

IBM Tivoli Storage FlashCopy Manager
Version 4.1.1

*Installation and User's Guide
for UNIX and Linux*



IBM Tivoli Storage FlashCopy Manager
Version 4.1.1

*Installation and User's Guide
for UNIX and Linux*



Note:

Before using this information and the product it supports, read the information in “Notices” on page 295.

Second edition (December 2014)

This edition applies to version 4, release 1, modification 1 of Tivoli Storage FlashCopy Manager for UNIX and Linux (product numbers 5608-W07, 5641-A06, and 5724-X94) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2001, 2014.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures	vii	Chapter 3. Installing and upgrading	39
Tables	ix	Installing on the production server	40
About this publication	xi	Installing separately on backup or clone servers	42
Who should read this publication	xii	Installing in silent mode	43
Publications	xii	Upgrading.	45
New for Tivoli Storage FlashCopy Manager Version 4.1.1	xiii	Migrating existing snapshot data	48
Chapter 1. Overview	1	Chapter 4. Configuring Tivoli Storage FlashCopy Manager	53
Protection in a DB2 pureScale HA environment.	2	Running the setup script for DB2	53
Backup and restore methods with FlashCopy and snapshots	2	Running the setup script for a DB2 pureScale environment	55
Database cloning	4	Configuring Tivoli Storage FlashCopy Manager for DB2	56
Software components	5	Running the setup script for Oracle	58
Chapter 2. Planning.	7	Configuring Tivoli Storage FlashCopy Manager for Oracle	59
IBM FlashCopy Manager Prerequisite Checker	7	Running the setup script for custom applications.	62
Capacity planning	8	Configuring Tivoli Storage FlashCopy Manager for custom applications	63
Required communication ports	9	Configuring storage environments.	65
Preparation for installation	10	Configuring the CIM adapter for SP 800-131A compliant encryption	65
Verify the DB2 system	10	Defining Logical Unit Numbers on DS8000 storage subsystems	66
Preparing the DB2 high-availability disaster recovery server or DB2 standby server	12	Defining virtual disks on SAN Volume Controller and Storwize family	67
Preparing DB2 in an SAP environment	13	Select the FLASHCOPY_TYPE	68
Preparing Oracle in an SAP environment	13	Target set definitions	69
Preparing Oracle systems (non-SAP, non-ASM)	14	LVM mirroring and ASM failure group environments.	72
Preparing Oracle Automatic Storage Management	15	Backup and clone server assignment	72
Preparing custom applications	18	Managing backups and clones with the DEVICE_CLASS parameter	74
Logical Volume Manager support (AIX only)	19	Configuring for remote mirroring	76
Preparing applications that run on VMware or KVM virtual machines.	20	Setting up the daemons on the production and backup systems	78
Checking the KVM setup.	21	Postinstallation and configuration	79
Preparing backup and cloning servers	21	Chapter 5. Backing up data	81
Determining the number of backup and clone servers in the environment	22	Backup commands for DB2 databases	81
Installation prerequisites for backup and clone servers	23	Backing up DB2 databases	82
Preparing a backup cluster in a DB2 pureScale environment	25	Serial and parallel backup modes for multi-partition DB2 database	82
Preparing backup or cloning servers for applications running on VMware or KVM virtual machines	26	Backing up DB2 to a Tivoli Storage Manager server	83
Storage solutions	26	Backup commands for DB2 in a pureScale environment	84
IBM XIV Storage System	26	Backing up DB2 (HADR) standby servers	84
IBM System Storage N series and NetApp storage systems	28	Backing up Oracle databases	86
SAN Volume Controller, DS8000, and Storwize family	29	Backing up an Oracle database to Tivoli Storage Manager server	86
Remote mirror integration	33	Backing up Oracle in an SAP environment databases	87
Reconciliation of backups.	36	Automate backups of Oracle in an SAP environment	93

Backing up file systems or custom applications	93
FlashCopy backup of individual mirrors.	94
Backing up data with remote mirroring	95
Usability states of snapshot backup operations	97

Chapter 6. Restoring data 103

Restoring DB2 databases	103
DB2 backup history file overview	105
Restoring Oracle databases	105
Restoring snapshots for Oracle databases	105
Restoring Oracle databases from Tivoli Storage Manager	106
Restoring Oracle in an SAP environment databases	108
Restoring file systems or custom applications.	108
Restoring data with remote mirroring	109

Chapter 7. Cloning databases 113

Tivoli Storage FlashCopy Manager cloning process	113
Cloning an Oracle Data Guard standby database	114
Database cloning preprocessing and postprocessing	115
Configuration files used for cloning	115

Chapter 8. Troubleshooting 119

General troubleshooting procedure	119
Logging and tracing files	120
Tivoli Storage FlashCopy Manager log and trace files	122
Storage system log and trace files	126
CIM log and trace files	126
GPFS log files	127
Tivoli Storage Manager for ERP log and trace files	127
Troubleshooting mirroring relationships	127
Troubleshooting storage solutions	128
Troubleshooting connectivity problems	130
Troubleshooting tips for Tivoli Storage FlashCopy Manager for Oracle	130
Guidelines for Oracle variables	132
Tivoli Storage FlashCopy Manager for Oracle miscellaneous errors	132
Internet Protocol Version 6 (IPv6) support	133

Appendix A. Configuration files 135

Profile overview	135
GLOBAL	140
ACSD	142
CLIENT	143
ORACLE	164
CLONING	165
DEVICE_CLASS <i>device</i>	171
OFFLOAD	187
DB2STANDBY	194
OFFLOAD_DB2STANDBY	198
Changing profile parameters	198
Interdependency of LVM_FREEZE_THAW and TARGET_DATABASE_SUSPEND	199
Target volumes	199
Managing target volumes by storage system	200
Target volume parameter settings (DS8000 configuration)	203

Target volume parameter settings for SAN Volume Controller configuration and Storwize family	204
Target set handling for cloning	205
Tivoli Storage FlashCopy Manager password file	207
BACKINT configuration file	207
IBM Global Security Kit configuration	216
Oracle in an SAP environment BR*Tools configuration profile (.sap)	218
Tivoli Storage Manager option files used by Data Protection for Oracle	220

Appendix B. Examples 223

Examples (DB2)	223
Example overall disk layout for a DB2 environment.	223
Example profile for Tivoli Storage FlashCopy Manager for DB2	224
Example profile for Tivoli Storage FlashCopy Manager for DB2 pureScale.	226
Examples (Oracle)	226
Example overall disk layout for a Oracle environment.	227
Example profile for Tivoli Storage FlashCopy Manager for Oracle	228
Example profile for Tivoli Storage FlashCopy Manager for Oracle with ASM.	229
Example of the RMAN backup script	230
Examples (SAP with Oracle)	230
Example overall disk layout for an Oracle in an SAP environment	230
Example profile for Tivoli Storage FlashCopy Manager for Oracle in an SAP environment (disk only)	231
Example profile for Tivoli Storage FlashCopy Manager for Oracle in an SAP environment (offload)	232
Example profile for Tivoli Storage FlashCopy Manager for Oracle in an SAP environment incremental (offload)	234
Example target volumes files	234
Example target volumes file DS8000 configuration	234
Example target volumes file (SAN Volume Controller configuration or Storwize family)	235
Example target volume file	237
Example profile for custom applications	238
Example profile for a DB2 HADR standby server environment.	239

Appendix C. Administrative commands 241

Configuration commands	241
Installation setup script	241
Installation setup script for DB2 pureScale.	243
Setup script values	245
Setting or changing passwords with the setup script	246
Password administration	247
GSKit commands	248

I	Query managed capacity	251
	Background daemons.	252
	Management agent: acsd	252
	Generic device agent: acsgen	254
	Mounting and unmounting snapshots on a secondary system	256
	Integration with Tivoli Storage Manager	259
	The fcmcli offload agent.	259

Appendix D. Backup, restore, cloning commands, and utilities. 265

	Commands for DB2 that use DB2 utilities	265
	fcmcli -f *_db2standby.	269
	Backup and restore commands for Oracle	273
	The acsora user interface for Oracle	273
	BR*TOOLS - User interface for Oracle in an SAP environment.	275
	acsutil Snapshot Object Manager for Oracle	277
	Backup and restore commands for custom applications	279
	Cloning commands	284
	Deleting Tivoli Storage FlashCopy Manager snapshot backups	289
	Snapshot backup status in the Tivoli Storage FlashCopy Manager repository	291

Appendix E. Accessibility features for the Tivoli Storage Manager product family. 293

Notices 295

	Trademarks	297
--	----------------------	-----

	Privacy policy considerations	297
--	---	-----

Glossary 299

A	299
B	301
C	302
D	303
E	305
F	306
G	306
H	307
I.	308
J.	308
K	308
L	309
M	310
N	311
O	312
P	312
Q	314
R	314
S	315
T	317
U	318
V	318
W	319

Index 321

Figures

1.	Tivoli Storage FlashCopy Manager backup and restore environment	3	11.	Usability states during snapshot restore	100
2.	Tivoli Storage FlashCopy Manager and database cloning	4	12.	Usability states during snapshot delete	100
3.	Tivoli Storage FlashCopy Manager system components	5	13.	Usability states during snapshot mount	101
4.	Protection of DB2 (HADR) standby nodes with IBM Tivoli Storage FlashCopy Manager . . .	12	14.	Usability states during snapshot offload	102
5.	Tivoli Storage FlashCopy Manager in an LVM environment	19	15.	Debugging workflow for SAP with Oracle Tivoli Storage FlashCopy Manager	121
6.	Remote mirroring using Metro Mirror and Global Mirror sources	36	16.	Debugging workflow for SAP with Oracle Tivoli Storage FlashCopy Manager with Tivoli Storage Manager	122
7.	Tivoli Storage FlashCopy Manager host assignments for DB2.	74	17.	SAP with Oracle, Tivoli Storage FlashCopy Manager with Tivoli Storage Manager	208
8.	The backup profiles on the production and backup systems	90	18.	Example overall disk layout for a DB2 environment	223
9.	Cross-site mirrored SAP database protected with Tivoli Storage FlashCopy Manager and Tivoli Storage Manager.	94	19.	Example overall disk layout for a Oracle environment	227
10.	Usability States during snapshot backup	99	20.	Example overall disk layout for an SAP with Oracle environment	230
			21.	Protection of DB2 HADR standby nodes with FlashCopy Manager for Custom Applications .	271

Tables

1.	Space requirements for a global product installation of Tivoli Storage FlashCopy Manager	8
2.	Tivoli Storage FlashCopy Manager for UNIX and Linux port numbers	9
3.	Selecting the FLASHCOPY_TYPE for DS8000, SAN Volume Controller, and Storwize family	68
4.	Supported storage subsystems and FlashCopy types.	69
5.	Summary of backup commands for DB2 databases	81
6.	Summary of backup commands for DB2 in a pureScale environment.	84
7.	Summary of Backup Commands for Oracle	86
8.	Files used during a manual backup	87
9.	Summary of backup commands (SAP with Oracle)	87
10.	Usability states	97
11.	Summary of Restore Commands for DB2	103
12.	Summary of Restore Commands for Native Oracle	105
13.	Summary of Restore Commands for Oracle in an SAP environment	108
14.	Message prefixes used in the summary log file	119
15.	Tivoli Storage FlashCopy Manager log files	122
16.	Tivoli Storage FlashCopy Manager trace files	123
17.	Tivoli Storage FlashCopy Manager return codes	123
18.	Tivoli Storage FlashCopy Manager installer exit codes.	124
19.	DB2 vendor reason codes	124
20.	Actions taken depending on values of LVM_FREEZE_THAW and TARGET_DATABASE_SUSPEND	199
21.	Managing target volume LUNs by storage system.	200
22.	Parameters of the 'VOLUMES_SET_x' Topic (DS8000)	203
23.	Parameters of the 'VOLUMES_SET_x' topic (SAN Volume Controller and Storwize family)	204
24.	Actions Taken Depending on Values of LVM_FREEZE_THAW and TARGET_DATABASE_SUSPEND	210
25.	Actions Taken Depending on Values of LVM_FREEZE_THAW and TARGET_DATABASE_SUSPEND	211
26.	Options for starting the management agent, acsd, as a daemon process	253
27.	Options for starting the generic device agent, acsgen	254
28.	Parameters for Oracle databases	274
29.	Parameters for Tivoli Storage FlashCopy Manager backint command.	276
30.	Options for the Tivoli Storage FlashCopy Manager fcmlcli command for custom applications	280

About this publication

This publication provides information about installing, configuring, administering, and using IBM® Tivoli® Storage FlashCopy® Manager for UNIX and Linux.

Tivoli Storage FlashCopy Manager for UNIX and Linux is provided as a single installation package that supports the following database applications, storage systems, and operating systems:

- One of these applications:
 - DB2®, DB2 pureScale®, or DB2 in an SAP environment
 - Oracle or Oracle in an SAP environment
 - Custom applications such as file systems or other than DB2 or Oracle databases
- One of these storage systems or file systems that are used for the application:
 - IBM System Storage® DS8000®
 - IBM System Storage SAN Volume Controller
 - IBM XIV® Storage System
 - IBM Storwize® family and IBM Storwize V7000 Unified
 - IBM System Storage N series
 - NetApp Storage Systems
 - IBM General Parallel File System (GPFS™) in combination with DB2 pureScale on any storage system
- One of these operating systems:
 - AIX®
 - Linux
 - Oracle Solaris
 - HP-UX

Tivoli Storage FlashCopy Manager performs online or offline backups of DB2, Oracle databases, or other applications that are on snapshot-oriented storage systems. Optionally, it performs backups to Tivoli Storage Manager storage by using IBM Tivoli Storage Manager for Enterprise Resource Planning, Tivoli Storage Manager for Databases, or Tivoli Storage Manager backup-archive client, as appropriate.

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 backup function of Tivoli Storage FlashCopy Manager is needed.

Who should read this publication

This publication is intended for system programmers and administrators who are responsible for implementing a backup and cloning solution in one of the supported environments.

The following list identifies hardware and software solutions and tasks that can be used with Tivoli Storage FlashCopy Manager. The information that is presented in this publication assumes that you have an understanding of the following solutions and topics, as applicable.

- Storage systems or file systems that are used for the database or custom application:
 - IBM System Storage DS8000
 - IBM System Storage SAN Volume Controller or IBM Storwize family
 - IBM XIV Storage System
 - IBM System Storage N series
 - NetApp systems
 - IBM General Parallel File System (GPFS)
- Oracle or DB2 database administration
- Tivoli Storage Manager

Publications

The Tivoli Storage Manager product family includes IBM Tivoli Storage FlashCopy Manager, IBM Tivoli Storage Manager for Space Management, IBM Tivoli Storage Manager for Databases, and several other storage management products from IBM Tivoli.

To view IBM product documentation, see <http://www.ibm.com/support/knowledgecenter/>.

New for Tivoli Storage FlashCopy Manager Version 4.1.1

New features and enhancements are available in Tivoli Storage FlashCopy Manager Version 4.1.1.

Cloning Oracle ASM databases

Clone Oracle ASM databases with Tivoli Storage FlashCopy Manager Version 4.1.1. Oracle ASM database clones can be created, refreshed, or deleted when you no longer need them.

For more information about ASM cloning, see “Preparing Oracle Automatic Storage Management” on page 15.

“IBM FlashCopy Manager Prerequisite Checker” on page 7

Use the IBM FlashCopy Prerequisite Checker to check whether your system meets all the required hardware, software, and operation system requirements that are needed to install and run Tivoli Storage FlashCopy Manager in a UNIX or Linux environment.

“Protection in a DB2 pureScale HA environment” on page 2

Tivoli Storage FlashCopy Manager supports DB2 pureScale High Availability (HA) in a DB2 cluster environment. When the setup script is run in a DB2 pureScale environment, the Tivoli Storage FlashCopy Manager is installed and configured in High Availability mode in the DB2 pureScale cluster. The instances in the pureScale cluster can be backed up and protected even if some members are offline. Scheduled and automatic backups can be run throughout the environment, or on a subset of hosts in the environment.

Tivoli Storage FlashCopy Manager password file

The master password is only prompted for in advanced mode, and is only needed when you are installing Tivoli Storage FlashCopy Manager separately on the backup servers or cloning servers without using SSH. In this case, you must know the password. The password is defined when you configure the production server; for backup and cloning servers this password must be used so that the servers can connect to the management agent on the production server. When you use SSH for remote deployment to the backup and cloning servers, the password file is copied to the servers automatically.

New and modified parameters or functions

The following parameters are new for Tivoli Storage FlashCopy Manager V4.1.1:

Oracle ASM Cloning

The existing parameter **VOLUME_MGR**, has a new setting of ASM to enable Oracle ASM cloning. For more information about parameters for ASM cloning, see “ASM cloning parameters and Tivoli Storage FlashCopy Manager” on page 17.

When you are configuring Tivoli Storage FlashCopy Manager V4.1.1, the following parameters can be edited in advanced mode only and default values are applied where applicable:

ACS_DIR

You can change **ACS_DIR** in advanced mode only. For more information about this parameter in the profile file, see “GLOBAL” on page 140.

ACSD You can change **ACSD** in advanced mode only. For more information about this parameter in the profile file, see “GLOBAL” on page 140.

ACS_REPOSITORY

You can change **ACS_REPOSITORY** in advanced mode only. For more information about this parameter in the profile file, see “ACSD” on page 142.

TARGET_DATABASE_SUSPEND

You can change **TARGET_DATABASE_SUSPEND** in advanced mode only. For more information about this parameter in the profile file, see “CLIENT” on page 143.

OVERWRITE_DATABASE_PARAMETER_FILE

You can change **OVERWRITE_DATABASE_PARAMETER_FILE** in advanced mode only. For more information about this parameter in the profile file, see “OFFLOAD” on page 187.

OVERWRITE_DATABASE_PARAMETER_FILE

You can change **OVERWRITE_DATABASE_PARAMETER_FILE** in advanced mode only. For more information about this parameter in the profile file, see “CLONING” on page 165.

STORAGE_SYSTEM_ID

You can change **STORAGE_SYSTEM_ID** in advanced mode only. For more information about this parameter in the profile file, see “DEVICE_CLASS *device*” on page 171.

COPYSERVICES_REMOTE

You can change **COPYSERVICES_REMOTE** in advanced mode only. For more information about this parameter in the profile file, see “DEVICE_CLASS *device*” on page 171.

COPYSERVICES_COMMPROTOCOL

You can change **COPYSERVICES_COMMPROTOCOL** in advanced mode only. For more information about this parameter in the profile file, see “DEVICE_CLASS *device*” on page 171.

When you are configuring Tivoli Storage FlashCopy Manager V4.1.1 for custom applications, the following CLIENT parameters can be edited in advanced mode only. For more information about configuring CLIENT parameters for custom applications, see “CLIENT parameters for custom applications” on page 158.

INFILE You can change **INFILE** in advanced mode only in the CLIENT section of the profile file.

PRE_FLASH_CMD

You can change **PRE_FLASH_CMD** in advanced mode only in the CLIENT section of the profile file.

POST_FLASH_CMD

You can change **POST_FLASH_CMD** in advanced mode only in the CLIENT section of the profile file.

The following parameters or functions are changed in Tivoli Storage FlashCopy Manager V4.1.1:

TARGET_SET in a DS8000 environment

TARGET_SET is preset to **VOLUMES_FILE**. If an older profile is loaded with a

| **TARGET_SET** value of **VOLUMES_DIR**, you are still prompted for the parameter
| **TARGET_SET**. When you are prompted, you can change the value to
| **VOLUMES_FILE** if appropriate.

| **used_capacity**

| The function **used_capacity** is renamed **managed_capacity**. Use the **fccli**
| **-f managed_capacity** command to list the source volumes that are
| protected by Tivoli Storage FlashCopy Manager for which a backup
| (FlashCopy or snapshot) was created. For information about how to run
| the command and the command syntax, see “Query managed capacity” on
| page 251.

| **Obsolete parameters**

| The following parameters or parameter options are deprecated in Tivoli Storage
| FlashCopy Manager V4.1.1.

| **VOLUMES_DIR for TARGET_SET**

| The **VOLUMES_DIR** option is deprecated in V4.1.1, and the wizard no longer
| shows it as a valid parameter. For older versions of the profile, the
| **VOLUMES_DIR** option is processed.

| **VOLUMES_DIR**

| The **VOLUMES_DIR** parameter is deprecated in V4.1.1, and the wizard no
| longer shows it as a valid parameter. For older versions of the profile, the
| **VOLUMES_DIR** parameter is processed.

Chapter 1. Overview

IBM Tivoli Storage FlashCopy Manager provides a method to back up and restore data by using the advanced snapshot technologies of storage systems.

Tivoli Storage FlashCopy Manager can back up DB2 databases, Oracle databases, or other applications that are on snapshot-oriented storage systems or file systems.

Tivoli Storage FlashCopy Manager backup operations are based on volume-level copy operations that are provided by the storage system. For GPFS in combination with DB2 pureScale, the backup operations are based on GPFS file sets. In this scenario, any storage solution that is supported by the GPFS file system can be used. Tivoli Storage FlashCopy Manager takes snapshots at a volume group or GPFS file set level for granular control.

When you use Tivoli Storage FlashCopy Manager with other Tivoli Storage Manager products, snapshots can be sent to the Tivoli Storage Manager server. Depending on the application, Tivoli Storage FlashCopy Manager can transfer snapshots by using IBM Tivoli Storage Manager for Enterprise Resource Planning, IBM Tivoli Storage Manager for Databases, or Tivoli Storage Manager backup-archive client. Tivoli Storage FlashCopy Manager uses Oracle RMAN Media Management API. Using RMAN maximizes the protection of Oracle data, and provides a comprehensive storage management solution. To send snapshot backups to Tivoli Storage Manager, you must configure a backup server or cluster.

The following list identifies the applications that can be protected and cloned with Tivoli Storage FlashCopy Manager.

- Protect the following database applications with Tivoli Storage FlashCopy Manager:
 - DB2, DB2 in an SAP environment, DB2 in a partitioned database environment, and DB2 pureScale environment. You can back up and restore data from single-partition databases, and logically or physically partitioned DB2 databases.
 - Oracle, Oracle with Automatic Storage Management (ASM), and Oracle in an SAP environment.
- Clone the following database applications with Tivoli Storage FlashCopy Manager:
 - DB2, DB2 in an SAP environment, DB2 with the Database Partitioning Feature included.
 - Oracle and Oracle in an SAP environment that is on a file system that is supported by Tivoli Storage FlashCopy Manager.
- Oracle with Automatic Storage Management (ASM)
- Back up and restore custom applications with Tivoli Storage FlashCopy Manager:
 - Any database application other than those database applications listed in the preceding list.
 - Any other applications that are on file systems that are supported by Tivoli Storage FlashCopy Manager.

Tivoli Storage FlashCopy Manager supports specific operating systems. All servers that have Tivoli Storage FlashCopy Manager installed must be at the same operating system release level. Certain high availability (HA) environments are supported.

The following list identifies the storage solutions or file systems that you can use with Tivoli Storage FlashCopy Manager software:

- IBM XIV Storage System
- IBM Storwize family
- IBM System Storage SAN Volume Controller
- IBM System Storage DS8000
- IBM System Storage N series
- NetApp Storage system
- GPFS file system in combination with DB2 pureScale

Protection in a DB2 pureScale HA environment

Tivoli Storage FlashCopy Manager in a DB2 pureScale environment provides high availability to Tivoli Storage FlashCopy Manager daemon processes.

