire Database) 130
  - Restore Method Two (Datafile Only) 131
  - snapshot restore
    - limitations 47
    - procedure 128
- restore status indicator (RSI) 218
- RMAN 16
- RMAN backup script
  - creating 115
  - example 115
- rman_parms 193

S

- samples
  - Data Protection for Snapshot Devices profile 200, 203, 205
  - disk layout 201, 203
- samples *(continued)*
  - target volumes files 205
- SAN Volume Controller
  - CIM Agent for SAN Volume Controller 100
  - sample target volume definitions 207
  - snapshot backup 79
- SAN Volume Controller (SVC)
  - description 26
  - source/target volumes 117
- SAP
  - Data Protection for Snapshot Devices 1
- SAP®
  - information sources xvii
- schedmode option 110
- scheduling
  - of backups 13
- SDD
  - restoring hdisks 223
- server script
  - definition 222
  - editing 222
- servername option 110, 112
- serverscript.smp.oracle 105
- setup_*.sh script 134
- setupfile.smp.oracle 105
- sharing target volumes 117
- snapshot backup
  - modes with DPF partitions 120
  - monitoring progress 34
  - usability states 35
- snapshot restore
  - backups in busy state 125, 126
  - limitations 47
  - overview 17
  - parameters required during backup 57
  - procedure 128
  - rerunning 45
  - with LVM mirrors 50
  - with N Series devices 46
- software
  - installation requirements 82
- Software Support
  - contact xix
  - describing problem for IBM Software Support xx
  - determining business impact for IBM Software Support xx
- SSL
  - certificate 97
  - configuring CIM environment 97
- storage system 24, 25
  - source/target volumes 116
- support information xviii

T

- tape_backup
  - function of tsm4acs 155
- target set selection 57
- target set states 34
- target volumes
  - sharing of 117

target volumes file
  in LVM mirrored environment 57, 58, 59
  sample 205
  structure and parameters 189
target_database_parameter_file 122
tcpserveraddress option 110, 112
Tivoli Storage Manager
  backup to Tivoli Storage Manager server 119
  information sources xiv, xxi
  management class
    example 105
    specifying 105
  registering workstations 105
  server 10
Tivoli technical training xviii
trace files
  CIM 230
  Data Protection for Snapshot Devices 228
  DB2 Advanced Copy Services 228
  storage system 229
  summary 225, 228
training, Tivoli technical xviii
troubleshooting 226
tsm4acs 6
  default location 105
  description 154
  mount function 157
  tape_backup function 155
  unmount function 158
two separate dsm.sys files 114

U
unmount
  function of tsm4acs 158
usability states (snapshot backups) 35
util_par_file 193
util_volr_access 193

V
vendor options for DB2 Advanced Copy Services commands 136
Volume Group Takeover script 147
volume groups
  installation requirements 90

X
XivAdapter.jar 147

Program Number: 5608-E10

Printed in USA

SC33-8331-00