In a DB2 pureScale cluster, Tivoli Storage FlashCopy Manager daemon processes are running on multiple hosts. These daemon processes are active on only one of the hosts, and are in standby mode on the other hosts. If a failover occurs and the current host, where Tivoli Storage FlashCopy Manager daemon processes were running, is unavailable, the daemon processes start on another host. Back up and restore operations can be run from any host that is active and configured to run Tivoli Storage FlashCopy Manager.

Backup and restore methods with FlashCopy and snapshots

A snapshot or FlashCopy is an instant, point-in-time copy of a logical unit (LUN) or a set of LUNs.

FlashCopy and snapshots

The term *FlashCopy* is used for IBM System Storage DS8000, IBM System Storage SAN Volume Controller, and IBM Storwize family storage devices. A FlashCopy creates a point-in-time copy in which the target volume represents an exact copy of the data on a source volume at the time the FlashCopy starts. Data that exists on the target volume is replaced by the copied data. When you create a FlashCopy of a source volume, Tivoli Storage FlashCopy Manager requires that the target volume must be the same size as the source volume. In addition, the target volume and source volume must have the same logical track format. The source and target volumes must also be on the same storage system.

For IBM XIV Storage System, IBM System Storage N series, NetApp, and file systems such as GPFS, the term *snapshot* is used. A snapshot represents a point-in-time copy of a volume or set of volumes without having to define a specific target volume. The source volumes and snapshots are located on the same storage system. Similarly, a file system snapshot represents a point-in-time copy of a file system or file set within a file system. The space that is required for the snapshot is allocated automatically within the same storage system or file system, and can increase over time.

Using a FlashCopy or snapshot you can back up data from source volumes to target volumes. Similarly, you can back up file systems or file sets within a file system. When data is restored, backup copies are retrieved and the data is copied to the source volume, or copied to the original location in the file system or file set.

Types of snapshot backups

There are two types of snapshot backups, a full copy snapshot and a space-efficient snapshot. The type of snapshot backups that are available depend on the storage environment. During a full copy snapshot, all blocks of data on the source volume are copied to the target volume. During a space efficient snapshot, only blocks of data that are overwritten on the source volume are copied.

Transferring snapshots to Tivoli Storage Manager

When you use Tivoli Storage FlashCopy Manager with Tivoli Storage Manager products, you can transfer snapshots to the Tivoli Storage Manager server. To send these snapshot backups to the Tivoli Storage Manager server, you must configure a backup server or cluster.

The following figure shows the relationship among the components in a production environment when you run a backup or restore snapshot.

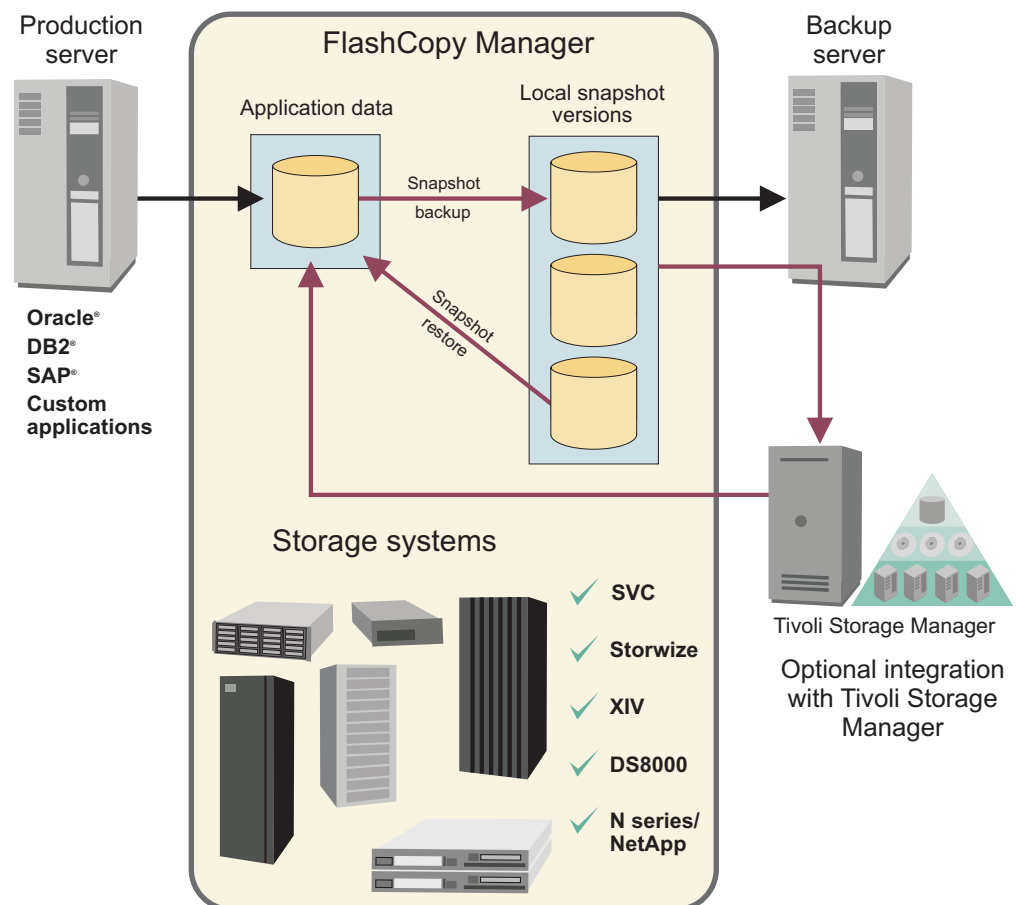


Figure 1. Tivoli Storage FlashCopy Manager backup and restore environment

Database cloning

The database cloning process creates an exact copy of a database to provide near-production data.

Tivoli Storage FlashCopy Manager uses the FlashCopy or snapshot function for database cloning. The following list identifies scenarios when you might clone a database:

- To create a test system before you introduce a new product release, or new functions into a production environment.
- To create an education system from a master training system. You can reset the cloned database before you start a new course.
- To create a dedicated reporting system to offload the workload away from the production environment.

Traditionally, the database cloning process redirected a restore operation to create the clone. This method has disadvantages, including system downtime and degraded system performance. Tivoli Storage FlashCopy Manager clones a database by using the storage system FlashCopy or snapshot capabilities to minimize the impact on the production database. A *clone server* or *clone system* is required by Tivoli Storage FlashCopy Manager to mount a cloned database.

The following figure shows how Tivoli Storage FlashCopy Manager creates and stores a cloned database on a clone server.

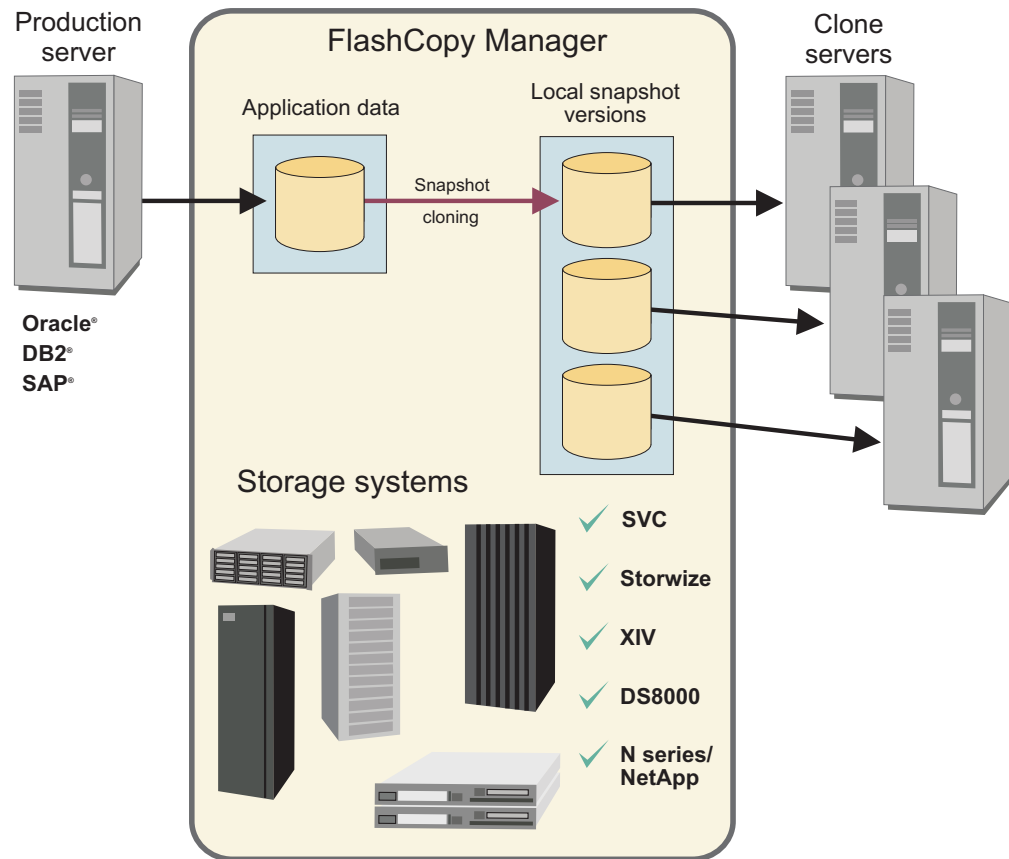


Figure 2. Tivoli Storage FlashCopy Manager and database cloning

Software components

Tivoli Storage FlashCopy Manager is composed of several software components.

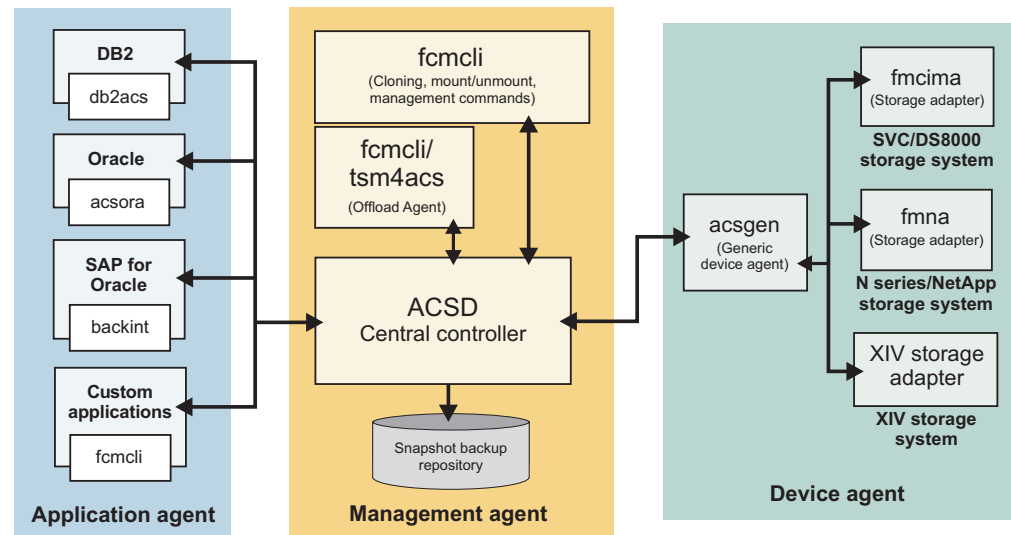


Figure 3. Tivoli Storage FlashCopy Manager system components

Application agent

The application agent provides the necessary support to implement snapshot-based backup and restore operations. This agent interacts with the applications and tracks when a Tivoli Storage FlashCopy Manager backup is created for a specific application.

Management agent

The management agent acsd coordinates all the components that are involved in backup, restore, and cloning operations. The agent controls the flow of information among the application and device agents, and other daemons. The agent provides access to the snapshot backup repository. This repository contains information about the snapshot backups and their relationships to snapshot-capable storage devices.

Device agent

The acsgen device agent is a generic agent that interacts with storage device-specific adapters and the central controller agent. This agent is also used to send and request updates of the progress and usability information that is stored in the local snapshot backup repository.

The following lists the storage device-specific agents that communicate with the acsgen agent:

- The CIM adapter fmcima is used with the generic device agent acsgen. This adapter issues commands to the supported storage device by using the CIM interface. Examples of supported storage include DS8000, Storwize family, and SAN Volume Controller.

- The XIV system storage adapter is used with the generic device agent `acsngen`. This adapter communicates with the `acsngen` agent and issues commands to the XIV system Storage System by using the command-line interface `XCLI`.
- The N series and NetApp storage adapter `fmna` is used with the generic device agent `acsngen`. This adapter issue commands to the storage device by using the NetApp `ONTAPI` interface.

Offload agent

The offload agent `tsm4acs` is used to send an existing snapshot to Tivoli Storage Manager. This agent also calls the generic device agent for mount and unmount operations on a backup system. From the command-line interface `fcmlcli`, you can manually start an offload backup to Tivoli Storage Manager.

Tivoli Storage FlashCopy Manager command-line interface

The command-line interface `fcmlcli`, is used to issue various commands.

Chapter 2. Planning

Before you install Tivoli Storage FlashCopy Manager for UNIX and Linux, review the system, application, and storage requirements.

Review the Tivoli Storage FlashCopy Manager Pre-installation Checklist that is attached to the technote for the hardware and software requirements for Tivoli Storage FlashCopy Manager. The detailed hardware and software requirements are published as a part of the following technote: <https://www.ibm.com/support/docview.wss?uid=swg21427692>. From this technote, select the required software version and then select the required component link. The hardware and software requirements page contains the Pre-installation Checklist and an installation planning worksheet.

Note: The pre-installation checklist contains the most current requirement information, use this list to validate your environment.

Tivoli Storage FlashCopy Manager depends on the correct setup of different subsystem components. The following conditions are the minimum environment requirements:

- A suitable disk layout of the application on the production server
- Correctly defined storage definitions on the storage system
- Connectivity from the production server to the storage system

The installation planning sheet helps you to determine the correct type of installation that is required for your environment. The following areas are covered in the planning sheet:

- How to determine the configuration mode for your environment.
- How to decide the parameters and settings for the specific application that you want to protect. The required parameters for each specific software application and custom application are outlined in the planning sheet.
- How to determine the parameters and settings for the specific storage system that you use in your environment.
- What passwords are required during the installation.

IBM FlashCopy Manager Prerequisite Checker

Run the IBM FlashCopy Manager Prerequisite Checker to check the compatibility of the operating system, and available software that is to be used by Tivoli Storage FlashCopy Manager.

The IBM FlashCopy Manager Prerequisite Checker is a tool that automates a subset of the checks that are documented in the Tivoli Storage FlashCopy Manager *Pre-installation Checklist*, which is attached to the IBM Tivoli Storage FlashCopy Manager Hardware and Software Requirements technote.

The hardware and software requirements for Tivoli Storage FlashCopy Manager for UNIX and Linux are published in the following technote: <http://www.ibm.com/support/docview.wss?uid=swg21427692>. Follow the link to the requirements

technote for your specific release or update level. From there you will find the *Pre-installation Checklist* and the *Installation Planning Worksheet* for the most recent version of the product.

For information about how to run the IBM FlashCopy Manager Prerequisite Checker, see the technote here <http://www.ibm.com/support/docview.wss?uid=swg27043307>.

Capacity planning

Ensure that there is sufficient storage space before you install and use IBM Tivoli Storage FlashCopy Manager.

The storage space that is required for Tivoli Storage FlashCopy Manager can be divided into the following categories:

- Space that is required for the global product installation on the system.
- Space that is required to enable each individual database instance or custom application instance with Tivoli Storage FlashCopy Manager. This enablement is referred to as activation.
- Space that is required on the storage system or in the GPFS file system to store the actual snapshot backups or clones.

Space requirement for global product installation

The space that is required for the product installation of Tivoli Storage FlashCopy Manager varies depending on the underlying operating system. The following table shows the default installation paths and the average space requirements.

Table 1. Space requirements for a global product installation of Tivoli Storage FlashCopy Manager

Operating system	Default installation path	Space required (MB)
AIX	/usr/tivoli/tsfcm/acs_version_number	1100
Solaris	/opt/tivoli/tsfcm/acs_version_number	700
Linux	/opt/tivoli/tsfcm/acs_version_number	500
HP-UX	/opt/tivoli/tsfcm/acs_version_number	1900

Space requirement for database instance or custom application installation

Tivoli Storage FlashCopy Manager must also be installed on each database and custom application instance that is enabled for snapshot-based data protection or cloning. This process is called activation and occurs during the installation. During this process, all necessary files are copied from the installation path to a database instance-specific or custom application-specific installation directory. The space that is required for each Tivoli Storage FlashCopy Manager enabled application is approximately equal to the amount of space that is required for the global product installation.

Tivoli Storage FlashCopy Manager must also be installed on application instances that are running on a backup server.

Extra space is required for Tivoli Storage FlashCopy Manager log files. Log files are written continuously by Tivoli Storage FlashCopy Manager without automatically deleting the older ones. You must monitor periodically the amount of space that is used by these log files and manually delete them if required.

Space requirement for snapshot copies

The snapshot copies of your application data or databases require the most space. The space that is required depends on the following factors:

- The total size of all storage system source volumes that are part of the volume group on the storage system. The volume groups contain the application data.
- The type of snapshot whether it is a full copy or a space-efficient snapshot.
- The number of backup copies.
- The number of changes that occur on the source volumes after a snapshot is taken. This factor applies to space-efficient snapshots only.
- In an IBM DB2 pureScale environment, snapshots are stored in the GPFS file system. Therefore, the GPFS file system must have sufficient free space to store all snapshots. The size of a snapshot depends on the number of changes to the GPFS file system content that occur after the snapshot was taken. As a consequence, space requirements for a single snapshot can increase over time.

Use the **MAX_VERSIONS** parameter in the Tivoli Storage FlashCopy Manager profile configuration file to limit the number of snapshots that are stored on a storage system or in a GPFS file system.

On SAN Volume Controller, IBM Storwize family, and IBM System Storage DS8000, full snapshot copies require the same amount of space as the corresponding source volumes.

Required communication ports

Tivoli Storage FlashCopy Manager for UNIX and Linux uses ports for communication between its daemon processes on backup or cloning systems, and the production system, and the storage systems. Port numbers are defined during the installation of Tivoli Storage FlashCopy Manager for UNIX and Linux.

To determine the port number for the ports that are used for Tivoli Storage FlashCopy Manager for UNIX and Linux see the following table:

Table 2. Tivoli Storage FlashCopy Manager for UNIX and Linux port numbers

TCP Port	Initiator: Out-Bound (From Host)	Target: In-Bound (To Host)
57328	Production server and backup/cloning server	ACSD port on production system
5989 (HTTPS port) ^[1] 5988 (HTTP port) ^[1]	Production server and backup/cloning server	SAN Volume Controller Storwize family cluster CIM agent
6989 (HTTPS port) ^[1] 6988 (HTTP port) ^[1]	Production server and backup/cloning server	DS8000 DS8000 CIM Agent
7778	Production server and backup/cloning server	XIV system XIV system CLI

Table 2. Tivoli Storage FlashCopy Manager for UNIX and Linux port numbers (continued)

TCP Port	Initiator: Out-Bound (From Host)	Target: In-Bound (To Host)
443 (HTTPS port) ^[1] 80 (HTTP port) ^[1]	Production server and backup/cloning server	N series systems NetApp NetApp Manageability SDK/ONTAP
[1] Where COPYSERVICES_COMMPROTOCOL is the corresponding parameter name in the profile.		

Preparation for installation

Before you install Tivoli Storage FlashCopy Manager, review the hardware, software requirements, and application environment. You must complete the Pre-installation Checklist and Planning Worksheet before you install Tivoli Storage FlashCopy Manager for UNIX and Linux.

The hardware and software requirements for Tivoli Storage FlashCopy Manager for UNIX and Linux are published in the following technote: <http://www.ibm.com/support/docview.wss?uid=swg21427692>. Follow the link to the requirements technote for your specific release or update level. From there you will find the *Pre-installation Checklist* and the *Installation Planning Worksheet* for the most recent version of the product.

To help you to prepare your environment for Tivoli Storage FlashCopy Manager for UNIX and Linux, you can run the preinstallation checker tool. For more information about the preinstallation checker, see “IBM FlashCopy Manager Prerequisite Checker” on page 7.

Before you start the installation process, complete the following tasks:

- Review the requirements and ensure that all requirements are met.
- Complete the *Pre-installation Checklist*.
- Complete the *Installation Planning Worksheet*.

Important: You must complete the *Pre-installation Checklist* and *Installation Planning Worksheet* as this information is required during the installation.

Before you install Tivoli Storage FlashCopy Manager, ensure that the volume and storage layout is correct for your application environment.

Verify the DB2 system

Ensure that the following structure is in place before you install and use Tivoli Storage FlashCopy Manager.

The DB2 configuration must have the following structure:

- At least one volume group for each database partition that contains table spaces and the local database directory.
- At least one volume group for each database partition that contains database log files.

- Data must be on file systems that are supported by Tivoli Storage FlashCopy Manager.
- Database log files and database data must be contained in separate independent file sets or in separate file systems in an IBM DB2 pureScale environment. Unless stated otherwise, the term *file set* can be interchanged with *volume group* when describing the DB2 structure.

Any other data that is stored on the volume groups is processed by Tivoli Storage FlashCopy Manager and included in the backup image. When you restore a backup image, the whole backup image is restored. Therefore, any data on the file system that is updated or created after the backup is taken is overwritten. To ensure that nothing is overwritten unintentionally, do not store any other data in the data and log volume groups.

For DB2 pureScale, any additional files that are stored in log file sets and data file sets are included in the backup. When you restore a backup image, extra files and nested file sets are overwritten. To avoid overwriting, do not store any other files in log file sets or database data file sets. Ensure that you do not link independent file sets containing unrelated data in file sets that participate in snapshots.

Extra files that are not associated with the database backup operation, but are stored in the volume groups, can cause the backup to fail. Use the **NEGATIVE_LIST** parameter in the Tivoli Storage FlashCopy Manager profile to control the processing of these files. For information about this parameter, see the “CLIENT” on page 143 profile section for details.

Tivoli Storage FlashCopy Manager processes table spaces, the local database directory, and log files. The volume group layout for DB2 is detailed in the *Pre-installation Checklist*.

The hardware and software requirements for Tivoli Storage FlashCopy Manager for UNIX and Linux are published in the following technote: <http://www.ibm.com/support/docview.wss?uid=swg21427692>. Follow the link to the requirements technote for your specific release or update level. From there you will find the *Pre-installation Checklist* and the *Installation Planning Worksheet* for the most recent version of the product.

Tivoli Storage FlashCopy Manager does not support a volume and storage layout where a single database partition is spread across multiple storage devices. In an AIX logical volume manager mirroring environment, each mirror must be located within a separate storage cluster.

To offload backups from this environment to Tivoli Storage Manager, Tivoli Storage FlashCopy Manager requires DB2 and the DB2 instance to be installed on a backup server. This server must be configured to ensure that the topology of the production and backup server are the same. The number of DB2 partitions and DB2 partition numbers must be identical on the production and backup server. However, the DB2 partitions on the backup server can be consolidated into one backup server even if the production database is spread across multiple hosts.

Related concepts:

“Logical Volume Manager support (AIX only)” on page 19

Preparing the DB2 high-availability disaster recovery server or DB2 standby server

Before you install Tivoli Storage FlashCopy Manager, verify the configuration of the DB2 high-availability disaster recovery (HADR) or DB2 standby server environment. Preparing a DB2 (HADR) server is not applicable to a DB2 pureScale environment or to a partitioned DB2 database.

A DB2 (HADR) server in primary mode is protected by Tivoli Storage FlashCopy Manager in the same way as for standard non-HADR DB2 servers. DB2 (HADR) servers in standby mode can be protected with Tivoli Storage FlashCopy Manager but use different commands independent from the standard DB2 commands.

Protecting a DB2 (HADR) server in standby mode with Tivoli Storage FlashCopy Manager assumes that the corresponding server in primary mode is also protected by Tivoli Storage FlashCopy Manager. After a DB2 (HADR) takeover operation, the protection of the former DB2 (HADR) standby server now taking the role of the primary server can be continued by Tivoli Storage FlashCopy Manager for DB2.

The storage layout for a DB2 (HADR) primary and standby server environment must be identical to the storage layout described in “Verify the DB2 system” on page 10. In addition, the names of files, file systems, and mount points must be identical for both the DB2 primary and the DB2 standby environments. When you use DB2 automatic storage, then the table space container IDs and names can be different between the primary and standby systems. However, the automatic storage paths must be identical.

Remember: In a typical environment, both sides of a DB2 (HADR) or DB2 standby server environment can act as the primary or the standby system. To support such configurations, you can create a single Tivoli Storage FlashCopy Manager profile at each site. This profile can be used regardless of whether the system is the active or inactive copy of DB2. For more information about standby nodes, see Figure 4.

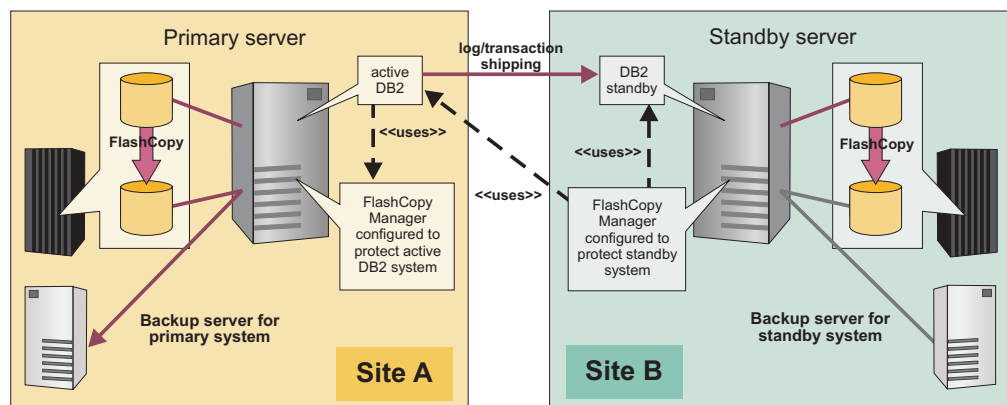


Figure 4. Protection of DB2 (HADR) standby nodes with IBM Tivoli Storage FlashCopy Manager

Although a single Tivoli Storage FlashCopy Manager profile can be used, on both sides, there are different commands for backing up DB2. For the primary server, the command is `db2 backup use snapshot` and for the standby system, the command is `fcmlcli -f backup_db2standby`. In an environment where Tivoli Storage Manager is configured, this configuration also affects the way Tivoli Storage FlashCopy Manager triggers the Tivoli Storage Manager offload backup. While DB2 is active, Tivoli Storage FlashCopy Manager issues a `db2 backup`

command for the backup to Tivoli Storage Manager. If DB2 is in standby mode, Tivoli Storage FlashCopy Manager creates the backup by using the Tivoli Storage Manager backup-archive client.

Restriction: Tivoli Storage FlashCopy Manager communicates with the active site to query DB2 for a list of files to back up. Therefore, the names of mount points and file systems that contain DB2 data must be identical in site A and site B.

Remember: Although you can create a single profile on either site that can be used regardless of whether the site is active or passive, you must install Tivoli Storage FlashCopy Manager separately on each site. There is no installation option that installs Tivoli Storage FlashCopy Manager on either site simultaneously.

Related reference:

Backup and restore commands for DB2 integrated with DB2 utilities

Preparing DB2 in an SAP environment

Before you install Tivoli Storage FlashCopy Manager, verify the configuration for SAP on DB2 system.

The storage layout for DB2 in an SAP environment is identical to the storage layout described in “Verify the DB2 system” on page 10. In addition, Tivoli Storage FlashCopy Manager supports SAP database environments where multiple logical partitions of a DB2 database are within a single volume group. This setting is referred to as volume sharing, see the **PARTITION_GROUP** parameter for more details. With volume sharing, individual database partitions cannot be restored because of the granularity of the DB2 partitions specified by the **PARTITION_GROUP** parameter.

Tivoli Storage FlashCopy Manager does not support a volume and storage layout where a single database partition is spread across multiple storage devices. In an AIX logical volume manager mirroring environment, each mirror must be located within a separate storage cluster.

Related concepts:

“Logical Volume Manager support (AIX only)” on page 19

Related reference:

Backup and restore commands for DB2 integrated with DB2 utilities

Preparing Oracle in an SAP environment

Before you install Tivoli Storage FlashCopy Manager, verify the configuration for Oracle in an SAP environment.

Tip: Review the exact volume layout specifications (supported through the SAP BR*Tools Disk - Volume Backup function) that are available in the *SAP Database Guide for Oracle*.

Tivoli Storage FlashCopy Manager requires that all Oracle table space data files, online redo logs, and control files are on file systems that are supported by Tivoli Storage FlashCopy Manager. The data that is under the sapdata, origlog and mirrlog directories must be on separate volume groups. If other data is stored within those volume groups, it is processed by Tivoli Storage FlashCopy Manager and included in the Tivoli Storage FlashCopy Manager backup image. This data is overwritten during a restore operation. As a result, do not store other objects such as database instance binary files and offline redo logs on the volume groups that you want to back up. SAP BR*Tools requires a list of files and directories that can

be backed up. If Tivoli Storage FlashCopy Manager detects such data in one of the volumes to be backed up, the backup operation can fail.

Tivoli Storage FlashCopy Manager processes table spaces at the volume level. The required volume group layout for Oracle in an SAP environment is detailed in the *Volume group layout requirements* section of the *Pre-installation Checklist*.

The hardware and software requirements for Tivoli Storage FlashCopy Manager for UNIX and Linux are published in the following technote: <http://www.ibm.com/support/docview.wss?uid=swg21427692>. Follow the link to the requirements technote for your specific release or update level. From there you will find the *Pre-installation Checklist* and the *Installation Planning Worksheet* for the most recent version of the product.

Tivoli Storage FlashCopy Manager does not support a volume and storage layout where the database is spread across multiple storage devices. In an AIX logical volume manager mirroring environment, each mirror must be located within a separate storage cluster.

Preparing Oracle systems (non-SAP, non-ASM)

Tivoli Storage FlashCopy Manager processes database files at a volume level on Oracle systems and requires these database files to be on one or more dedicated volume groups.

The Oracle table space database files must be on file systems that are supported by Tivoli Storage FlashCopy Manager on your system. However, Oracle database control files and Oracle active log files must not be in the same volume groups as the table space data files.

If other data is stored in the table space data volume groups, it is processed by Tivoli Storage FlashCopy Manager and included in the Tivoli Storage FlashCopy Manager backup image. During a restore operation, this data is overwritten. Therefore, do not store objects such as database binary files, online redo logs, offline redo logs, or control files on the data volume groups.

Extra files that are not associated with the database backup operation but are stored within the same file system, can cause the backup to fail. Use the **NEGATIVE_LIST** parameter in the Tivoli Storage FlashCopy Manager profile to control the processing of these files. For information about this parameter, see the profile section "CLIENT" on page 143 for details.

Tivoli Storage FlashCopy Manager processes table spaces only. The volume group layout that is required for Oracle systems (non-SAP and non-ASM) is detailed in the *Volume group layout requirements* section of the *Pre-installation Checklist*.

The hardware and software requirements for Tivoli Storage FlashCopy Manager for UNIX and Linux are published in the following technote: <http://www.ibm.com/support/docview.wss?uid=swg21427692>. Follow the link to the requirements technote for your specific release or update level. From there you will find the *Pre-installation Checklist* and the *Installation Planning Worksheet* for the most recent version of the product.

Tivoli Storage FlashCopy Manager does not support a volume and storage layout where the database is spread across multiple storage devices. In an AIX logical volume manager mirroring environment, each mirror must be located within a separate storage cluster.

Tivoli Storage FlashCopy Manager requires that an Oracle recovery catalog database is available when you back up data. This recovery catalog must be present regardless of the type of backup.

If a shell other than ksh or bash is used, Oracle specific environment variables such as `ORACLE_HOME` and paths must be accessible when the `su - oracle_user -c` command is entered.

Preparing Oracle Automatic Storage Management

Ensure that you have your environment set up to protect your Oracle ASM data with Tivoli Storage FlashCopy Manager.

Procedure

1. Define the storage clusters in the Tivoli Storage FlashCopy Manager profile with the **DEVICE_CLASS** profile parameter. The definitions must specify that Tivoli Storage FlashCopy Manager selects the cluster for the current operation.
For an ASM disk group with normal redundancy, the backup completes even if one of the failure groups is not on the storage device. For an ASM disk group with high redundancy, the backup completes even if two of the failure groups are not on the storage device.
2. Create the ASM disk groups. If you already created the ASM disk groups, verify that they meet the following criteria.
 - For an ASM backup, create a disk group on the backup system to host an Oracle control file. This disk group has the same name as the disk group where the control file is on the production system. During a backup operation, the Oracle control file is stored in the Tivoli Storage FlashCopy Manager repository directory on the production server.
 - For ASM cloning, ensure that the ASM disk groups are on supported storage systems, otherwise the cloning operation fails.
3. During the offload operation, the control file is transferred into a temporary directory within `ACS_DIR` on the backup server by Tivoli Storage FlashCopy Manager. RMAN restores the control file into the locations that are specified within the database profile from this location as part of the offload operation.
4. Tivoli Storage FlashCopy Manager must have an Oracle recovery catalog database available when you back up data. This recovery catalog must be present regardless of the type of backup. Typically one ASM instance can serve multiple databases.
Tivoli Storage FlashCopy Manager supports this setup when dedicated disk groups are used for each database. For normal-redundancy disk groups and high-redundancy disk groups, Tivoli Storage FlashCopy Manager handles failure groups by allowing backups of disk groups that are on supported storage systems.
5. If needed, you can change the redundancy level and add failure groups after a restore operation. Tivoli Storage FlashCopy Manager does not re-create failure groups when a restore operation completes.
6. Export Oracle specific environment variables, such as `ORACLE_HOME` and paths so that they are accessible if the `su - oracle_user -c` is entered.

For ksh or bash, enter the following command with root user ID to verify that the Oracle variables are accessible: `su - oracle_user -c env | grep ORA`

ASM disk group layout

An ASM disk group is a collection of disks that Oracle ASM manages as a unit. Because Tivoli Storage FlashCopy Manager processes database files at the ASM disk group level, the database files are required to be on dedicated disk groups. Non-application data that is stored on these disk groups is also processed by Tivoli Storage FlashCopy Manager and is included in the backup images. This non-application data is overwritten during a restore operation.

For ASM cloning, the control files must be stored in an ASM disk group. If any control file is not on an ASM disk group, the cloning operation fails with an error.

Extra files that are not associated with the database backup operation but are stored within the same file system, can cause the backup to fail. Use the **NEGATIVE_LIST** parameter in the Tivoli Storage FlashCopy Manager profile to control the processing of these files. For information about this parameter, see the profile section “CLIENT” on page 143 for details.

Tivoli Storage FlashCopy Manager processes table spaces only. The disk group layouts that are required when you are backing up or cloning in an ASM environment are detailed in the *Volume group layout requirements* section of the *Pre-installation Checklist*.

The hardware and software requirements for Tivoli Storage FlashCopy Manager for UNIX and Linux are published in the following technote: <http://www.ibm.com/support/docview.wss?uid=swg21427692>. Follow the link to the requirements technote for your specific release or update level. From there you will find the *Pre-installation Checklist* and the *Installation Planning Worksheet* for the most recent version of the product.

ASM in a DS8000 environment

For IBM System Storage DS8000 environments, Tivoli Storage FlashCopy Manager does not use FlashCopy consistency groups when a FlashCopy backup is created. All table space files must be on a single disk group. There is no consistency across multiple LUNs on this storage system.

Ensure that all table space files are on a single disk group on DS8000 system. In addition, verify that the disk group contains exactly one LUN on the DS8000. Tivoli Storage FlashCopy Manager does not support databases that are distributed across multiple storage clusters. There is one exception to this statement, and that is in environments where failure groups are used in a manner where every storage cluster contains a complete image of the databases.

ASM failure groups

Tivoli Storage FlashCopy Manager supports Oracle Automatic Storage Management (ASM) failure groups.

When the ASM database is configured with normal or high redundancy, the disk groups are composed of two or three failure groups. These groups can be on two or three respective storage clusters. Tivoli Storage FlashCopy Manager creates a backup entirely within only one of the storage clusters.

If you use ASM failure groups, review these guidelines:

- In setups where all failure groups are on one storage cluster, Tivoli Storage FlashCopy Manager backs up all failure groups.
- In setups where all failure groups are on different storage clusters, Tivoli Storage FlashCopy Manager backs up all failure groups that are on the storage cluster that is configured for the current operation. For more information, see “*DEVICE_CLASS device*” on page 171.
- Tivoli Storage FlashCopy Manager does not split the failure groups on a remote system.
- Failure group support does not require a backup server.
- Tivoli Storage FlashCopy Manager does not re-create failure groups when a restore operation is completed. You can reset the redundancy level manually by adding the missing failure groups after the restore operation.

ASM cloning parameters and Tivoli Storage FlashCopy Manager

The ASM parameters that point to ASM disk groups on a clone system affect the Tivoli Storage FlashCopy Manager in certain scenarios. Review the list of ASM parameters when you are preparing Tivoli Storage FlashCopy Manager for Oracle ASM.

Tivoli Storage FlashCopy Manager parameters

ENHANCED_PARTITIONING

In a clone system when **VOLUME_MGR** is set to *ASM*, the **ENHANCED_PARTITIONING** parameter is ignored by Tivoli Storage FlashCopy Manager.

FLASH_DIR_LIST

For ASM cloning, ensure that this parameter is not configured. If this parameter is configured in the cloning section of the profile file when **VOLUME_MGR** is set to *ASM*, Tivoli Storage FlashCopy Manager stops and sends an error message.

VOLUME_MGR

For the cloning section of the Tivoli Storage FlashCopy Manager profile, this parameter must be set to *ASM* to support ASM cloning.

Oracle parameters

DB_CREATE_FILE_DEST

The parameter **DB_CREATE_FILE_DEST** setting on your production system is also used on the clone system when the parameter **OVERWRITE_DATABASE_PARAMETER_FILE** is set to YES. When you create new data files, the specified location must be available on the clone system.

The following situations are possible:

DB_CREATE_FILE_DEST points to the ASM disk group that is part of the snapshot. No action is required.

DB_CREATE_FILE_DEST points to the ASM disk group that is not part of the snapshot. The ASM disk groups must be created on the clone server before the clone operation.

DB_CREATE_FILE_DEST points to a directory on a file system. No action is required. The directory is created on the clone system.

DB_CREATE_ONLINE_LOG_DEST_n

The parameter **DB_CREATE_ONLINE_LOG_DEST_n** setting on your production system is also used on the clone system when the parameter **OVERWRITE_DATABASE_PARAMETER_FILE** is set to YES. When you create new log files, the specified location must be available on the clone system. The same situations as specified for parameter **DB_CREATE_FILE_DEST** are possible.

LOG_ARCHIVE_DEST

The log archive destination that is specified with **LOG_ARCHIVE_DEST** and **LOG_ARCHIVE_DEST_n** can point to regular file systems or ASM disk groups. Tivoli Storage FlashCopy Manager turns off archive logging on the clone database as part of the clone operation. Archive logging can be activated manually after the clone operation finishes, or through postprocessing scripts.

CONTROL_FILES

All database control files for ASM cloning must be on ASM disk groups. The LUNs of these disk groups are added to the snapshot backup.

Preparing custom applications

Some prerequisites are necessary when you are preparing a custom application environment.

Tivoli Storage FlashCopy Manager performs snapshot backups of plain file systems on a volume group level. Therefore, ensure that the files you want to protect are stored in dedicated file systems and volume groups.

In addition to storing the data in dedicated volume groups, those volume groups must be on a file system type that is supported by Tivoli Storage FlashCopy Manager. Any other data that is stored on these volume groups, is also processed by Tivoli Storage FlashCopy Manager, and it is included in the backup images. When the backup image is restored, any additional data on the file system that is updated or created after the backup is overwritten.

Attention: Do not store any data that you do not want to restore within volume groups that are being processed by Tivoli Storage FlashCopy Manager. If Tivoli Storage FlashCopy Manager detects such data in one of the volumes to be backed up, the backup operation can fail.

In situations where files not associated with the database are stored with the file system that is used for backup and restore operations, use the **NEGATIVE_LIST** parameter. This Tivoli Storage FlashCopy Manager profile parameter can be used to control file processing. For information about the **NEGATIVE_LIST** profile parameter, see the profile section “CLIENT” on page 143 for details.

Tip: To create a transaction-consistent backup of your custom application, configure Tivoli Storage FlashCopy Manager to run a pre-flash and post-flash command immediately before and after, the creation of the snapshot. These commands can suspend and resume the application to create a consistent backup. For more information about these commands, see “Backup and restore commands for custom applications” on page 279

Logical Volume Manager support (AIX only)

You can use Tivoli Storage FlashCopy Manager in environments where volume groups are mirrored between two storage clusters by using Logical Volume Manager (LVM) mirroring on AIX.

This support is provided on IBM System Storage DS8000, IBM System Storage SAN Volume Controller, IBM Storwize family, IBM XIV Storage System, IBM System Storage N series, and NetApp environments. When LVM mirroring is used to mirror volume groups between two storage clusters, a FlashCopy backup is created such that only one mirror is being copied.

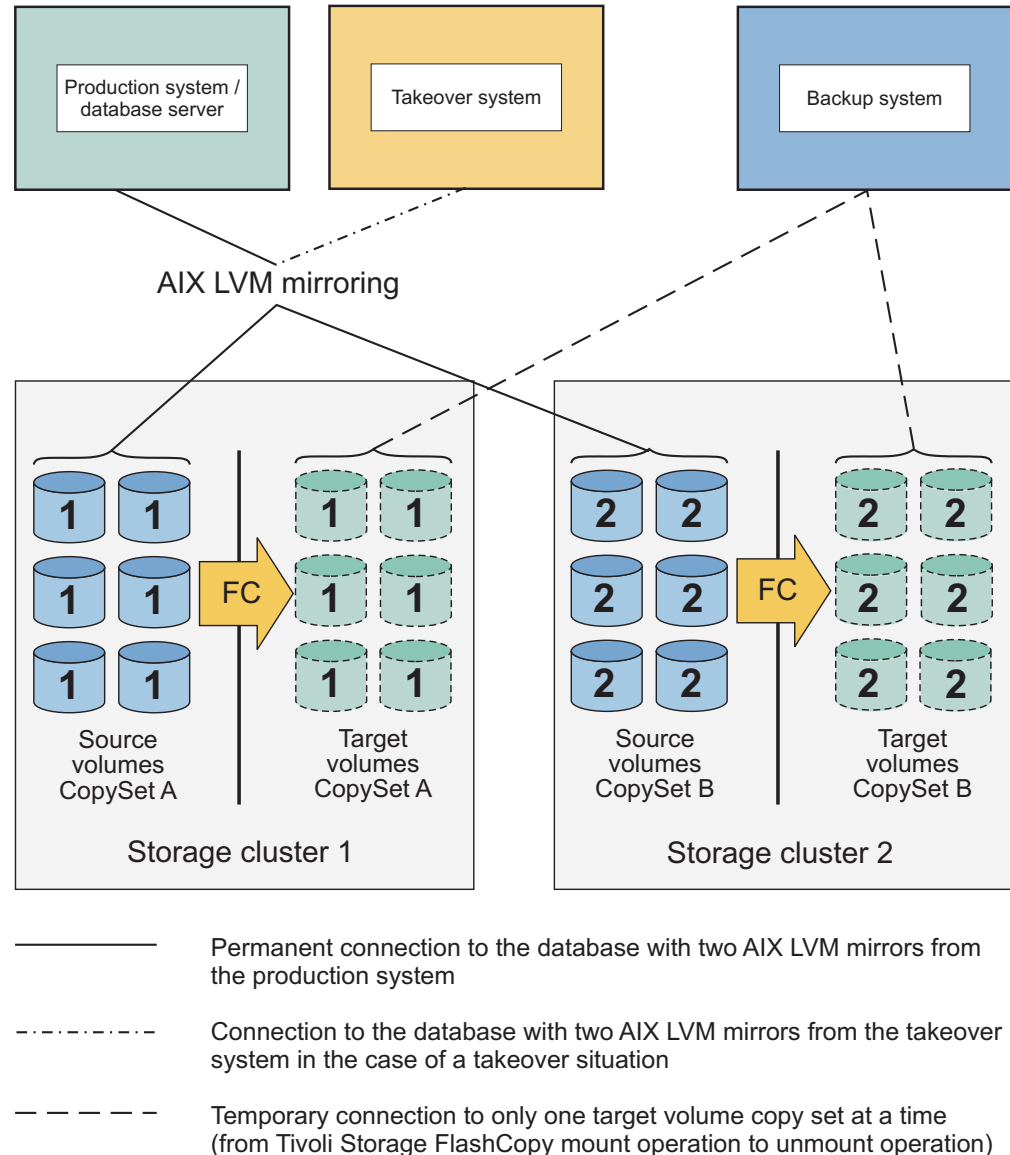


Figure 5. Tivoli Storage FlashCopy Manager in an LVM environment

AIX LVM mirroring provides these advantages:

- Only one of the two LVM mirrors are used in the FlashCopy process. Using one mirror saves the number of needed target volumes and reduces the time that is needed for the FlashCopy process.
- Avoids unnecessary performance degradation within the storage system.

- All LVM mirrors on the production system remain synchronized during the FlashCopy backup process.
- Online or offline FlashCopy backups can be created in both LVM mirrored and non-LVM mirrored environments. There is no change in the backup and restore procedures as provided in the applicable documentation.
- The FlashCopy backup process at no time compromises the high-availability purpose for which the mirrors were set up. It is not necessary to resynchronize the logical volumes after the FlashCopy backup request.
- Tivoli Storage FlashCopy Manager provides information about asymmetrical LVM mirror setups when encountered. This information can prevent the FlashCopy backup from running in unfavorable situations but can also reveal a general deficiency of the high-availability setup as well.

Tivoli Storage FlashCopy Manager requires that the LVM mirroring sets are in different storage subsystems. For example, different SAN Volume Controller clusters, Storwize family, DS8000, or XIV system. Complete mirrors are recommended to be stored on both storage clusters. If this setting is not possible, Tivoli Storage FlashCopy Manager continues processing for those clusters where a complete image of the application can be found.

To configure Tivoli Storage FlashCopy Manager for LVM mirroring, define both storage subsystems within the Tivoli Storage FlashCopy Manager profile. Use the **DEVICE_CLASS** parameter to allow Tivoli Storage FlashCopy Manager to select the storage subsystem. At least one backup server is required so that Tivoli Storage FlashCopy Manager can mount a FlashCopy backup to verify the consistency of the backup and split the LVM mirrors.

During a restore operation, Tivoli Storage FlashCopy Manager runs all the commands that are required to prepare the LVM environment again for the second mirror. The administrator is informed by message FMM0755I in the detailed restore log file that the volume groups are ready for synchronization. The administrator can run this operation at a more suitable time for instance after completion of the database recovery.

Note: The administrator must examine the log files for these messages. They do not display on the screen.

Preparing applications that run on VMware or KVM virtual machines

Before you install Tivoli Storage FlashCopy Manager on VMware or KVM virtual machines that run Linux guest operating systems, you must verify the configuration of the application that you want to protect.

Before you begin

Different applications have specific Tivoli Storage FlashCopy Manager configuration requirements. For more information about application-specific requirements, see Chapter 2, “Planning,” on page 7.

Procedure

VMware

- Before you back up data or clone databases on VMware virtual machines, ensure that all source LUNs in the backup or clone operations are attached to the virtual machine with one of the following methods:
 - VMware physical mode raw device mapping (pRDM)
 - iSCSI
 - Network file system (NFS)
- Run a Tivoli Storage FlashCopy Manager restore operation from a snapshot to an existing pRDM disk. The operation does not create a virtual machine or pRDM definition as part of the restore process.

KVM

- Before you back up data or clone databases on KVM virtual machines, ensure that all source LUNs in the backup or clone operations are attached to the virtual machine with one of the following methods:
 - Block device mapping (BDM)
 - iSCSI
 - Network file system (NFS)
 - PCI Passthrough
- Run a Tivoli Storage FlashCopy Manager restore operation from a snapshot to an existing BDM disk. The restore operation does not create a virtual machine or BDM definition as part of the restore process.

Checking the KVM setup

Ensure that when the Tivoli Storage FlashCopy Manager KVM setup uses Block Device Mapping, the LUNs are mapped to the KVM guest as multipath devices. The LUNs must be visible as multipath devices inside the KVM guest. Run the **multipath** command to check your setup for KVM.

Procedure

To verify your KVM setup, run the **multipath** command from within the KVM guest. The command output looks similar to the following example:

```
kvm-guest:~ # multipath -ll
mpathat (360050768018205de4000000000001949) dm-7 IBM ,2145
size=2.0G features='1 queue_if_no_path' hwhandler='0' wp=rw
~+- policy='service-time 0' prio=50 status=active
~- 3:0:0:3 sdf 8:80 active ready running
```

In the example, *360050768018205de4000000000001949* is the LUN identifier. It is a unique number that must not be overwritten by the KVM stack. The product storage identifier must be visible inside the KVM guest. In the example, this identifier is *IBM ,2145*.

Preparing backup and cloning servers

Backup servers and clone servers are auxiliary hosts where Tivoli Storage FlashCopy Manager can mount backups and clones.

A backup server or clone server is used to offload the workload from the production server where the protected application is running. You must configure a backup or clone server when you want to offload snapshots to Tivoli Storage Manager. You can share one backup or clone server among multiple applications or you can have multiple backup or clone servers.

However, Tivoli Storage FlashCopy Manager does not allow backup images or clone images to be mounted directly on the production server. A backup or clone server must be set up as a separate host.

Determining the number of backup and clone servers in the environment

The number of required Tivoli Storage FlashCopy Manager backup servers is determined by the number of servers that are used to access backup images. The number of clone servers is determined by the number of servers where you want to store a cloned database of the production database. A clone server can also be used as a backup server.

For example, to access backup images on either site of a disaster recovery environment, at least two backup servers are needed. A backup server can also simultaneously be used for multiple applications and multiple production servers. Tivoli Storage FlashCopy Manager can mount a backup image on a backup server. For the following scenarios, at least one backup server is required or if FlashCopy cloning is used, a clone server is required.

- Mount backup images on another server.
- When Tivoli Storage FlashCopy Manager is used with other products for example, IBM Tivoli Storage Manager for Enterprise Resource Planning to offload backups to Tivoli Storage Manager.
- When Tivoli Storage FlashCopy Manager requires a mount operation, during a backup operation because the following conditions exist:
 - The database is running in an LVM mirrored environment on AIX
 - FlashCopy cloning is used
 - Conditions that require a so called Tivoli Storage FlashCopy Manager forced mount operation for the different storage subsystem environments:

SAN Volume Controller, Storwize family, and DS8000

A forced mount is required if the option `PREASSIGNED_VOLUMES` is set for the profile parameter `BACKUP_HOST_NAME` and the operating system is Linux or Solaris.

DS8000

A forced mount is required if the option `PREASSIGNED_VOLUMES` is set for the profile parameter `BACKUP_HOST_NAME`. In addition, the following conditions must also exist a freeze and thaw action was not used for the file systems and the operating system is AIX or HP-UX.

For a physically partitioned DB2 database, multiple backup servers can be used. The physical partitioning of the production server is not required to be identical to the physical partitioning of the backup server. However, the number of DB2 partitions and the DB2 partition numbers must be identical on the production and backup server.

Related reference:

“CLIENT” on page 143

Installation prerequisites for backup and clone servers

For hosts that are used as a backup server or clone server, the operating system version and maintenance level must be the same as the production server. For IBM DB2 pureScale, a host that is used as a backup server must have the same version of IBM General Parallel File System (GPFS) and DB2 as the production server.

Backup server requirements

For the IBM Tivoli Storage FlashCopy Manager software to run correctly, the following settings are required on the backup server:

- The user name and group name of the database instance owner or application owner on the production server must be available on the backup server. The same user ID (UID) and group ID (GID) must be used.
- IBM DB2 and Oracle environment: A database instance with the same version as the database instance on the production server must be installed on the backup server.
- Oracle in an SAP environment: An Oracle database instance is required when incremental backups that use Oracle RMAN are run. SAP BR*Tools are optional on the backup server.
- IBM DB2 pureScale: A GPFS cluster and a DB2 instance with the same topology and number of nodes as on the production server must be installed. However, the nodes are not required to be distributed across systems in the same way, but can be collocated. The backup cluster must be authorized to mount the production file system in read and write mode.

When Tivoli Storage FlashCopy Manager is used in an environment with IBM Tivoli Storage Manager, a backup server is required. This backup server is used to offload the backup workload from the production server to the backup server and sends the application critical backups to Tivoli Storage Manager.

The following Tivoli Storage Manager Data Protection clients are used by Tivoli Storage FlashCopy Manager to initiate a subsequent backup to Tivoli Storage Manager and must be installed and configured on the backup server:

- IBM DB2 Tivoli Storage Manager agent for DB2 environments. Use the agent that is associated with the DB2 instance.
- DB2 Tivoli Storage Manager agent for IBM DB2 pureScale environments. Use the agent that is associated with the DB2 instance.
- IBM Tivoli Storage Manager for Enterprise Resource Planning agent is optional for DB2 in an SAP environment.
- IBM Tivoli Storage Manager for Databases agent for Oracle only environments.
- Tivoli Storage Manager for ERP agent for Oracle in an SAP environment.
- Tivoli Storage Manager Backup-Archive client for custom application environments.

Update the Tivoli Storage Manager Data Protection client node password on the production server and all backup servers whenever it changes. When Tivoli Storage Manager is configured to use the **PASSWORDACCESS GENERATE** parameter, the password can change without notification. If the Tivoli Storage Manager Data Protection client is configured to use the **PASSWORDACCESS GENERATE** parameter, use the Tivoli Storage Manager proxy-node capability to avoid authentication errors when the password is reset. Create one data node on the Tivoli Storage Manager where all Data Protection clients from all backup and production servers are sending and retrieving data. Create one authentication node for each production

server and backup server that is configured as proxy node to this data node.

Offload backups to Tivoli Storage Manager with Oracle RMAN

To offload incremental backups from an Oracle environment, Tivoli Storage FlashCopy Manager requires an Oracle database instance to be installed and configured on the backup server. The Oracle specific environment variables, for example **ORACLE_HOME**, and paths must be exported so that they are accessible if the `su - oracle_user -c` command is entered. This accessibility can be verified by running `su - oracle_user -c env | grep ORACLE` as root user. The Oracle recovery catalog database must exist and must be accessible from the production and backup server for the Oracle user ID. In this database, Oracle RMAN records all offloaded backups. For details on the setup of a recovery catalog database, see the Oracle manuals. To verify this setup, run the following command as the Oracle user on the production host:

```
rman target / catalog catalog_user/catalog_password@
<catalog_connect_string>
```

To verify the setup of the backup system, run the following command as the root user on the backup host:

```
su -oracle user -c "rman target / catalog catalog_user/
catalog_password@catalog_connect_string"
```

The command must be able to connect to both the target and the recovery catalog databases, and show the RMAN prompt. This operation can be finished with the quit command. For example:

```
$ rman target / catalog rman/rman@catdb
,
Recovery Manager: Release 11.2.0.3.0 - Production on Mon Aug 5 13:59:53 2013

Copyright (c) 1982, 2011, Oracle and/or its affiliates. All rights reserved.

connected to target database: P01 (DBID=1213110920, not open)
connected to recovery catalog database

RMAN> quit

Recovery Manager complete.
$
```

Clone server requirements

For FlashCopy cloning, the database instances must be installed and configured on the clone server. Database cloning does not apply to IBM DB2 pureScale, or custom application environments.

Tivoli Storage FlashCopy Manager requires the following settings for cloning:

DB2 and DB2 in an SAP environment

Two database instances must be installed on the clone server. These database instances must be the same version as the database instance on the production server. One of the two database instances is assigned the same name as the production instance (on the production server). The other database instance is assigned the clone instance name. If the clone database name is the same name as the production database name, only one database instance with this common name is required on the clone server.

On the clone server, the database instance with the same name as production database instance must be assigned a user name and group name. The user name and group name must be the same names that are assigned to the database instance on the production server. The same user ID (UID) and group ID (GID) must be used. The user name, group name, UID, and GID for the clone instance must be different.

Oracle and Oracle in an SAP environment

A clone database instance with the same version and name as the database instance on the production server must be installed on the clone server.

The user name and group name of the clone database instance owner on the clone system must be available on the clone server. The user ID (UID) and group ID (GID) can be different from the UID and GID of the production server database instance.

For cloning in Oracle environments, the database SID cannot contain lowercase letters. If the SID contains lowercase letters, the clone database is created, but the lowercase letters in the SID of the clone system are converted to capitalized letters.

All supported applications

To archive database log files and transfer database backups to Tivoli Storage Manager, the Data Protection clients must be installed and configured on the clone server. The Tivoli Storage Manager Data Protection clients version on the clone server must be the same level as on the production server.

Related reference:

“Backing up Oracle in an SAP environment databases” on page 87

Preparing a backup cluster in a DB2 pureScale environment

A backup cluster is a second DB2 pureScale instance that is contained within an independent GPFS cluster. Tivoli Storage FlashCopy Manager uses the backup cluster to send a snapshot of a DB2 pureScale database to Tivoli Storage Manager. A production cluster is the cluster that owns the file systems that contain the production DB2 pureScale instance and the production database.

Ensure that the topology of the production and backup cluster are the same. The backup cluster must have the same number of members with identical member numbers as the production cluster. This requirement does not apply to the cluster caching facility (CF) members. You can create multiple members that are known as logical members on the same host. Creating multiple logical members, can help reduce the number of hosts that are required for the backup cluster in comparison to the production cluster. For more information about configuring multiple members on the same host, see the IBM DB2(r) Knowledge Center.

Tivoli Storage FlashCopy Manager mounts the GPFS file systems that contain the snapshot backup on a backup cluster. To allow Tivoli Storage FlashCopy Manager to mount the file systems on the backup cluster, the system administrator issues the following commands:

- On the production cluster:
 - Issue the **mmauth add** command to authorize the backup cluster to mount one or more file systems of the database that is protected on the production cluster. Issue this command only once per cluster.

- Issue the **mmauth grant** command to grant permission to the backup cluster to mount the file systems of the database that are enabled for snapshot-based data protection. Issue this command only once per file system.
- On the backup cluster:
 - Issue the **mmremoteccluster add** command to add the production cluster to the backup cluster.

Note: The file systems must not already be mounted on the backup cluster or added to the backup cluster before a Tivoli Storage FlashCopy Manager backup to Tivoli Storage Manager or mount operation.

Preparing backup or cloning servers for applications running on VMware or KVM virtual machines

If a backup or clone server you are using is a VMware or KVM virtual machine, the storage device must be attached to the virtual machine with either iSCSI or Network file system.

Before you begin

If physical hosts are used as backup or clone servers, see “Installation prerequisites for backup and clone servers” on page 23.

Procedure

Verify that all target LUNs in backup or clone operations are attached to the virtual machine with one of the following attachment methods:

- iSCSI
- Network file system (NFS)

Storage solutions

Before you install and configure Tivoli Storage FlashCopy Manager software, review the storage solution setup. In an IBM DB2 pureScale environment, Tivoli Storage FlashCopy Manager is independent of the underlying storage that is used by the GPFS file system. Therefore, no additional configuration other than what is required by DB2 pureScale is necessary.

IBM XIV Storage System

When Tivoli Storage FlashCopy Manager creates a backup on an IBM XIV Storage System, a snapshot of all source volumes that belong to the protected application is created on the storage system. This snapshot is a space-efficient read-only copy of the application.

The storage device and its storage volumes must be accessible from either a storage area network (SAN) zone, network or both. During the Tivoli Storage FlashCopy Manager configuration process, if you set the **USE_WRITABLE_SNAPSHOTS** parameter to NO, the snapshots are not mounted directly on another host. Instead, Tivoli Storage FlashCopy Manager creates duplicates from the snapshots as part of the mount procedure, these duplicates are removed when the backup is unmounted. A duplicate is a space-efficient logical copy of the snapshot and this copy is writable.

The **USE_WRITABLE_SNAPSHOTS** parameter specifies whether writable snapshots can be used for mount or restore operations. If writable snapshots are used, no

duplicates are created during mount operations and all changes that are applied to the snapshot are preserved. Writable snapshots are only required in LVM mirroring environments. A typical IBM XIV Storage System profile entry is provided here:

```
>>>
DEVICE_CLASS                XIV01
COPYSERVICES_HARDWARE_TYPE  XIV
PATH_TO_XCLI                 path where XCLI is installed
COPYSERVICES_SERVERNAME     xiv_hostname
COPYSERVICES_USERNAME       admin
COPYSERVICES_REMOTE         YES
COPYSERVICES_PRIMARY_SERVERNAME xiv_hostname
COPYSERVICES_REMOTE_SERVERNAME xiv_remote_hostname
COPYSERVICES_REMOTE_USERNAME admin
USE_WRITABLE_SNAPSHOTS      AUTO
BACKUP_HOST_NAME             backup_host
<<<
```

To offload backups to Tivoli Storage Manager, Tivoli Storage FlashCopy Manager must be installed on a backup server. You must also configure the **TSM_BACKUP** profile parameter to YES and set the **BACKUP_HOST_NAME** profile parameter to the name of the hostname or cluster name as defined on the storage system.

Dependent software packages

Tivoli Storage FlashCopy Manager requires the IBM XIV Storage System command-line interface (XCLI) to be installed on all hosts, production, backup, or clone servers where Tivoli Storage FlashCopy Manager is installed.

Support for LVM mirroring (AIX only) and ASM failure groups

If AIX Logical Volume Manager (LVM) mirroring is used in the environment, Tivoli Storage FlashCopy Manager can create separate snapshots of either mirror. In an Oracle ASM environment, a snapshot of selected failure groups is created. However, there must be enough remaining failure groups to mount the corresponding disk group for this image to be created. Each mirror or failure group must be located on a different XIV Storage System.

In LVM mirroring environments, the use of writable snapshots is required. Tivoli Storage FlashCopy Manager uses IBM XIV Storage System capabilities to restore writable snapshots. For writable snapshots, a mount operation directly mounts the original snapshot to another host. All changes to the snapshot are preserved, and a subsequent mount or backup operation contains all changes that occurred to the snapshot while mounted. For more information about using writable snapshots, see information about the **USE_WRITABLE_SNAPSHOTS** parameter in “*DEVICE_CLASS device*” on page 171.

(AIX only) Support for virtual I/O

IBM XIV Storage System and Tivoli Storage FlashCopy Manager support virtual I/O with n-port ID virtualization. On the production server, Tivoli Storage FlashCopy Manager supports virtual I/O with N_Port ID Virtualization (NPIV) and Virtual I/O Server (VIOS). There is a one to one relationship between the virtual I/O logical volume and the storage LUN. On the backup server, Tivoli Storage FlashCopy Manager supports virtual I/O with NPIV only.

Remote access to snapshot backups

Tivoli Storage FlashCopy Manager allows mounting a backup image on another host. Unlike FlashCopy devices, Tivoli Storage FlashCopy Manager creates a duplicate from the snapshot, which is then mounted on the host. As the duplicate is effectively another image, changes to the duplicate are not reflected in the snapshot. As a result, the mounted image can be altered without affecting the backup image and any subsequent restore of that backup. Tivoli Storage FlashCopy Manager removes the duplicate during the unmount operation. All changes that were made on the duplicate are undone. A subsequent mount operation, presents the image as created when the snapshot occurred.

IBM System Storage N series and NetApp storage systems

When Tivoli Storage FlashCopy Manager creates backups on IBM System Storage N series and NetApp storage system, space efficient snapshots are created. The underlying storage can be network-attached storage (NAS) or storage area network (SAN). For Oracle with Automatic Storage Management (ASM), the underlying storage is storage area network (SAN) only.

In addition to creating snapshot backups you can also complete the following tasks:

- Offload backups to Tivoli Storage Manager by using an auxiliary or backup server.
- Restore data from DB2, Oracle, DB2 in an SAP environment, Oracle in an SAP environment, and custom applications snapshots.
- Create database clones, you cannot clone a custom application. For database cloning, a new independent volume is created from a snapshot. This new independent volume is similar to a complete copy. Database cloning is supported for SAN-attached storage only.

For SAN-attached storage, the production and backup servers must be connected by using Fibre Channel and TCP/IP. For NAS attached storage, the production and backup servers are connected by using TCP/IP only.

To offload backups to Tivoli Storage Manager, Tivoli Storage FlashCopy Manager must be installed on the backup server. You must also configure the **TSM_BACKUP** profile parameter to YES. In addition, you must set the **BACKUP_HOST_NAME** profile parameter to the name of the initiator group as defined on the storage system.

The following example shows a sample profile for IBM System Storage N series and NetApp storage solutions with SAN-attached storage:

```
>>>
DEVICE_CLASS          N6240
COPYSERVICES_HARDWARE_TYPE SAN_NSERIES
COPYSERVICES_SERVERNAME n6240_hostname
COPYSERVICES_USERNAME  root
BACKUP_HOST_NAME       backup_host
<<<
```

The following profile example, shows the same storage solutions but with NAS attached storage:

```
>>>
DEVICE_CLASS          N6240
COPYSERVICES_HARDWARE_TYPE NAS_NSERIES
```

```
COPYSERVICES_SERVERNAME    n6240_hostname
COPYSERVICES_USERNAME      root
BACKUP_HOST_NAME            backup_host
<<<
```

Support for LVM mirroring (AIX only) and ASM failure groups

If AIX Logical Volume Manager (LVM) mirroring is used in the environment, Tivoli Storage FlashCopy Manager can create separate snapshots of either mirror. In an Oracle ASM environment, a snapshot of selected failure groups is created. However, there must be enough remaining failure groups to mount the corresponding disk group for this image to be created. Each mirror or failure group must be located in a different N series or NetApp Storage System.

Support for virtual I/O (AIX only)

IBM System Storage N series or NetApp storage solutions and Tivoli Storage FlashCopy Manager supports a virtual I/O with n-port ID virtualization. On the production server, Tivoli Storage FlashCopy Manager supports virtual I/O with N_Port ID Virtualization (NPIV) and Virtual I/O Server (VIOS). There is a one to one relationship between the virtual I/O logical volume and the storage LUN. On the backup server, Tivoli Storage FlashCopy Manager supports virtual I/O with NPIV only.

Remote access to snapshot backups

Tivoli Storage FlashCopy Manager allows mounting a backup image on another host. Unlike FlashCopy devices, Tivoli Storage FlashCopy Manager creates a duplicate from the snapshot, which is then mounted on the host. As the duplicate is effectively another image, changes to the duplicate are not reflected in the snapshot. As a result, the mounted image can be altered without affecting the backup image and any subsequent restore of that backup. Tivoli Storage FlashCopy Manager removes the duplicate during the unmount operation. All changes that were made on the duplicate are undone. A subsequent mount presents the image as created when the snapshot occurred.

SAN Volume Controller, DS8000, and Storwize family

IBM Tivoli Storage FlashCopy Manager can restore point-in-time copies from backups on SAN Volume Controller 6.1, or later and Storwize family storage systems. For the DS8000 storage system, it is not possible to restore point-in-time copies when you set the **FLASHCOPY_TYPE** parameter to **NOCOPY** in the Tivoli Storage FlashCopy Manager profile file.

You can mount images on a remote server and back up the images to Tivoli Storage Manager when you use DS8000, SAN Volume Controller 6.1 or later, and Storwize family storage systems.

CIM server

Starting with DS8000 R4.1 the Common Information Model (CIM) server is embedded with the storage device. It is not necessary to install and configure the CIM server separately. For earlier releases of DS8000, a proxy CIM server is required and must be configured to manage the necessary storage clusters. For more information about configuring a proxy CIM server, see the DS8000 documentation.

Tivoli Storage FlashCopy Manager supports Storwize family and SAN Volume Controller, Version 6.1 and later with an embedded CIM server.

Unlike IBM XIV[®] Storage Systems, Tivoli Storage FlashCopy Manager requires that FlashCopy backup target volumes be created in advance on SAN Volume Controller, Storwize family, and DS8000. To provide a target set definition to Tivoli Storage FlashCopy Manager, organize target volumes into target sets, where each target set represents one backup generation. Tivoli Storage FlashCopy Manager automatically matches source volumes to suitable target volumes. However, each target set must contain at least one suitable target volume for each source volume to be backed up. Additional target volumes in a target set are allowed, but these target volumes are ignored.

Support for LVM mirroring (AIX only) and ASM failure groups

If AIX Logical Volume Manager (LVM) mirroring is used in the environment, Tivoli Storage FlashCopy Manager can create separate FlashCopy images of either mirror. In an Oracle Automatic Storage Management (ASM) environment, a FlashCopy image of selected failure groups is created. However, there must be enough remaining failure groups to mount the corresponding disk group for this image to be created. Each mirror or failure group must be located in a different storage system.

DS8000 allows one incremental FlashCopy per source volume. When production volumes are mirrored by using Logical Volume Manager (LVM) mirroring or ASM failure groups, only one FlashCopy backup of this type per volume mirror is created. For incremental snapshots with DS8000 storage, only one target set can be specified in the target volumes file (.fct).

Support for virtual I/O (AIX only)

DS8000, SAN Volume Controller, and Storwize family logical unit numbers (LUNs) can be attached to a host directly or by using Virtual I/O (VIO). Both setups are supported, when there is a 1-1 relation between VIO logical volumes and storage LUNs on the storage subsystem.

A VIO is a logical partition (LPAR) on a pSeries system that is controlled by the IBM Hardware Management Console (HMC) or IBM Integrated Virtualization Manager (IVM). It owns the hardware adapters and allows access for other logical partitions. This feature allows the device to be shared. The LPAR associated with the resources is the VIO Server and the logical partitions that use it are VIO Clients. For example, they can share one disk on the VIO Server instead of rebooting each logical partition from a Small Computer System Interface (SCSI) adapter and SCSI disk. This function eliminates the number of required adapters, adapter slots, and disks.

Tivoli Storage FlashCopy Manager uses virtual SCSI adapters to map disks from a VIO to a client LPAR. Physical volumes are required to be mapped from the VIO to the client. However, mapping logical volumes or storage pools is not supported. On the production server, Tivoli Storage FlashCopy Manager supports virtual I/O with N_Port ID Virtualization (NPIV) and Virtual I/O Server (VIOS). There is a one to one relationship between the virtual I/O logical volume and the storage LUN. On the backup server, Tivoli Storage FlashCopy Manager supports virtual I/O with NPIV. In addition, VIOS is supported when you configure the **BACKUP_HOST_NAME** parameter to use the **PREASSIGNED_VOLUMES** in the Tivoli Storage FlashCopy Manager profile file.

More details about supported combinations of operating system and storage subsystem levels, are available in the Pre-installation Checklist that is available at this URL <https://www.ibm.com/support/docview.wss?uid=swg21427692>. From this technote, select the required software version and then select the required component link. The hardware and software requirement page contains the Pre-installation Checklist and an installation planning worksheet.

Remote access to FlashCopy images

Tivoli Storage FlashCopy Manager allows mounting a FlashCopy backup image to another host. This image is writable and any changes that are made on that image are reflected in the backup and are included in the subsequent restore.

Related information:

 <https://www.ibm.com/support/docview.wss?uid=swg21427692>

Space-efficient multi-target FlashCopy on SAN Volume Controller and Storwize family

Space-efficient targets that are part of a multi-target FlashCopy cascade might be deleted by SAN Volume Controller and Storwize family if other targets of the same cascade are restored or overwritten by a new snapshot.

In a SAN Volume Controller or a Storwize family environment, the following situations might cause space-efficient targets to be deleted:

Backup operations and cloning operations

A Tivoli Storage FlashCopy Manager backup operation uses the oldest target set that is available for the specified **DEVICE_CLASS**. However, that target set might not be the oldest target set that is associated with the source volumes. This scenario is possible when more than one **DEVICE_CLASS** is specified in the Tivoli Storage FlashCopy Manager profile. When the FlashCopy backup that is available on the target set is not the oldest backup, then the older backups are deleted during the backup operation. The oldest target set is the set that is used for the oldest FlashCopy backup in a multiple target set configuration. This situation can also happen when a new FlashCopy cloning operation is started with the force option (-F).

Restore operation

A Tivoli Storage FlashCopy Manager restore operation deletes any FlashCopy backups that are newer than the backup that is being restored. In addition, the backup that is restored with the current operation can also be deleted.

Target volume storage space exceeded

When the available storage capacity of a space-efficient FlashCopy target volume is exceeded, the target volume is taken offline. The data on the target volume that is taken offline is deleted.

SAN Volume Controller and Storwize family

When you use SAN Volume Controller and Storwize family, Tivoli Storage FlashCopy Manager software can restore FlashCopy backups before completion of a background copy.

When you restore FlashCopy backups before completion of a background copy, space-efficient volumes can be enabled as backup targets. The background copy rate is set to zero to prevent the FlashCopy target from becoming fully allocated. When you use either SAN Volume Controller or Storwize family, and Tivoli Storage FlashCopy Manager software in this scenario, use the following guidelines for the environment:

Physical capacity

The physically allocated capacity of a space-efficient target volume must be large enough to contain all changes that occur to your production environment. Specifically, all changes that occur between the current and the subsequent backup. If the capacity is insufficient, the target volume goes offline and the corresponding backup becomes invalid.

SAN Volume Controller and Storwize family support the creation of automatically expanding target volumes. If you create target volumes that automatically expand, more storage is assigned to the target when storage capacity decreases. This additional storage ensures that sufficient capacity is available.

FlashCopy relationships

During a restore, Tivoli Storage FlashCopy Manager software stops FlashCopy relationships. These relationships include relationships that are established at the time when the backup is created to any subsequent relationships that are created on the same source LUN. All backups to space-efficient targets that are newer than the backup used for restore, and the backup from which you are restoring, are deleted. If the background copy was not completed, the same restriction applies to full and incremental FlashCopy backups.

To check whether a backup is going to be deleted, query the usability state of Tivoli Storage FlashCopy Manager backups. If the backup is going to be deleted, during the restore process, the `DESTRUCTIVELY_RESTORABLE` state is set. Otherwise, the state is set to `REPETITIVELY_RESTORABLE`.

Target sets

Tivoli Storage FlashCopy Manager cannot reuse a target set for a new FlashCopy backup unless it corresponds to the last FlashCopy mapping in a cascaded FlashCopy relationship. This scenario implies that when Tivoli Storage FlashCopy Manager reuses a target set, all backups that are created before this point in time are deleted. In a non-mirrored environment, all backups that are created before this point in time are deleted when the following conditions are met:

- The same profile for the Tivoli Storage FlashCopy Manager backups is used.
- This profile contains only one **DEVICE_CLASS** statement in the `CLIENT` section.

In a mirrored environment, all backups that are created before this point in time are deleted when the `CLIENT` section of the profile contains one **DEVICE_CLASS** statement for each LVM mirror. If multiple device classes are specified within this statement, each device class must manage the same number of target sets.

Recommendations for setting up the environment

When you set up the SAN Volume Controller and Storwize family environments for use with Tivoli Storage FlashCopy Manager software, the following list identifies guidelines for the environment:

- Do not use space-efficient volumes as source volumes.
- Decide whether you want to use space-efficient or fully allocated backup targets. In mirrored environments, a different choice can be made for each mirror.
- For each mirror, use one **DEVICE_CLASS** statement for disk-only backups. In addition, use one **DEVICE_CLASS** statement for dual backups. A dual backup is a disk backup and tape backup. Make sure that the schedule is defined so that the target sets are reused cyclically across both device classes per mirror.

For example:

- Define three target sets in the **DISK_ONLY** device class. Schedule these disk only backups to occur at 6:00, 12:00, and 18:00.
- Define one target set in a **DUAL_BACKUP** device class. Set this schedule to create a disk and Tivoli Storage Manager backup at 00:15.

If you retain only one target set generation for dual backups, do not specify six target sets to retain disk only backups (created at 6:00, 12:00, and 18:00) for two days. The second dual backup operation attempts to reuse the target set of the previous dual backup. If the version policy specifies ADAPTIVE, this action results in a deletion of all disk-only backups that are taken before that point in time. Otherwise, the version policy causes the dual backup to fail if **retain** specifies seven versions.

- If a backup that is characterized as DESTRUCTIVELY_RESTORABLE is restored, the backup you are restoring and all backups that are taken after that point in time are deleted. The backup is not deleted when the backup is created with FLASHCOPY_TYPE FULL or INCR, and the background copy completed.

Remote mirror integration

When you use storage solutions with mirror technologies and Tivoli Storage FlashCopy Manager, there are steps to complete for integrating backup and restore operations. For IBM System Storage SAN Volume Controller, mirror technologies are labeled Global Mirror and Metro Mirror. For IBM XIV Storage System, mirror technologies are labeled Synchronous Remote Mirroring and Asynchronous Remote Mirroring.

SAN Volume Controller

Tivoli Storage FlashCopy Manager can back up application data consistently on SAN Volume Controller storage solutions with volumes that are simultaneously used as Metro Mirror or Global Mirror sources. You can configure either the sources or the targets of the Remote Mirror to be selected as the sources for the FlashCopy backup. For environments with a SAN Volume Controller version 6.1 and earlier, Tivoli Storage FlashCopy Manager must stop and deactivate the Global Mirror or Metro Mirror before you run a restore operation. In addition, do not use FlashCopy targets as Global Mirror or Metro Mirror sources.

IBM System Storage DS8000

Tivoli Storage FlashCopy Manager can back up DS8000 storage solutions with volumes that are simultaneously used as Global Mirror or Metro Mirror sources. In contrast to SAN Volume Controller, you can configure only the sources of the Global Mirror or Metro Mirror to be selected as the

sources of the FlashCopy backup. When you use Tivoli Storage FlashCopy Manager in this environment, do not use FlashCopy targets as Global Mirror and Metro Mirror sources.

IBM XIV Storage System

Tivoli Storage FlashCopy Manager can back up application data consistently on XIV system storage solutions with volumes that are simultaneously used as Synchronous Remote Mirroring or Asynchronous Remote Mirroring sources. You can configure either the sources or the targets of the Remote Mirror to be selected as the sources for the FlashCopy backup.

For all storage solutions that use mirror technologies, when you use Tivoli Storage FlashCopy Manager, the following list describes the environment. If the environment setup differs from this description, Tivoli Storage FlashCopy Manager might not work as expected.

- The connectivity state must be online.
- The cluster partnership between the primary and secondary clusters must be configured before you use Tivoli Storage FlashCopy Manager. The following list identifies what you must configure when you are setting up the cluster partnership:
 - Tivoli Storage FlashCopy Manager is installed on the production and backup host on the local site (primary cluster).
 - Tivoli Storage FlashCopy Manager is installed on all systems, including the takeover and standby servers, running at the remote site (secondary cluster).
 - The local site contains the primary storage cluster for the production hosts. The primary cluster has data that is replicated to a secondary cluster on the remote site or to the same cluster.
 - For intersystem copying, the remote site contains the mirror volumes in another storage cluster. In addition, the remote site also hosts the takeover and standby servers.
 - SAN Volume Controller supports both intrasystem and intersystem Metro and Global Mirror.
 - For XIV system Synchronous Remote Mirroring and Asynchronous Remote Mirroring, configure either the source or the targets as a source for the snapshot backup.
- Tivoli Storage FlashCopy Manager uses a consistency group on the SAN Volume Controller and XIV system storage solutions for the FlashCopy or snapshot. A consistency group is a group of volumes that are associated with a FlashCopy pair. A FlashCopy pair is a group of two corresponding instant copies of data, that is, point-in-time copies of a volume. For the FlashCopy pair, the logically related data must be kept consistent across the volumes. The FlashCopy consistency group can be used for a consistent point-in-time copy for an application or database that spans multiple volumes. The following list identifies more information about using consistency groups with Tivoli Storage FlashCopy Manager:

SAN Volume Controller

- A consistency group contains a list of FlashCopy or Remote Copy relationships.
- The Tivoli Storage FlashCopy Manager software creates a FlashCopy consistency group on the secondary site to build a consistency unit between the source and target of the FlashCopy.

- You must define the consistency group for the mirror relationships between the master and auxiliary virtual disks.
- For Metro and Global Mirror, the state of the consistency group must be consistently synchronized.

XIV system

- The operational state of mirror must be operational.
- A consistency group contains a list of volumes.
- A consistency group that contains all of the remote copy target volumes must exist before starting the snapshot on the remote system. Apply the storage commands to the consistency group to simplify management.
- The mirror relationship between the master and slave volumes must be defined in the consistency group.
The master is where source volumes are located for the remote replication. The slave is where target volumes are located.
- For XIV system synchronous mirroring, the state of the consistency group must be consistently synchronized.
- For XIV system asynchronous mirroring, the state of the consistency group must be RPO_OK.
- For Metro Mirror and Synchronous Remote Mirroring, the write operation is committed to the host after the data is written to both the source and target volumes.
- For Global Mirror and Asynchronous Remote Mirroring, the write operation is committed to the host immediately after the data is written to the source volume.
- In terms of master and slave sites, the master site is where source volumes are located for the remote replication. The slave site is where target volumes are located. When a disaster occurs or when maintenance is necessary, the roles of master site and slave site can be changed.

The following figure illustrates the hosts and volumes that are involved in remote mirroring that uses Metro and Global mirrors.

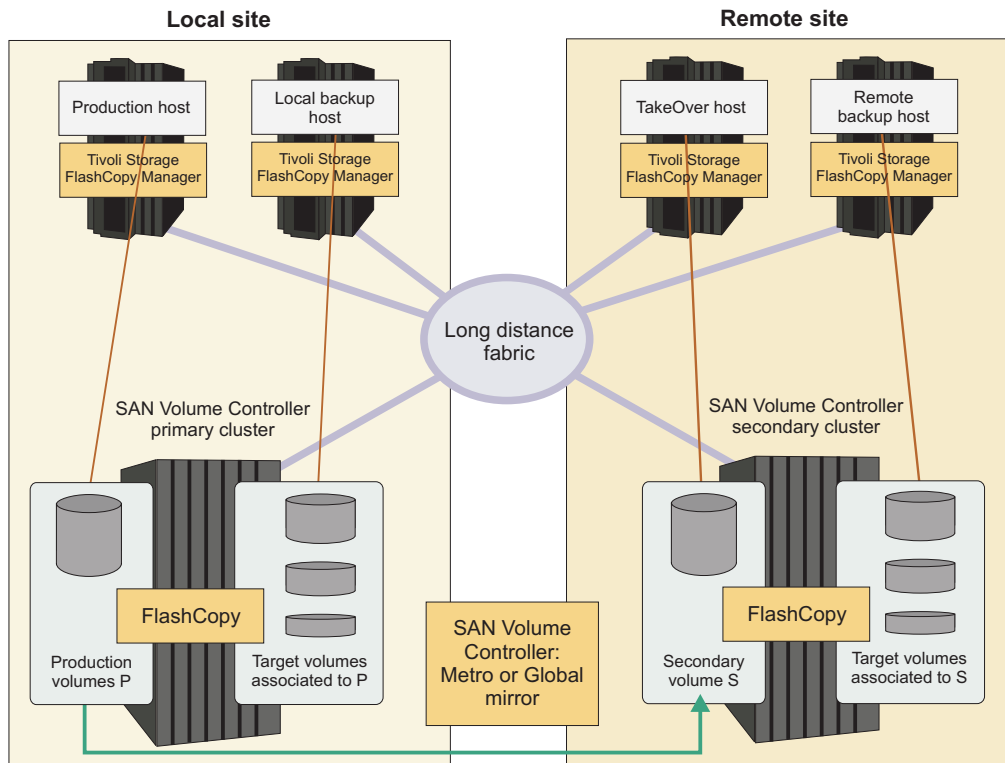


Figure 6. Remote mirroring using Metro Mirror and Global Mirror sources

Reconciliation of backups

Reconciliation is the process where Tivoli Storage FlashCopy Manager periodically verifies that backups on the storage system are valid.

Depending on the storage system, FlashCopy or snapshot backups can be deleted, withdrawn, or stopped by certain operations on the storage system. When these events occur, it invalidates the FlashCopy or snapshot backup. During reconciliation FlashCopy or snapshots backups that are no longer present or are invalid on the storage system are removed from Tivoli Storage FlashCopy Manager repository.

The reconciliation process removes Tivoli Storage FlashCopy Manager backups when the following events take place on storage systems:

All storage systems

Manual intervention causes the following events to occur:

- The source volume or target volume relationship is withdrawn.
- The snapshot or FlashCopy is deleted.
- The FlashCopy mappings are stopped.

IBM XIV Storage System

When there is no available space for snapshot backups, the XIV system Storage System deletes old snapshots to free space for new snapshots.

IBM System Storage N series and NetApp storage systems

When either of the following events occur:

- When there is no available space for snapshot backups, both of these storage systems delete old snapshots to free space for new snapshots.

- When a snapshot backup becomes invalid, because it was created after the creation of the original backup that was later restored.

IBM System Storage SAN Volume Controller and IBM Storwize family storage systems

When either of the following events occur:

- When a FlashCopy backup becomes invalid, because it was created after the creation of the original backup that was later restored. This issue applies to backups with space efficient target volumes or if the background copy process is not yet finished. In addition, the backup that is subject to restore can also be invalidated by the storage system.
- In this environment FlashCopy mappings of target volumes are used by the storage system for FlashCopy backups. When used in a specific FlashCopy backup, then previous FlashCopy backups can become invalid if they were dependent on the same mapping. This issue applies to backups with space efficient target volumes or if the background copy process is not yet finished.

IBM System Storage DS8000

When a source target relationship is withdrawn. This process cannot happen automatically in this environment.

Chapter 3. Installing and upgrading

Installation of Tivoli Storage FlashCopy Manager includes the following steps: installation, activation, and configuration. You must install Tivoli Storage FlashCopy Manager on the production server. Depending on your environment, a separate installation of Tivoli Storage FlashCopy Manager can be required on a backup or clone server. You can upgrade your system from a previous version of Tivoli Storage FlashCopy Manager to version 4.1.1.

About this task

When you are installing Tivoli Storage FlashCopy Manager software, the installation process varies, depending on the environment.

The following set of tasks must be completed during the installation process:

- Install Tivoli Storage FlashCopy Manager on the production server. The production server is where Tivoli Storage FlashCopy Manager protects critical business applications by providing a method to back up and restore these applications.
- Activate the applications that you want to protect with Tivoli Storage FlashCopy Manager. During the activation all the necessary files are copied from the installation directory (FCM_INSTALL_DIR) to the application-specific installation directory (INSTANCE_DIR). The installation directory is referred to as the FCM_INSTALL_DIR directory and the application-specific installation directory is referred to as INSTANCE_DIR directory. The default location for the FCM_INSTALL_DIR directory is:
 - AIX: /usr/tivoli/tsfcm/acs_4.1.1
 - Linux: /opt/tivoli/tsfcm/acs_4.1.1
 - Solaris: /opt/tivoli/tsfcm/acs_4.1.1
 - HP-UX: /opt/tivoli/tsfcm/acs_4.1.1

Note: Only instances that are selected during installation are activated.

- Configure Tivoli Storage FlashCopy Manager.

The following files and directories are created during the configuration process:

- An ACS_DIR configuration directory, if the ACS_DIR directory is not identical to the INSTANCE_DIR directory. The path for the ACS_DIR directory is specified in the Tivoli Storage FlashCopy Manager profile file.
- A profile file within the ACS_DIR configuration directory.
- A symbolic link is created from the INSTANCE_DIR/profile file that points to the ACS_DIR/profile file when the two directories are not identical.
- A password file within ACS_DIR/shared directory.
- An entry /etc/inittab for daemon processes if requested.

For Red Hat Enterprise Linux 6, the daemon processes are started automatically by using the upstart program when requested.

- Install Tivoli Storage FlashCopy Manager on a backup or clone server, if not automatically installed and configured. Backup servers or clone servers are auxiliary hosts that are required by Tivoli Storage FlashCopy Manager to mount backup images and clone databases. A backup or clone server also is required to offload backups to IBM Tivoli Storage Manager.

If Open Secure Shell (OpenSSH) is configured between the production and the backup or clone servers, Tivoli Storage FlashCopy Manager is installed and configured automatically. Otherwise, a separate installation on a backup or clone server is required.

Installing on the production server

To install Tivoli Storage FlashCopy Manager on the production server, you can use the graphical installation wizard, the console wizard, or the console in silent mode.

Before you begin

For the current requirements, review the *Hardware and Software Requirements* technote that is associated with the Tivoli Storage FlashCopy Manager release. This technote is available in the *Tivoli Storage FlashCopy Manager - All Requirement Documents* website at: <https://www.ibm.com/support/docview.wss?uid=swg21427692>. Follow the link to the requirements technote for your specific release or update level and review the pre-installation checklist and planning worksheet.

Tivoli Storage FlashCopy Manager installation packages are delivered as individual files. They are provided on an installation DVD or from an image that is downloaded from IBM Passport Advantage®. These files use the following name format:

`4.1.1-TIV-TSFCM-OS-platform.bin`

For the *OS-platform* variable, the following list identifies valid options:

- AIX
- Linux
- Solaris
- HP/UX

Before you install, ensure that the installation planning worksheet is completed as this information is required during the installation.

Procedure

To install Tivoli Storage FlashCopy Manager on the production server, complete the following steps.

1. Log on to the production server and use the root user ID. Change to the directory where you downloaded the package file or insert the DVD into the DVD drive. Use one of the following methods to start the installation:

Graphical user interface with the installation wizard

The installation wizard requires a graphical X Window System installation. Make sure the environment variable *DISPLAY* specifies *host:display*, where *host* identifies the host name of the X Server to be contacted and *display* is the display number. To use the graphical installation wizard, from the command line, enter this command:

`./4.1.1-TIV-TSFCM-OS-platform.bin`

If the graphical X Window System is not present, the installation continues in console mode.

Console mode

To install in console mode, from the command line, enter this command:

```
./4.1.1-TIV-TSFCM-OS-platform.bin -i console
```

2. Follow the prompts to install Tivoli Storage FlashCopy Manager.

Note: During the installation, you are prompted to activate the database or database instances. Depending on your database application, complete one of the following steps:

- Select one or more DB2 instances.
 - Enter the Oracle database instance home directory.
3. On the Summary page, review your installation settings. If an error occurs during the installation process, correct the errors and restart the installation procedure. Tivoli Storage FlashCopy Manager creates an `installation.log` file in the `FCM_INSTALL_DIR` directory. You can use the log file to troubleshoot installation errors.

What to do next

After the installation, you must configure the application and database instances to complete the installation.

During the installation, you select the database instances or custom applications to activate. For all instances selected, the installer copies all the necessary files from the installation directory (`FCM_INSTALL_DIR`) to a database or application instance-specific installation directory (`INSTANCE_DIR`). The correct access rights for the directories are assigned.

To activate any additional instances or custom applications that were not selected during the installation, complete the following steps:

1. Log in to the production server and use the root user ID. Change to the `FCM_INSTALL_DIR` directory.
2. Run the appropriate command to activate the database or custom application instance:

```
DB2    ./setup_db2.sh -a install -d DB2_instance_owner_${HOME_directory}/  
sqllib/
```

Oracle in an SAP environment

```
./setup_ora.sh -a install -d  
Oracle_instance_owner_${HOME_directory}
```

```
Oracle ./setup_ora.sh -a install -d  
Oracle_instance_owner_${HOME_directory}
```

If the home directory of the database instance owner is not identical to the database instance directory, install in the database instance directory. For example, `$ORACLE_HOME`. For installations where `$ORACLE_HOME` is shared between multiple database instances, any other directory that is unique to this instance can be used.

Custom applications

The default installation directory is `$HOME/acs`. `$HOME` is the home directory of the application backup user. The following command creates the `$HOME/acs` directory:

```
./setup_gen.sh -a install -d Application_owner_${HOME_directory}
```

Related tasks:

Chapter 4, “Configuring Tivoli Storage FlashCopy Manager,” on page 53

Installing separately on backup or clone servers

If Tivoli Storage FlashCopy Manager is not installed remotely on the backup or clone server by using OpenSSH, use the following instructions to install Tivoli Storage FlashCopy Manager on a backup or clone server.

Before you begin

If a setup using OpenSSH is not possible, install Tivoli Storage FlashCopy Manager software separately on the backup or clone server:

Information about when a backup server or clone server is needed is available at “Preparing backup and cloning servers” on page 21.

Tip: If you are using self-assigned certificates you must manually copy the .arm file from the production server to the auxiliary server INSTANCE_DIR.

Procedure

To install Tivoli Storage FlashCopy Manager on the backup or clone server, complete the following steps:

1. Log on to the server and use the root user ID. Change to the directory where you downloaded the package file or insert the DVD into the DVD drive. Use one of the following methods to start the installation:

Graphical user interface with the installation wizard

The installation wizard requires a graphical X Window System installation. Make sure the environment variable *DISPLAY* specifies host:display, where host identifies the host name of the X Server to be contacted and display is the display number. To use the graphical installation wizard, from the command line, enter this command:

```
./4.1.1-TIV-TSFCM-OS-platform.bin
```

If the graphical X Window System is not present, the installation continues in console mode.

Console mode

To install in console mode, from the command line, enter this command:

```
./4.1.1-TIV-TSFCM-OS-platform.bin -i console
```

2. Follow the prompts to install Tivoli Storage FlashCopy Manager.

Note: During the installation, you are prompted to activate the database or database instances. Depending on your database application, complete one of the following steps:

- Select one or more DB2 instances.
- Enter the Oracle database instance home directory.

3. On the Summary page, review your installation settings. If an error occurs during the installation process, correct the errors and restart the installation procedure. Tivoli Storage FlashCopy Manager creates an *installation.log* file in the FCM_INSTALL_DIR directory. You can use the log file to troubleshoot installation errors.

What to do next

After the installation and activation are completed, you must configure Tivoli Storage FlashCopy Manager for use with your environment.

Related tasks:

Chapter 4, “Configuring Tivoli Storage FlashCopy Manager,” on page 53

Installing in silent mode

To install Tivoli Storage FlashCopy Manager in silent mode you require a response or properties file.

About this task

You can generate a properties file during installation in either graphic or console mode by starting the executable file as follows:

```
./4.1.1-TIV-TSFCM-platform.bin [-i console]  
-DRECORDFILE=/tmp/installer.properties
```

Procedure

1. To install in silent mode, create the response or 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:

- AIX: `/usr/tivoli/tsfcm/acs_4.1.1`
- Linux: `/opt/tivoli/tsfcm/acs_4.1.1`
- Solaris: `/opt/tivoli/tsfcm/acs_4.1.1`
- HP-UX: `/opt/tivoli/tsfcm/acs_4.1.1`

- b. To create a log file during installation, set the variable:

```
INSTALL_LOG_DESTINATION=installation_directory/log_file_name
```

- c. Set the variable for the license file:

```
LICENSE_ACCEPTED=TRUE
```

- d. To define the product database component that is installed, set the following variable:

```
CHOSEN_INSTALL_SET=InstallSet
```

where *InstallSet* is

```
TSMFCMORA (Oracle component)  
TSMFCMSAP (SAP with Oracle component)  
TSMFCMDB2 (DB2 component)  
TSMFCMGEN (Custom application agent component)
```

- e. (Oracle and Oracle in an SAP environment) To set the home folder of the Oracle *SID*, use the following variable:

```
ORACLE_HOME_FOLDER=/oracle/SID
```

- f. (DB2): To copy the required files directly to desired DB2 instances after installing in the main installation directory, set the following variable with a comma-separated list of existing 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 and the `-f` option to specify the properties file:

```
./version-TIV-TSFCM-OS-platform.bin -i silent -f properties_file
```

The *properties_file* specification must contain a full path.

Results

Sample properties file (DB2)

```
# Properties file for Tivoli Storage FlashCopy® Manager Installations
# Created on: May 8, 2014 4:18:38 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=TSMFCMDB2

# Installation Directory
# -----
USER_INSTALL_DIR=/usr/tivoli/tsfcm/acs_4.1.1

# 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

# Linux Distribution
# This can either be SLES10, SLES11, RHEL5 or RHEL6
LINUX_DISTRO=SLES11
```

Sample properties file (Oracle)

```
# Properties file for Tivoli Storage FlashCopy® Manager Installations
# Created on: May 6, 2013 10:45:09 AM
# 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=TSMFCMORA

# Installation Directory
# -----
USER_INSTALL_DIR=/usr/tivoli/tsfcm/acs_4.1.1

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

```
# Linux Distribution
# This can either be SLES10, SLES11, RHEL5 or RHEL6
LINUX_DISTRO=SLES11
```

Sample properties file for Oracle in an SAP environment

```
# Properties file for Tivoli Storage FlashCopy® Manager Installations
# Created on: May 11, 2013 1:02:55 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=TSMFCMSAP

# Installation Directory
# -----
USER_INSTALL_DIR=/usr/tivoli/tsfcm/acs_4.1.1

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

# Selected IBM DB2 Instances
# -----

# Linux Distribution
# This can either be SLES10, SLES11, RHEL5 or RHEL6
LINUX_DISTRO=SLES11
```

Sample properties file for FlashCopy Manager for Custom Applications

The following sample is the properties file for FlashCopy Manager for Custom Applications on a Linux system.

```
LICENSE_ACCEPTED=TRUE
CHOSEN_INSTALL_SET=TSMFCMGEN
USER_INSTALL_DIR=/opt/tivoli/tsfcm/acs_4.1.1
#ORACLE_HOME_FOLDER=
#DB2_INSTANCES_SELECTED=
LINUX_DISTRO=SLES11, RHEL5 or RHEL6
```

Lines starting with the # character are treated as comments.

Related tasks:

Chapter 4, “Configuring Tivoli Storage FlashCopy Manager,” on page 53

Upgrading

Use the Tivoli Storage FlashCopy Manager installation program to upgrade your current Tivoli Storage FlashCopy Manager version to Version 4.1.1.

Before you begin

For the current requirements, review the *Hardware and Software Requirements* technote that is associated with the Tivoli Storage FlashCopy Manager release. This technote is available in the *Tivoli Storage FlashCopy Manager - All Requirement Documents* website at: <https://www.ibm.com/support/>

docview.wss?uid=swg21427692. Follow the link to the requirements technote for your specific release or update level and review the pre-installation checklist and planning worksheet.

Tivoli Storage FlashCopy Manager installation packages are delivered as individual files. They are provided on an installation DVD or from an image that is downloaded from IBM Passport Advantage. These files use the following name format:

4.1.1-TIV-TSFCM-OS-*platform*.bin

For the *OS-platform* variable, the following list identifies valid options:

- AIX
- Linux
- Solaris
- HPUX

Uninstall the current version of Tivoli Storage FlashCopy Manager on every server where you want to upgrade Tivoli Storage FlashCopy Manager.

1. Log on to the server and use the root user ID.
2. Determine the installation path of the current version of Tivoli Storage FlashCopy Manager. The following paths provide the default location of the installation files:
 - For AIX operating systems: /usr/tivoli/tsfcm/acs_version_number.
 - For Linux, Solaris, and HP-UX operating systems: /opt/tivoli/tsfcm/acs_version_number.
3. Run the appropriate command for your operating system from the installation path:
 - For AIX operating systems: /usr/tivoli/tsfcm/acs_version_number/uninstall/uninstaller.bin.
 - For Linux, Solaris, and HP-UX operating systems: /opt/tivoli/tsfcm/acs_version_number/uninstall/uninstaller.bin.

Note: Only global installation files are removed. The database instances remain activated with your current version of Tivoli Storage FlashCopy Manager.

Procedure

To install Tivoli Storage FlashCopy Manager on the production server, complete the following steps.

1. Log on to the production server and use the root user ID. Change to the directory where you downloaded the package file or insert the DVD into the DVD drive. Use one of the following methods to start the installation:

Graphical user interface with the installation wizard

The installation wizard requires a graphical X Window System installation. Make sure the environment variable *DISPLAY* specifies host:display, where host identifies the host name of the X Server to be contacted and display is the display number. To use the graphical installation wizard, from the command line, enter this command:

```
./4.1.1-TIV-TSFCM-OS-platform.bin
```

If the graphical X Window System is not present, the installation continues in console mode.

Console mode

To install in console mode, from the command line, enter this command:

```
./4.1.1-TIV-TSFCM-OS-platform.bin -i console
```

2. Follow the prompts to install Tivoli Storage FlashCopy Manager.

Note: During the installation, you are prompted to activate the database or database instances. Depending on your database application, complete one of the following steps:

- Select one or more DB2 instances.
 - Enter the Oracle database instance home directory.
3. On the Summary page, review your installation settings. If an error occurs during the installation process, correct the errors and restart the installation procedure. Tivoli Storage FlashCopy Manager creates an `installation.log` file in the `FCM_INSTALL_DIR` directory. You can use the log file to troubleshoot installation errors.

What to do next

During the installation, you select the database instances or custom applications to activate. For all instances selected, the installer copies all the necessary files from the installation directory (`FCM_INSTALL_DIR`) to a database or application instance-specific installation directory (`INSTANCE_DIR`). The correct access rights for the directories are assigned.

To activate any additional instances or custom applications that were not selected during the installation, complete the following steps:

1. Log in to the production server and use the root user ID. Change to the `FCM_INSTALL_DIR` directory.
2. Run the appropriate command to activate the database or custom application instance:

```
DB2    ./setup_db2.sh -a install -d DB2_instance_owner_${HOME_directory}/  
       sqllib/
```

Oracle in an SAP environment

```
./setup_ora.sh -a install -d  
Oracle_instance_owner_${HOME_directory}
```

```
Oracle ./setup_ora.sh -a install -d  
Oracle_instance_owner_${HOME_directory}
```

If the home directory of the database instance owner is not identical to the database instance directory, install in the database instance directory. For example, `$ORACLE_HOME`. For installations where `$ORACLE_HOME` is shared between multiple database instances, any other directory that is unique to this instance can be used.

Custom applications

The default installation directory is `$HOME/acs`. `$HOME` is the home directory of the application backup user. The following command creates the `$HOME/acs` directory:

```
./setup_gen.sh -a install -d Application_owner_${HOME_directory}
```

Related tasks:

Chapter 4, “Configuring Tivoli Storage FlashCopy Manager,” on page 53

Migrating existing snapshot data

You can upgrade to IBM Tivoli Storage FlashCopy Manager and migrate data from Tivoli Storage Manager for Advanced Copy Services.

Migration from Tivoli Storage Manager for Advanced Copy Services to Tivoli Storage FlashCopy Manager on an IBM XIV Storage System

For the IBM XIV Storage System, Tivoli Storage FlashCopy Manager retains the configuration and backup history of an existing Tivoli Storage Manager for Advanced Copy Services installation. The backups that are created separately for each instance with Tivoli Storage Manager for Advanced Copy Services can be restored with Tivoli Storage FlashCopy Manager.

The upgrade from Tivoli Storage Manager for Advanced Copy Services to Tivoli Storage FlashCopy Manager, uses the Tivoli Storage FlashCopy Manager installation program. During the installation, select the database instances to activate.

To upgrade dedicated database instances after you install Tivoli Storage FlashCopy Manager, run the setup utility separately and use the root user ID. Start the installation setup script as the database instance owner from the `INSTANCE_DIR` directory. This task updates the current configuration file and Tivoli Storage FlashCopy Manager can use the Tivoli Storage Manager for Advanced Copy Services profile file.

Note: Tivoli Storage FlashCopy Manager uses the production server to control offloaded backups to Tivoli Storage Manager. This behavior is different from Tivoli Storage Manager for Advanced Copy Services installation. Therefore, an `OFFLOAD` section must be defined in the profile configuration file on the production server. Any `OFFLOAD` section that is present in the backup system configuration file is discarded.

Migration from Tivoli Storage Manager for Advanced Copy Services 5.4 on SAN Volume Controller or DS8000

Tivoli Storage FlashCopy Manager and Tivoli Storage Manager for Advanced Copy Services 5.4 are separate products. Tivoli Storage FlashCopy Manager can preserve any incremental FlashCopy relations that are established with Tivoli Storage Manager for Advanced Copy Services 5.4. Tivoli Storage FlashCopy Manager does not restore backups that are created with Tivoli Storage Manager for Advanced Copy Services 5.4. You must use Tivoli Storage Manager for Advanced Copy Services 5.4.

The upgrade from Tivoli Storage Manager for Advanced Copy Services to Tivoli Storage FlashCopy Manager is processed as a new installation. The volumes file cannot be retained when you migrate to Tivoli Storage FlashCopy Manager. You must create new volumes files with **VOLUMES_FILE** syntax. For more information about **VOLUMES_FILE**, see “Target set definitions” on page 69. Use the following settings when you configure the `DEVICE_CLASS` section of the profile:

```
TARGET_SET VOLUMES_FILE
VOLUMES_FILE .fct_files
```

Tivoli Storage FlashCopy Manager and Tivoli Storage Manager for Advanced Copy Services can be used concurrently. Both products cannot use the same target set

definition file. Consider using Tivoli Storage Manager for Advanced Copy Services in emergency situations only. For example, use Tivoli Storage Manager for Advanced Copy Services to restore target sets unused by Tivoli Storage FlashCopy Manager. Before you attempt this restore, ensure that Tivoli Storage FlashCopy Manager has not used the target sets that you want to restore. Check in the Tivoli Storage FlashCopy Manager summary log file message FMM1582I. This log file is in the logs directory and the path is specified by ACS_DIR parameter in the profile.

Note:

- For logically partitioned DB2 environments, Tivoli Storage Manager for Advanced Copy Services 5.4 uses one target set definition file for each database host. Target set definition files are saved with a fct file extension. Tivoli Storage FlashCopy Manager uses one target set definition file for each node. To reuse the content of existing target set definition file, associate all nodes on the same host with a single partition group name. Use the **PARTITION_GROUP** parameter to associate the nodes. In this situation, Tivoli Storage FlashCopy Manager uses one volume file for each **PARTITION_GROUP**. This setting allows the reuse of the volumes file content with minimal changes.
- In an AIX LVM mirrored environment, the **STORAGE_SYSTEM_ID** profile parameter must be added to the DEVICE_CLASS section of the profile.

Migration from Tivoli Storage Manager for Advanced Copy Services 5.5 or later on SAN Volume Controller or DS8000

Tivoli Storage FlashCopy Manager and Tivoli Storage Manager for Advanced Copy Services Version 5.5 are separate products. However, Tivoli Storage FlashCopy Manager can preserve any incremental FlashCopy relations that are established with Tivoli Storage Manager for Advanced Copy Services 5.5, and reuse most of the Tivoli Storage Manager for Advanced Copy Services 5.5 profile.

Tivoli Storage FlashCopy Manager cannot restore backups that are created with Tivoli Storage Manager for Advanced Copy Services 5.5. These two products cannot be installed and configured simultaneously for the same database instance. However, the master copy of both products can be installed in the /usr/tivoli/ directory.

Before you configure Tivoli Storage FlashCopy Manager, follow these tasks:

- Create a copy of the existing Tivoli Storage Manager for Advanced Copy Services profile and repository directory. The repository directory is identified by the **ACS_REPOSITORY** parameter in the profile.
- When you run the installation setup script, update the **ACS_REPOSITORY** parameter with a new location for Tivoli Storage FlashCopy Manager metadata.
- Set the **TARGET_SETS** parameter to **VOLUMES_FILE**, and specify a valid .fct file.

After you install and configure Tivoli Storage FlashCopy Manager, all future operations are processed with Tivoli Storage FlashCopy Manager. In emergency situations, you can use Tivoli Storage Manager for Advanced Copy Services 5.5 or later to restore from target sets that are not used by Tivoli Storage FlashCopy Manager. In this scenario,

- Restore the original profile and the original Tivoli Storage Manager for Advanced Copy Services ACS_REPOSITORY directory.
- Run the Tivoli Storage Manager for Advanced Copy Services 5.5 setup script again for the current database instance.

- Before you restore with Tivoli Storage Manager for Advanced Copy Services 5.5, ensure that Tivoli Storage FlashCopy Manager has not used the target that you selected for the restore. To verify, check the Tivoli Storage FlashCopy Manager summary log file message FMM1582I. This log file is in the logs directory and the path that is specified by **ACS_DIR** parameter.

Note: In an AIX LVM mirrored environment, the **STORAGE_SYSTEM_ID** profile parameter must be added to the **DEVICE_CLASS** section.

Migrating from a proxy to an embedded CIMOM

Unlike LVM mirrored environments, there is no difference between the proxy CIMOM (Common Information Model Object Manager) and the embedded CIMOM. The following changes are required when migrating:

- The setup script updates the **COPYSERVICES_PRIMARY_SERVERNAME** parameter in the profile.
- The setup script updates the **COPYSERVICES_SECONDARY_SERVERNAME** parameter in the profile if specified.
- Reset the passwords.

Note: The minimum length of the master password is 8 characters. It must contain at least one number and one letter. The use of special symbols increases the strength of the password.

In LVM mirrored environments, you must use separate **DEVICE_CLASS** sections for each of the storage devices. Create a second **DEVICE_CLASS** statement in the profile. This statement can be identical to the first statement except for the **COPYSERVICES_PRIMARY_SERVERNAME** and **COPYSERVICES_SECONDARY_SERVERNAME** parameters. Both device classes now refer to separate target set definition files because of the following reasons:

- The device classes have a different value for the **VOLUMES_FILE** parameter.
- The naming conventions of volumes files are different, if the target sets are specified by using the **VOLUMES_FILE** parameter.

Make sure to separate the existing file into two files. Each file contains only those target sets that are eligible for the specific mirror. If the **VOLUMES_FILE** parameter is used in an LVM mirroring environment, the **STORAGE_SYSTEM_ID** parameter must be specified in the **DEVICE_CLASS** sections. Make sure to add rules to the **CLIENT** section of the profile that control the mirror to be used for the next backup operation. For more information about **DEVICE_CLASS name**, see the **CLIENT** section for your database type "CLIENT" on page 143.

Upgrading from Tivoli Storage FlashCopy Manager version 3.1, or earlier

If you are upgrading from Tivoli Storage FlashCopy Manager, Version 3.1 and the **USE_CONSISTENCY_GROUP** parameter is set to NO, the later version of Tivoli Storage FlashCopy Manager does not work. Tivoli Storage FlashCopy Manager Version 3.2 and later software requires the use of consistency groups. To remove the **USE_CONSISTENCY_GROUP** parameter, complete the following steps:

1. Log in to the production server by using the database user or custom application user ID and go to the **INSTANCE_DIR** directory.
2. Start the setup script by entering one of the following commands:

DB2

`./setup_db2.sh`

Oracle in an SAP environment

`./setup_ora.sh`

Oracle

`./setup_ora.sh`

Custom applications

The default installation directory is `$HOME/acs`. `$HOME` is the home directory of the application backup user.

`./setup_gen.sh`

3. Follow the setup script instructions that are displayed. For each Tivoli Storage FlashCopy Manager, Version 3.1 profile configuration that has the **USE_CONSISTENCY_GROUP** parameter, repeat these steps to automatically remove the **USE_CONSISTENCY_GROUP** parameter.

Chapter 4. Configuring Tivoli Storage FlashCopy Manager

After the installation and activation procedure is complete, configure Tivoli Storage FlashCopy Manager. To configure Tivoli Storage FlashCopy Manager, use the setup script for your environment. The information that you enter is used to create the profile configuration file.

Before you begin

Review the installation planning sheet that is associated with the *Hardware and Software Requirements* technote. This sheet contains the required parameters for each specific software application and custom application that are required during the configuration.

For the current requirements, review the *Hardware and Software Requirements* technote that is associated with the Tivoli Storage FlashCopy Manager release. This technote is available in the *Tivoli Storage FlashCopy Manager - All Requirement Documents* website at: <http://www.ibm.com/support/docview.wss?uid=swg21427692>. Follow the link to the requirements technote for your specific release or update level. Use the *Pre-installation checklist*, and *Installation Planning worksheet* before you install Tivoli Storage FlashCopy Manager.

About this task

When you configure Tivoli Storage FlashCopy Manager, you are prompted to enter parameter values that are specific to your environment. Syntax and value ranges are checked during the setup. Also, you must enter password information that is used to create a password file. A separate Tivoli Storage FlashCopy Manager profile is created for each application.

Procedure

Run the setup script for your environment. For more information about running the setup script, see the following topics, “Running the setup script for custom applications” on page 62, “Running the setup script for DB2,” “Running the setup script for a DB2 pureScale environment” on page 55, “Running the setup script for Oracle” on page 58

Running the setup script for DB2

Run the DB2 setup script to configure Tivoli Storage FlashCopy Manager for DB2. You can create a new profile, or reuse an existing one.

Before you begin

Choose whether to create a new profile, use an existing profile, or use an existing profile with updated parameters.

The profile configuration file is stored in the ACS_DIR/profile file. When the ACS_DIR directory is not identical to the INSTANCE_DIR directory, a symbolic link is created from the INSTANCE_DIR/profile pointing to the ACS_DIR/profile. If the profile is not stored in the ACS_DIR directory, an error is reported. This profile directory must not be included in any snapshots when you back up data.

For DB2 databases, the ACS_DIR directory can be exported from a Network file system (NFS) and the NFS shared on all DB2 Data Partitioning Feature (DPF) partitions.

About this task

Review the completed Tivoli Storage FlashCopy Manager installation sheet to ensure that the product installed correctly.

You can configure Tivoli Storage FlashCopy Manager in advanced mode by using the -advanced option with the appropriate setup script command. When you start the setup script in advanced mode, you can edit the parameters. To display help for the parameters, enter the ? character. The help is best viewed in a terminal window that is set for at least 130 characters.

Procedure

1. From the production database instance, log on as the database instance owner.
2. Go to the DB2 installation directory: `INSTANCE_DIR: DB2 instance owner $HOME/sql1lib/acs/`
3. Start the setup script by entering the following command:
`./setup_db2.sh`
4. Follow the setup script instructions. For information about the configuration steps, see “Configuring Tivoli Storage FlashCopy Manager for DB2” on page 56

Results

The setup script creates the following directories on the instance directories:

- The sql1lib/acs directory contains the Tivoli Storage FlashCopy Manager binary files.
- The ACS_DIR directory is the Tivoli Storage FlashCopy Manager configuration directory. It contains the following files and directories:
 - The profile configuration file.
 - The Tivoli Storage FlashCopy Manager repository.
 - The logs directory. All newly started daemons and active daemons processes are recorded in the summary log file.
 - The configuration wizard registers the Tivoli Storage FlashCopy Manager management daemon acsd and generic device agent acsgen in the /etc/inittab or creates and starts upstart jobs on the production server. These processes are started automatically even after a system restart.

Note: If you are installing Tivoli Storage FlashCopy Manager in an HA environment, these processes must be started from your HA environment. Add the processes to your HA startup scripts. In addition, you must ensure that these daemon processes are restarted if they are ended. In HA environments, nothing is added to /etc/inittab and no upstart jobs are created.

Running the setup script for a DB2 pureScale environment

Run the DB2 setup script to configure Tivoli Storage FlashCopy Manager in a DB2 pureScale environment. Running the script on one DB2 pureScale member updates the profile file. The hosts are configured for Tivoli Storage FlashCopy Manager high availability in a DB2 pureScale clustered environment.

Before you begin

Review the completed Tivoli Storage FlashCopy Manager installation sheet to ensure that the product installed correctly.

You can configure Tivoli Storage FlashCopy Manager in advanced mode by using the `-advanced` option with the appropriate setup script command. When you start the setup script in advanced mode, you can edit the parameters. To display help for the parameters, enter the `?` character. The help is best viewed in a terminal window that is set for at least 130 characters.

About this task

The `-hosts` option is used to specify either all hosts or to specify individual host names. The first time that you run the DB2 setup script after the installation, you must include the host name where the Tivoli Storage FlashCopy Manager installation was run. All specified hosts in the cluster are configured for Tivoli Storage FlashCopy Manager high availability.

Procedure

1. From the production database instance, log on as the database instance owner.
2. Go to the DB2 installation directory: `INSTANCE_DIR: DB2 instance owner $HOME/sql1ib/acs/`
3. Start the setup script by entering the following command:
`./setup_db2.sh`
4. Follow the setup script instructions. For information about the configuration steps, see “Configuring Tivoli Storage FlashCopy Manager for DB2” on page 56

Results

The setup script creates the following directories on the instance shared file system:

- The `sql1ib/acs` directory contains the Tivoli Storage FlashCopy Manager binary files.
- The `dbinstance_shared_directory-name/acs_dir` directory is the Tivoli Storage FlashCopy Manager configuration directory. It contains the following files and directories:
 - The profile configuration file.
 - The Tivoli Storage FlashCopy Manager repository.
 - The `.acsdLockFile.lock`, `.acsgenLockFile.lock`, and `.tsm4acsLockFile.lock` files. These files coordinate on which hosts the Tivoli Storage FlashCopy Manager daemon processes are running.
 - The logs directory. All newly started daemons and active daemon processes are recorded in the summary log file.

- The configuration wizard registers the Tivoli Storage FlashCopy Manager management daemon `acsd` and generic device agent `acsgen` in the `/etc/inittab` directory. These processes are started automatically even after a system restart.

Note: If you are installing Tivoli Storage FlashCopy Manager in an HA environment, these processes must be started from your HA environment. Add the processes to your HA startup scripts. In addition, you must ensure that these daemon processes are restarted if they are ended. In HA environments, nothing is added to the `/etc/inittab` directory.

Configuring Tivoli Storage FlashCopy Manager for DB2

After you run the setup script, the configuration wizard leads you through the configuration of the Tivoli Storage FlashCopy Manager for DB2.

Before you begin

To start the configuration process, run the setup script for DB2 with the following command: `./setup_db2.sh`

If you are using the setup script to configure an onsite backup server and you do not use standard CA-signed certificates for server authentication, you must copy `fcmselfcert.arm` from `INSTALL_DIR` on the production server to `INSTALL_DIR` on your backup or clone server. For information about IBM Global Security Kit configuration, see “IBM Global Security Kit configuration” on page 216.

About this task

For some parameters, you can create multiple entries with different values. To create these multiple entries, when prompted **Do you want to add another instance of this parameter?**, enter `y`. To delete a parameter entry, when prompted for the parameter value, enter `!d`.

Procedure

1. Choose either (1) or (2) depending on the type of configuration that you want:
 - (1) On-site Production Server configuration with optional remote Backup Server configuration.

This selection guides you through the configuration of Tivoli Storage FlashCopy Manager on the production server. It also provides the option to remotely activate and synchronize the configuration of one or more backup servers by using the OpenSSH protocol.

- (2) On-site Backup Server configuration.

This selection guides you through the configuration of Tivoli Storage FlashCopy Manager on the backup server as a separate installation.

2. Select one of these configurations for the database instance:

- (1) Backup only
- (2) Cloning only
- (3) Backup and cloning

Note: In an environment where cloning is not supported by Tivoli Storage FlashCopy Manager choose (1) Backup only.

3. Choose if you are going to run offload backups.

Are you going to perform offloaded backups to Tivoli Storage Manager?
[Y|N]

- Specify Y to configure support for offloaded tape backups.
- Specify N to configure support for disk-based snapshot backups only.

4. Choose if you want to start offloaded tape backups after the snapshot.

Do you want to start offloaded tape backups after the snapshot? [Y/N]

- Choose Y to start the offload immediately after the FlashCopy backup completes.
- Choose N if you want to schedule the offload operation to run later by scheduling backups individually. The backup to Tivoli Storage Manager can be delayed until the necessary resources in Tivoli Storage Manager server are available. This answer requires the scheduled backup process to be started manually.

For example, add a crontab entry. The default value is to run tsm4acs as a daemon process on the production server.

5. Choose one of the following options:

- Linux Do you want IBM Tivoli Storage FlashCopy(R) Manager to create and start the upstart jobs for you? [Y|N]
- AIX, Solaris, and HP-UX Do you want FlashCopy Manager to create the inittab entries for you? [Y/N]

Specify N for the executable files that include command-line options not to be added to the /etc/inittab and not to create upstart jobs. You must make sure that they are started by your HA startup scripts and that they are restarted whenever they are ended.

Specify Y to enter the daemon processes in the /etc/inittab or to create and start upstart jobs.

Important: After this procedure completes, you are prompted whether to deploy the configuration to one or multiple backup or clone systems. This deployment associates the device classes that are specified in the profile with the backup or clone systems. The following section describes the configuration of a backup system. When you configure a clone system, similar options are displayed.

6. Select the backup system to update or delete:

- n) To configure a new backup system
- b) Return to the previous menu
- q) To quit the configuration

Tivoli Storage FlashCopy Manager requires a backup server to be available when the following conditions exist:

- Offload backups to Tivoli Storage Manager are run.
- FlashCopy backup consistency must be verified during a forced mount operation.

Select n to configure and activate Tivoli Storage FlashCopy Manager on a remote site by using OpenSSH. OpenSSH must already be available for remote connections from the production system to the backup system. You are prompted to specify the **DEVICE_CLASS** to be enabled on the backup system. Select one or more **DEVICE_CLASS** parameters from the list that is displayed on the console.

Enter q to quit the configuration of the backup system and exit the setup script if one of the following conditions exist:

- OpenSSH is not available.
- You want to configure the backup system in a separate step.

When a backup system is configured, it is possible to run several actions on this backup system. For example, update, stop, start, delete FlashCopy Manager agents that are running on the backup system or you can set up SSH key authentication to the backup system.

The following example illustrates these actions.

Select the backup system to update or delete:

- 1) acsback1
- 2) acsback2
- 3) acsback5

n) to configure a new backup system

q) to quit configuration

1

selected backup system: acsback1

The backup system on acsback1 is configured with the device class DISK_ONLY3.

Select the action you want to take on the backup system acsback1:

- 1) update IBM Tivoli Storage FlashCopy Manager installation
- 2) start IBM Tivoli Storage FlashCopy Manager services
- 3) stop IBM Tivoli Storage FlashCopy Manager services
- 4) uninstall IBM Tivoli Storage FlashCopy Manager
- 5) setup the SSH key authentication

b) return to the backup system selection

q) quit the configuration

Select one of the options.

The same set of functions is provided for the configuration of the clone instances with SSH.

7. If this DB2 instance is a DB2 standby server source or target, or is a source or target in a DB2 HADR configuration, you can also back up the database while it serves as the standby (or HADR) target.

Do you want to configure Tivoli Storage FlashCopy Manager to also protect the database while it acts as a standby (or HADR) target? [Y/N]

Specify YES to back up a DB2 standby server. An extra DB2STANDBY section is added to the profile. If you are using an offloaded backup configuration, an offload section OFFLOAD_DB2STANDBY is also added.

Running the setup script for Oracle

Run the Oracle setup script to configure Tivoli Storage FlashCopy Manager for Oracle, or Oracle in an SAP environment.

Before you begin

Review the completed Tivoli Storage FlashCopy Manager installation sheet to ensure that the product installed correctly.

You can configure Tivoli Storage FlashCopy Manager in advanced mode by using the -advanced option with the appropriate setup script command. When you start the setup script in advanced mode, you can edit the parameters. To display help for the parameters, enter the ? character. The help is best viewed in a terminal window that is set for at least 130 characters.

Procedure

1. From the production database instance, log on as the database instance owner.
2. Go to the Oracle or Oracle in an SAP environment installation directory:
INSTANCE_DIR: *Oracle instance owner \$HOME/acs/*
3. Start the setup script by entering the following command:
./setup_ora.sh
4. Follow the setup script instructions. For information about the configuration steps, see “Configuring Tivoli Storage FlashCopy Manager for Oracle”

Results

The setup script creates the following directories on the instance directories:

- The \$HOME/acs directory contains the Tivoli Storage FlashCopy Manager binary files.
- The ACS_DIR directory is the Tivoli Storage FlashCopy Manager configuration directory. It contains the following files and directories:
 - The profile configuration file.
 - The Tivoli Storage FlashCopy Manager repository.
 - The logs directory. All newly started daemons and active daemons processes are recorded in the summary log file.
 - The configuration wizard registers the Tivoli Storage FlashCopy Manager management daemon acsd and generic device agent acsgen in the /etc/inittab or creates and starts upstart jobs on the production server. These processes are started automatically even after a system restart.

Note: If you are installing Tivoli Storage FlashCopy Manager in an HA environment, these processes must be started from your HA environment. Add the processes to your HA startup scripts. In addition, you must ensure that these daemon processes are restarted if they are ended. In HA environments, nothing is added to /etc/inittab and no upstart jobs are created.

Configuring Tivoli Storage FlashCopy Manager for Oracle

After you run the setup script, the configuration wizard leads you through the configuration of the Tivoli Storage FlashCopy Manager for Oracle.

Before you begin

To start the configuration process, run the setup script for Oracle with the following command: ./setup_ora.sh

If you are using the setup script to configure an onsite backup server and you do not use standard CA-signed certificates for server authentication, you must copy fcmselfcert.arm from INSTALL_DIR on the production server to INSTALL_DIR on your backup or clone server. For information about IBM Global Security Kit configuration, see “IBM Global Security Kit configuration” on page 216.

About this task

For some parameters, you can create multiple entries with different values. To create these multiple entries, when prompted **Do you want to add another**

instance of this parameter?, enter y. To delete a parameter entry, when prompted for the parameter value, enter !d.

Procedure

1. Choose either (1) or (2) depending on the type of configuration you want:

- (1) On-site Production Server configuration with optional remote Backup Server configuration.

This selection guides you through the configuration of Tivoli Storage FlashCopy Manager on the production server. It also provides the option to remotely activate and synchronize the configuration of one or more backup servers by using the OpenSSH protocol.

- (2) On-site Backup Server configuration.

This selection guides you through the configuration of Tivoli Storage FlashCopy Manager on the backup server as a separate installation.

2. Select one of these configurations for the database instance:

- (1) Backup only
- (2) Cloning only
- (3) Backup and cloning

Note: In an environment, where cloning is not supported by Tivoli Storage FlashCopy Manager choose (1) Backup only.

3. Choose if you are going to run offload backups.

Are you going to perform offloaded backups to Tivoli Storage Manager?
[Y|N]

- Specify yes to configure support for offloaded tape backups.

Note: For Oracle in an SAP environment, you must manually update the IBM Tivoli Storage Manager for Enterprise Resource Planning profile `initSID.utl` file after the configuration completes.

- Specify no to configure support for disk-based snapshot backups only.

4. Choose if you want to start offloaded tape backups after the snapshot.

Do you want to start offloaded tape backups after the snapshot? [Y/N]

- Choose yes to start the offload immediately after the FlashCopy backup completes.
- Choose no if you want to schedule the offload operation to run later by scheduling backups individually. The backup to Tivoli Storage Manager can be delayed until the necessary resources in Tivoli Storage Manager server are available. This answer requires the scheduled backup process to be started manually. For example, add a crontab entry. The default value is to run `tsm4acs` as a daemon process on the production server.

5. Choose one of the following options:

- Linux Do you want IBM Tivoli Storage FlashCopy(R) Manager to create and start the upstart jobs for you? [y|n]

- AIX, Solaris, and HP-UX Do you want FlashCopy Manager to create the `inittab` entries for you? [Y/N]

Specify NO for the executable files that include command-line options not to be added to the `/etc/inittab` and not to create upstart jobs. You must make sure that they are started by your HA startup scripts and that they are restarted whenever they are ended.

Specify YES to enter the daemon processes in the /etc/inittab or to create and start upstart jobs.

Important: After this procedure completes, you are prompted whether to deploy the configuration to one or multiple backup or clone systems. This deployment associates the device classes that are specified in the profile with the backup or clone systems. The following section describes the configuration of a backup system. When you configure a clone system, similar options are displayed.

6. Select the backup system to update or delete:

- n) To configure a new backup system
- b) Return to the previous menu
- q) To quit the configuration

Tivoli Storage FlashCopy Manager requires a backup server to be available when the following conditions exist:

- Offload backups to Tivoli Storage Manager are run.
- FlashCopy backup consistency must be verified during a forced mount operation.

Select n to configure and activate Tivoli Storage FlashCopy Manager on a remote site by using OpenSSH. OpenSSH must already be available for remote connections from the production system to the backup system. You are prompted to specify the **DEVICE_CLASS** to be enabled on the backup system. Select one or more **DEVICE_CLASS** parameters from the list that is displayed on the console.

Enter q to quit the configuration of the backup system and exit the setup script if one of the following conditions exist:

- OpenSSH is not available.
- You want to configure the backup system in a separate step.

When a backup system is configured, it is possible to run several actions on this backup system. For example, update, stop, start, delete FlashCopy Manager agents that are running on the backup system or you can set up SSH key authentication to the backup system.

The following example illustrates these actions.

Select the backup system to update or delete:

- 1) acsback1
- 2) acsback2
- 3) acsback5

- n) to configure a new backup system
 - q) to quit configuration
- 1
- selected backup system: acsback1

The backup system on acsback1 is configured with the device class DISK_ONLY3. Select the action you want to take on the backup system acsback1:

- 1) update IBM Tivoli Storage FlashCopy Manager installation
- 2) start IBM Tivoli Storage FlashCopy Manager services
- 3) stop IBM Tivoli Storage FlashCopy Manager services
- 4) uninstall IBM Tivoli Storage FlashCopy Manager
- 5) setup the SSH key authentication

- b) return to the backup system selection
- q) quit the configuration

Select one of the options.

The same set of functions is provided for the configuration of the clone instances with SSH.

Running the setup script for custom applications

Run the setup script `./setup_gen.sh` to configure Tivoli Storage FlashCopy Manager for custom applications.

Before you begin

Review the completed Tivoli Storage FlashCopy Manager installation sheet to ensure that the product installed correctly.

You can configure Tivoli Storage FlashCopy Manager in advanced mode by using the `-advanced` option with the appropriate setup script command. When you start the setup script in advanced mode, you can edit the parameters. To display help for the parameters, enter the `?` character. The help is best viewed in a terminal window that is set for at least 130 characters.

Procedure

1. From the production server, log on as the application backup user.
2. Go to the installation directory: `INSTANCE_DIR: $HOME/acs/`
3. Start the setup script by entering the following command:
`./setup_gen.sh`
4. Follow the setup script instructions. For information about the configuration steps, see “Configuring Tivoli Storage FlashCopy Manager for custom applications” on page 63.

Results

The setup script creates the following directories on the instance directory:

- The `$HOME/acs` directory contains the Tivoli Storage FlashCopy Manager binary files.
- The `ACS_DIR` directory is the Tivoli Storage FlashCopy Manager configuration directory. It contains the following files and subdirectories:
 - The profile configuration file.
 - The Tivoli Storage FlashCopy Manager repository.
 - The logs directory. All newly started daemons and active daemons processes are recorded in the summary log file.
 - The configuration wizard registers the Tivoli Storage FlashCopy Manager management daemon `acsd` and generic device agent `acsngen` in the `/etc/inittab` or creates and starts upstart jobs on the production server. These processes are started automatically even after a system restart.

Note: If you are installing Tivoli Storage FlashCopy Manager in an HA environment, these processes must be started from your HA environment. Add the processes to your HA startup scripts. In addition, you must ensure that these daemon processes are restarted if they are ended. In HA environments, nothing is added to `/etc/inittab` and no upstart jobs are created.

Configuring Tivoli Storage FlashCopy Manager for custom applications

After you run the setup script, the configuration wizard leads you through the configuration of the Tivoli Storage FlashCopy Manager for custom applications.

Before you begin

To start the configuration process, run the setup script for custom applications with the following command: `./setup_gen.sh`

If you are using the setup script to configure an onsite backup server and you do not use standard CA-signed certificates for server authentication, you must copy `fcmselcert.arm` from `INSTALL_DIR` on the production server to `INSTALL_DIR` on your backup or clone server. For information about IBM Global Security Kit configuration, see “IBM Global Security Kit configuration” on page 216.

About this task

For some parameters, you can create multiple entries with different values. To create these multiple entries, when prompted **Do you want to add another instance of this parameter?**, enter `y`. To delete a parameter entry, when prompted for the parameter value, enter `!`d.

Procedure

1. Choose either (1) or (2) depending on the type of configuration you want:

- (1) On-site Production Server configuration with optional remote Backup Server configuration.

This selection guides you through the configuration of Tivoli Storage FlashCopy Manager on the production server. It also provides the option to remotely activate and synchronize the configuration of one or more backup servers by using the OpenSSH protocol.

- (2) On-site Backup Server configuration.

This selection guides you through the configuration of Tivoli Storage FlashCopy Manager on the backup server as a separate installation.

2. Choose if you are going to run offload backups.

Are you going to perform offloaded backups to Tivoli Storage Manager?
[Y|N]

- Specify `Y` to configure support for offloaded tape backups.
- Specify `N` to configure support for disk-based snapshot backups only.

3. Choose if you want to start offloaded tape backups after the snapshot.

Do you want to start offloaded tape backups after the snapshot? [Y/N]

- Choose `Y` to start the offload immediately after the FlashCopy backup completes.
- Choose `N` if you want to schedule the offload operation to run later by scheduling backups individually. The backup to Tivoli Storage Manager can be delayed until the necessary resources in Tivoli Storage Manager server are available. This answer requires the scheduled backup process to be started manually. For example, add a crontab entry. The default value is to run `tsm4acs` as a daemon process on the production server.

4. Choose one of the following options:

- Linux Do you want IBM Tivoli Storage FlashCopy(R) Manager to create and start the upstart jobs for you? [Y|N]

- AIX, Solaris, and HP-UX Do you want FlashCopy Manager to create the inittab entries for you? [Y/N]
Specify N for the executable files that include command-line options not to be added to the /etc/inittab and not to create upstart jobs. You must make sure that they are started by your HA startup scripts and that they are restarted whenever they are ended.
Specify Y to enter the daemon processes in the /etc/inittab directory, or to create and start upstart jobs.

Important: After this procedure completes, you are prompted whether you want to deploy the configuration to one or multiple backup or clone systems. This deployment associates the device classes that are specified in the profile with the backup or clone systems. The following section describes the configuration of a backup system. When you configure a clone system, similar options are displayed.

5. Select the backup system to update or delete:

- n) To configure a new backup system
- b) Return to the previous menu
- q) To quit the configuration

Tivoli Storage FlashCopy Manager requires a backup server to be available when the following conditions exist:

- Offload backups to Tivoli Storage Manager are run.
- FlashCopy backup consistency must be verified during a forced mount operation.

Select n to configure and activate Tivoli Storage FlashCopy Manager on a remote site by using OpenSSH. OpenSSH must already be available for remote connections from the production system to the backup system. You are prompted to specify the **DEVICE_CLASS** to be enabled on the backup system. Select one or more **DEVICE_CLASS** parameters from the list that is displayed on the console.

Enter q to quit the configuration of the backup system and exit the setup script if one of the following conditions exist:

- OpenSSH is not available.
- You want to configure the backup system in a separate step.

When a backup system is configured, it is possible to run several actions on this backup system. For example, update, stop, start, delete FlashCopy Manager agents that are running on the backup system or you can set up SSH key authentication to the backup system.

The following example illustrates these actions.

Select the backup system to update or delete:

- 1) acsback1
- 2) acsback2
- 3) acsback5

n) to configure a new backup system

q) to quit configuration

1

selected backup system: acsback1

The backup system on acsback1 is configured with the device class DISK_ONLY3.
Select the action you want to take on the backup system acsback1:

- 1) update IBM Tivoli Storage FlashCopy Manager installation
- 2) start IBM Tivoli Storage FlashCopy Manager services
- 3) stop IBM Tivoli Storage FlashCopy Manager services
- 4) uninstall IBM Tivoli Storage FlashCopy Manager

- 5) setup the SSH key authentication
- b) return to the backup system selection
- q) quit the configuration

Select one of the options.

The same set of functions is provided for the configuration of the clone instances with SSH.

Configuring storage environments

You must configure all storage devices but IBM System Storage DS8000, IBM System Storage SAN Volume Controller, and IBM Storwize family storage devices require more configuration to prepare for source and target volume relationships.

About this task

The Tivoli Storage FlashCopy Manager profile configuration file can contain one or more **DEVICE_CLASS** sections. This section is used to configure Tivoli Storage FlashCopy Manager for use with a particular storage solution. The parameters do not depend on the database or custom application that is protected. Follow the steps in the appropriate procedure for your disk storage environment. For your disk storage subsystem, data files must be defined on volume groups that are separate from the volume groups where the control files and redo logs are defined. For more information about volume group layout requirements, see “Preparation for installation” on page 10.

Configuring the CIM adapter for SP 800-131A compliant encryption

CIM agents are provided by IBM System Storage SAN Volume Controller, IBM Storwize, and IBM System Storage DS8000 systems. Tivoli Storage FlashCopy Manager for UNIX and Linux communicates with a CIM agent through the CIM interface. You must configure the Tivoli Storage FlashCopy Manager CIM adapter to use the security standards, as defined in the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-131A for encryption.

Before you begin

Ensure that the storage system is enabled for SP 800-131A standard encryption. For instructions about how to identify if the system is enabled, see the documentation that is provided for your storage system.

Procedure

1. Extract the Secure Sockets Layer (SSL) certificate from the IBM storage system cluster. The certificate must be in the Privacy Enhanced Mail (PEM) format. From any Linux or UNIX system with a LAN connection to the storage system, run the following shell command,

```
echo | openssl s_client -connect ibm_storage_cluster_ip:5989 2>&1
| sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
```

where *ibm_storage_cluster_ip* specifies the IP address of the storage system, and 5989 specifies the port number for the HTTPS connection.

2. Save the output to a text file and place the file in a secure location on the Tivoli Storage FlashCopy Manager production and backup servers.

3. Run the Tivoli Storage FlashCopy Manager setup script in advanced mode by entering the following command:
`./setup.sh -advanced`
4. When prompted for the **COPYSERVICES_CERTIFICATEFILE** parameter for the storage system device class, enter the fully qualified path to the certificate file. For example:
`COPYSERVICES_CERTIFICATEFILE ACS_DIR/truststore/svc_cluster.cert`
5. Follow the setup script instructions to save the profile and restart the Tivoli Storage FlashCopy Manager daemons.

Defining Logical Unit Numbers on DS8000 storage subsystems

Logical Unit Numbers (LUNs) must be defined for the DS8000 storage subsystem.

Before you begin

Before you start defining LUNs on the storage subsystem, verify that the following prerequisites are met:

- The LUNs are located where the production database or application is located.
- The size of the LUNs is dependent upon the size of the database or application.
- The size of the source volumes on the production server and size of the target volumes on the backup server must be the same.
- Both the source volume and target volume must be defined on the same storage subsystem.
- Assign the source volume to the DS8000 volume group that is associated with the production server.

Procedure

Perform these steps so that the correct LUNs are defined on both the production server and backup server.

1. Use the DS8000 Storage Manager to create two or more fixed block LUNs on the production server.

2. Use the DS8000 Storage Manager to create the same number of LUNs for the backup server as were created for the production server in the previous step.

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 for the production server. Assign the target volume to the DS8000 volume group that is associated with the backup server.

3. Identify the serial numbers of the target LUNs by using the DS8000 Storage Manager.

Real-time manager (or Simulated manager)-> Configure storage -> Open systems -> Volumes-open systems

Select the target LUNs created on the backup server in Step 2. Identify the serial numbers with the matching size in the source LUNs. For example:

```
7501901
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 75019013300 and 75019013400.

4. Define the **TARGET_VOLUME** parameter in the target volumes file specified by the **VOLUMES_FILE** profile parameter with the appropriate serial numbers of the target LUN. For example:

```
TARGET_VOLUME 75019013300
TARGET_VOLUME 75019013400
```

This setting specifies the target volumes where the database or application is backed up.

Related concepts:

“Target set definition files” on page 70

Defining virtual disks on SAN Volume Controller and Storwize family

When you define virtual disks for the SAN Volume Controller and the Storwize family storage devices, you can use either the graphical user interface or the command-line interface.

Before you begin

Before you start defining virtual disks, verify that the following prerequisites are met:

- A storage area network is available.
- Storage disks are attached and available in the SAN Volume Controller or Storwize family environment.
- Subsystem Device Driver (SDD) or Subsystem Device Driver Path Control Module (SDDPCM) is installed and available on the host systems.
- A cluster is available in the SAN Volume Controller or Storwize family environment.
- Each host has at least two paths to the SAN Volume Controller or Storwize family storage device.

Procedure

To create virtual disks on the production server and backup server, complete the following steps.

1. From the graphical user interface, select **Work with Virtual Disks > Virtual Disks > Create Virtual Disks**. The virtual disks are created by using the managed disk group.
2. Map the virtual disk to the hosts that are created for the production server. To map the virtual disks to the backup server, in the Tivoli Storage FlashCopy Manager profile file, configure the **BACKUP_HOST_NAME** parameter by assigning one of the following values:
 - Assign the value **PREASSIGNED_VOLUMES** to use a static predefined map.
 - Assign the *backup_server_hostname* to allow Tivoli Storage FlashCopy Manager to dynamically map the target virtual disks when needed.
3. Define the **TARGET_VOLUME** parameter in the target volumes file (.fct). This name is specified by the **DEVICE_CLASS > TARGET_SETS > VOLUMES_FILE** parameter with the appropriate virtual disk names of the target LUNs in the profile configuration file. For example:

```
TARGET_VOLUME A01pro1_1_t1
TARGET_VOLUME A01pro1_2_t1
```

In this example, the source volume names are A01pro1_1 and A01pro1_2 with target set named 1.

Alternatively, you can define the target names by using the **TARGET_NAMING** parameter in the Tivoli Storage FlashCopy Manager profile file.

Related concepts:

“Target set definitions using the naming convention” on page 71

Select the FLASHCOPY_TYPE

DS8000, SAN Volume Controller, and Storwize family storage solutions support various FlashCopy types that provide different capabilities for your backup strategy.

Using different FlashCopy types for different backup generations is a valid strategy for Tivoli Storage FlashCopy Manager. To implement such a backup strategy, define multiple **DEVICE_CLASS** sections in the profile, where each section specifies the same storage device. The only difference is that each section specifies a different FlashCopy type. These **DEVICE_CLASS** section definitions allow rules to be defined in the **CLIENT** profile section. These rules allow Tivoli Storage FlashCopy Manager to select the appropriate **DEVICE_CLASS** section for the next backup. For more information about the **DEVICE_CLASS** parameter, see the **CLIENT** section.

If the **FLASHCOPY_TYPE** is changed for one **DEVICE_CLASS**, complete the following steps:

1. Unmount the backup if it is mounted on a backup system.
2. Delete the backup with the delete force option.
3. Change the **FLASHCOPY_TYPE** in the **DEVICE_CLASS** and run a new backup with the new **FLASHCOPY_TYPE**.

Table 3. Selecting the **FLASHCOPY_TYPE** for DS8000, SAN Volume Controller, and Storwize family

FLASHCOPY_TYPE	DS8000	SAN Volume Controller Storwize family
COPY	Can be used for backup and restore. Protects from physical failures of the source volumes when the background copy completes.	Can be used for backup and restore. Protects from physical failures of the source volumes when the background copy completes. Avoid creating a COPY FlashCopy to a space-efficient target because the target eventually becomes fully allocated due to background copying of data.
INCR	Same characteristics as COPY FLASHCOPY_TYPE but with fewer COPY activities in the background. DS8000 allows at most 1 incremental FlashCopy per source volume. In mirroring environments, this setting allows it to retain 1 backup generation per mirror. For DS8000, there must be only one target set specified in the target volumes file (.fct) for incremental snapshots. CIM errors might occur when more than one target set is specified.	Same characteristics as COPY FlashCopy but with fewer COPY activities in the background. Avoid creating an incremental FlashCopy to a space-efficient target. The target eventually becomes fully allocated because the data is copied in the background.

Table 3. Selecting the **FLASHCOPY_TYPE** for DS8000, SAN Volume Controller, and Storwize family (continued)

FLASHCOPY_TYPE	DS8000	SAN Volume Controller Storwize family
NOCOPY	Can be mounted remotely, but cannot be restored.	Can be mounted remotely and can be restored. Can be used to create a FlashCopy to a space-efficient target, but does not offer protection from physical failures to the source volume. Note: Space-efficient target volumes can reach capacity limits in which case they go offline. In this scenario, you lose the current backup and all older backups that are not at FULL_COPY. You can choose to create space-efficient targets with the AUTOEXPAND option. In this scenario, the target is allocated more physical storage to prevent going offline.

The types of snapshots that are supported by Tivoli Storage FlashCopy Manager, depending on the storage solution and operating system, are indicated in the following table.

Table 4. Supported storage subsystems and FlashCopy types

Device	COPY	INCR	NOCOPY	Space-efficient snapshots	Changes made to a mounted snapshot backup
IBM System Storage DS8000	Yes	Yes	Yes	N/A	Remains persistent and alters the content of the backup.
IBM System Storage SAN Volume Controller IBM Storwize family	Yes	Yes	Yes Includes space-efficient copies if configured so.	N/A	Remains persistent and alters the content of the backup.
IBM XIV Storage System	N/A	N/A	N/A	Yes	Reverted during unmount and does not alter the backup or remains persistent and alters the content of the backup.
IBM System Storage N series NetApp systems	N/A	N/A	N/A	Yes	Reverted during unmount and does not alter the backup.

Target set definitions

Tivoli Storage FlashCopy Manager requires target sets to be defined for SAN Volume Controller, Storwize family, and DS8000.

Define targets by using target set definition files (SAN Volume Controller, Storwize family, and DS8000) or by using a naming convention (SAN Volume Controller and Storwize family only). This convention determines the name of the target for both the source volume name and the target set name as specified for the current operation.

Target set definition files

A target set definition file contains a list of target volumes that are organized into target sets.

During the backup process, Tivoli Storage FlashCopy Manager software matches source volumes to suitable targets within a target set. To determine source target relations, associate a source name with a target name in a target set definition file. In this scenario, the relationship between the source and target is required. Backup processing fails if one of the targets is unavailable for the specified source. For details on the target selection algorithms, see “Target volumes” on page 199.

If Tivoli Storage FlashCopy Manager attempts to mount the target set, the volumes within the target set must be assigned to a backup host. For example, the target set is mounted to create a backup to Tivoli Storage Manager. Because all target volumes within a single target are mounted to the same host, assign all target volumes within a target set to the same host. When you use multiple backup servers within your environment, use multiple target set definition files.

For SAN Volume Controller and Storwize family storage solutions, Tivoli Storage FlashCopy Manager can assign the target volumes dynamically during the mount operation. In this case, you must not assign the target volumes in advance of the mount operation.

Example

The example is of a target set definition file for an application that is running on DS8000:

```
>>> TARGET_SET SET_1 # FCM determines a suitable target for every source
TARGET_VOLUME 40913158
TARGET_VOLUME 40A13158
TARGET_VOLUME 40B13158
<<<
>>> TARGET_SET SET_2 # For every source the target is mandated in the target set
                        # definition (source name following target name)
TARGET_VOLUME 40C13158 40613158
TARGET_VOLUME 40D13158 40713158
TARGET_VOLUME 40E13158 40813158
<<<
```

Target set definition file for multi-partition DB2 databases

Multi-partition DB2 database target set definitions must be specified for each partition.

As a result, the contents of the target set definition file is separated into multiple sections. One section is used for each partition, as shown in this example:

```
>>> TARGET_SET SET_1 # FCM determines a suitable target for every source
>>> PARTITION NODE0000
TARGET_VOLUME 40913158
TARGET_VOLUME 40A13158
<<<
>>> PARTITION NODE0001
TARGET_VOLUME 40B13158
TARGET_VOLUME 50913158
TARGET_VOLUME 50A13158
TARGET_VOLUME 50B13158
TARGET_VOLUME 51713158
<<<
>>> PARTITION NODE0002
TARGET_VOLUME 51813158
```

```

TARGET_VOLUME 52113158
TARGET_VOLUME 52313158
<<<
<<<

```

A single backup server environment (for a multi-partition DB2 database) can be distributed across multiple servers. In this situation, make sure that the target volumes in the target set definition file are assigned to the correct host. For best results, assign all target volumes in the target set definition file (and that are associated with the same partition) to the same host. In environments where multiple partitions reside on the same volume group (volume sharing), target set definition files need to specify certain values. See the `PARTITION_GROUP` parameter for more information.

Referring to target set definitions from the profile

The target set definition file must be specified in the `DEVICE_CLASS` section of the profile.

The following example is a section from a Tivoli Storage FlashCopy Manager profile file that shows the association between `TARGET_SETS`, `VOLUMES_FILE`, and *name of target set definition file* parameters.

```

>>> DEVICE_CLASS STANDARD
COPYSERVICES_HARDWARE TYPE DS8000
COPYSERVICES_PRIMARY_SERVERNAME <hostname> #
TARGET_SETS VOLUMES_FILE
VOLUMES_FILE name of target set definition file
FLASHCOPY_TYPE INCR
<<<

```

If multiple `DEVICE_CLASS` configuration sections are specified within the profile, associate each `DEVICE_CLASS` section with a unique target set definition file for best results. If all target sets within the target set definition file are assigned to the same host and associated with one `DEVICE_CLASS`, they are mounted on the same host.

Target set definitions using the naming convention

Target set definitions can also be provided by using a naming convention on SAN Volume Controller and Storwize family.

Tivoli Storage FlashCopy Manager supports using a naming convention, instead of a definition file, for target set definitions on SAN Volume Controller and Storwize family storage systems. Tivoli Storage FlashCopy Manager determines the target volume names from the name of the target set, used for the current backup, and the name of the source volume. Target sets are specified directly in the `DEVICE_CLASS` configuration section of the profile for example, `TARGET_SETS 1 2 3`. A `TARGET_NAMING` rule is also specified for example, `TARGET_NAMING %SOURCE_bt%TARGETSET`. This rule determines the name of the target volume from the name of the source. For example, if the application is stored on a volume named `db_vol`, the targets required by Tivoli Storage FlashCopy Manager are `db_vol_bt1`, `db_vol_bt2`, and `db_vol_bt3`. These targets depend on the target set selected for the current backup.

```

>>> DEVICE_CLASS STANDARD
COPYSERVICES_HARDWARE TYPE SVC
COPYSERVICES_PRIMARY_SERVERNAME <hostname> #
TARGET_SETS 1 2 3
TARGET_NAMING %SOURCE_bt%TARGETSET
FLASHCOPY_TYPE NOCOPY
<<<

```

Related concepts:

“Target volumes” on page 199

LVM mirroring and ASM failure group environments

In a Logical Volume Manager (LVM) mirroring on AIX and Oracle Automatic Storage Management (ASM) failure group environments, multiple `DEVICE_CLASS` configuration sections are required. One section per storage cluster or LVM mirror is required.

The storage system ID must be specified in the Tivoli Storage FlashCopy Manager `DEVICE_CLASS` configuration section. For example:

```
>>> DEVICE_CLASS MIRR_1
COPYSERVICES_HARDWARE_TYPE DS8000
COPYSERVICES_PRIMARY_SERVERNAME DS8000_1
STORAGE_SYSTEM_ID 7513158
TARGET_SETS VOLUMES_FILE
VOLUMES_FILE <name of target set definition file 1>
FLASHCOPY_TYPE INCR
<<<

>>> DEVICE_CLASS MIRR_2
COPYSERVICES_HARDWARE_TYPE DS8000
COPYSERVICES_PRIMARY_SERVERNAME DS8000_2
STORAGE_SYSTEM_ID 7512067
TARGET_SETS VOLUMES_FILE
VOLUMES_FILE <name of target set definition file 2>
FLASHCOPY_TYPE INCR
<<<
```

The **`STORAGE_SYSTEM_ID`** parameter is required when ASM failure groups are distributed across multiple storage devices. Each device section in the profile requires this parameter to specify the storage subsystem ID. Do not specify this parameter when all failure groups are on the same storage subsystem. For information about this parameter, see the `DEVICE_CLASS` device section of the profile configuration file.

Related reference:

“`DEVICE_CLASS device`” on page 171

Backup and clone server assignment

With Tivoli Storage FlashCopy Manager software, you can mount backup images and clone images. Each backup image and clone image is mounted on a server. However, you cannot mount a backup image or a clone image on more than one server at one time.

Tivoli Storage FlashCopy Manager mount operation can be started by one of the following methods:

- By issuing a mount command from the command-line interface.
- By issuing a create or refresh clone command from the command-line interface.
- When Tivoli Storage FlashCopy Manager is used with Tivoli Storage Manager and you offload backups to Tivoli Storage Manager.

The information that you enter during the installation and configuration of Tivoli Storage FlashCopy Manager is used to create a profile configuration file. The `DEVICE_CLASS` section of this profile specifies the backup host name where the backup or clone images are mounted. There can be multiple `DEVICE_CLASS` sections.

The CLIENT section specifies the DEVICE_CLASS to use for backup and offload operations. The CLONING section specifies the DEVICE_CLASS to use for cloning operations.

FlashCopy or snapshot target volumes are mounted and assigned to selected backup or clone server. Depending on the storage system and profile configuration the following assignments occur:

IBM XIV Storage Systems, IBM System Storage N series, and NetApp storage systems

The assignment automatically occurs during the mount request.

SAN Volume Controller and Storwize family

If the **BACKUP_HOST_NAME** parameter is specified as *backup_server_hostname* in the DEVICE_CLASS section, the target volumes are mapped dynamically from the storage system to the backup and clone server.

DS8000, SAN Volume Controller, and Storwize family

If the **BACKUP_HOST_NAME** parameter is specified as *PREASSIGNED_VOLUMES* in the DEVICE_CLASS section, the target volumes must be preassigned to a specific backup or clone server before you issue a mount command. Ensure that the target volumes of all target sets associated with a specific DEVICE_CLASS are assigned to the same hosts. If target set definition files are used, assign all volumes within one target set definition file to the same host. This setting ensures that targets associated with a single device class are mounted from the same backup or clone server.

For all Tivoli Storage FlashCopy Manager mount operations, there can be only one backup or clone server for each device class. If the identified servers have not mounted a backup or clone image, the mount request is propagated to those servers. The backup or clone is then mounted. The following figure shows a sample configuration and host assignments for DB2.

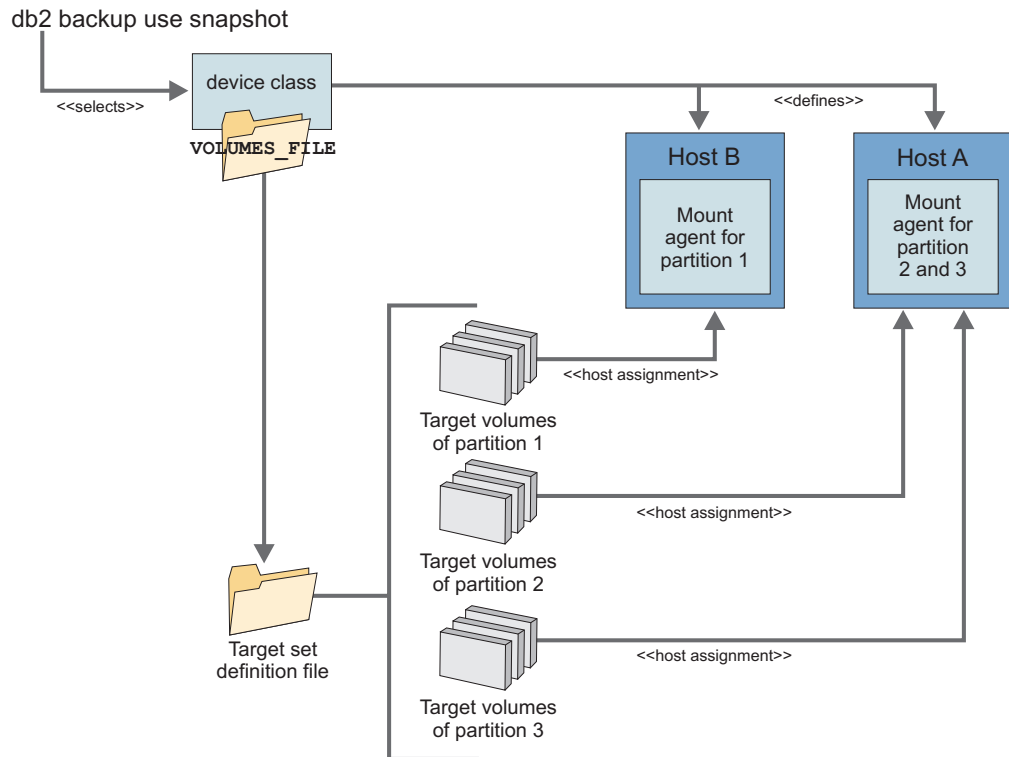


Figure 7. Tivoli Storage FlashCopy Manager host assignments for DB2.

Related concepts:

“Managing backups and clones with the **DEVICE_CLASS** parameter”

Managing backups and clones with the **DEVICE_CLASS** parameter

Use the **DEVICE_CLASS** parameter in the CLIENT section of the Tivoli Storage FlashCopy Manager profile file to select the storage device configuration for backups. In the CLONING section of the profile file, use this parameter to select the storage device configurations for cloning.

The Tivoli Storage FlashCopy Manager **DEVICE_CLASS** profile parameter can be used as a filter to determine these backup criteria:

- Partition number
- Day of week
- Time of backup
- Cloning only: Clone database name

When used in this manner, the **DEVICE_CLASS** parameter provides access to a specific storage device. This device is identified by the copy services type, user name, and server name that is defined by the corresponding **DEVICE_CLASS** profile section. It also provides a backup policy that is device-specific. For example, this device-specific backup policy might be defined by these factors:

- List of target sets on DS8000, SAN Volume Controller, or Storwize family
- The type of FlashCopy backup to be completed (for example, incremental or copy)
- The mount location of the backup

- Whether a backup to Tivoli Storage Manager server storage is created from the snapshot

The **DEVICE_CLASS** parameter is specified in the client section of Tivoli Storage FlashCopy Manager profile file. The settings for this parameter can be overridden with a command-line option during backup operations. Depending on the application, use one of the following command-line options:

From the DB2 command line

OPTIONS "DEVICE_CLASS=*device class*"

From the Oracle in an SAP environment interface

-S *device class* in SAP BR*Tools configuration profile (.sap)
util_options parameter.

For all other applications

-s *device class* on the command line of the corresponding application.

The **DEVICE_CLASS** parameter cannot be specified with the **restore**, **mount**, **unmount**, and **delete** commands. You can specify the backup ID, if it is not specified the latest backup is used. Tivoli Storage FlashCopy Manager automatically uses the **DEVICE_CLASS** that was used for the selected backup at backup time.

Examples of how to use DEVICE_CLASS filters

This example creates alternating backups to each mirror. Device classes MIRROR_1 and MIRROR_2 refer to two separate storage clusters. Only those backups that are created to MIRROR_2 are backed up to Tivoli Storage Manager server storage:

```
>>> CLIENT
TSM_BACKUP LATEST USE_FOR MIRROR_2
DEVICE_CLASS MIRROR_1 MIRROR_2
[...]
<<<
```

This example creates backups of a partitioned DB2 database with five partitions. While partition 0 uses **DEVICE_CLASS PARTITION0**, the partitions 1-4 use **DEVICE_CLASS PARTITIONX**:

```
>>> CLIENT
DEVICE_CLASS PARTITION0 ON_DBPARTITIONNUMS 0
DEVICE_CLASS PARTITIONX ON_DBPARTITIONNUMS 1 2 3 4
[...]
<<<
```

This example creates backups to MIRROR_1 on Monday (1), Wednesday (3), and Friday (5). It creates backups to MIRROR_2 on Sunday (0), Tuesday (2), and Thursday (4), and Saturday (6). All backups are stored on Tivoli Storage Manager server storage:

```
>>> CLIENT
TSM_BACKUP LATEST
DEVICE_CLASS MIRROR_1 USE_AT Mon Wed Fri
DEVICE_CLASS MIRROR_2 USE_AT Sun Tue Thu Sat
[...]
<<<
```

This example creates disk only backups during the specified period of the day. These disk only backups are considered space-efficient. A full backup is also created at midnight that is stored on Tivoli Storage Manager server storage. Although the *DAYTIME* and *MIDNIGHT* device classes might have the same

configuration, two different device classes are used. This setting is used even if both device classes point to the same SAN Volume Controller cluster:

```
>>> CLIENT
TSM_BACKUP LATEST USE_FOR MIDNIGHT
DEVICE_CLASS DAYTIME FROM 1:00 TO 23:59
DEVICE_CLASS MIDNIGHT FROM 0:00 TO 0:59
[...]
<<<
>>> DEVICE_CLASS DAYTIME
COPYSERVICES_HARDWARE_TYPE SVC
FLASHCOPY_TYPE NOCOPY
[...]
<<<
>>> DEVICE_CLASS MIDNIGHT
COPYSERVICES_HARDWARE_TYPE SVC
FLASHCOPY_TYPE INCR
SVC_COPY_RATE 80
[...]
<<<
```

Note: The time period that is specified cannot span midnight for a device class. If a device class time period is required to span midnight, you must specify two time periods for the device class. The first time period must end with a value 1 minute before midnight and the second time period must start at midnight. The following example shows how to specify a time period that spans midnight for a device class:

```
DEVICE_CLASS myClass FROM 20:00 TO 23:59
DEVICE_CLASS myClass FROM 00:00 TO 06:00
```

This example demonstrates how to create clone databases on different clone servers from the same production database. In this scenario, there are two clone servers, each one uses a different device class. The clone server host1 uses DEVICE_CLASS CLONE1 and host2 uses DEVICE_CLASS CLONE2. When a clone request is started with clone database B01 selected, this clone is created with DEVICE_CLASS CLONE1 and it is created on clone server host1.

```
>>> CLONING
DEVICE_CLASS CLONE1 USE_FOR_CLONING B01 C01
DEVICE_CLASS CLONE2 USE_FOR_CLONING B02 C02
<<<
>>> DEVICE_CLASS CLONE1
CLONE_DATABASE YES
...
<<<
>>> DEVICE_CLASS CLONE2
CLONE_DATABASE YES
...
<<<
```

Configuring for remote mirroring

When you configure Tivoli Storage FlashCopy Manager, you can set the configuration parameters to create snapshots by using target volumes of remote mirroring relationships. These target volumes are used to create application consistent snapshot backups.

Before you begin

Before, you configure Tivoli Storage FlashCopy Manager to use target volumes that are associated with remote mirroring one of the following technologies must be deployed:

- SAN Volume Controller or Storwize family Global Mirror and Metro Mirror
- IBM XIV Storage System Synchronous Remote Mirroring and Asynchronous Remote Mirroring

Procedure

1. To configure Tivoli Storage FlashCopy Manager with SAN Volume Controller or Storwize family Global Mirror and Metro Mirror, complete the following steps:
 - a. On the SAN Volume Controller or Storwize family system, create a partnership between the primary and auxiliary cluster. For example, you can run the following commands from the command-line interface:


```
ssh -i/dir/ssh-identity username@hostname or ip_primary_cluster
svctask mkpartnership -bandwidth bandwidth_in_mbps remote_cluster_name
or remote_cluster_id
```
 - b. Start the Global Mirror and Metro Mirror relationship by using either the graphical user interface or command-line interface. If you use the command-line interface, the following commands are provided as an example:


```
ssh -i/dir/ssh-identity username@hostname or ip_primary_cluster
svctask chpartnership -start remote_cluster_name or remote_cluster_id
```
 - c. Verify the following information about the environment:
 - Production volumes are on the primary storage system.
 - Production volumes are in a remote mirror relationship with the remote volumes that are either in the auxiliary cluster, or in the same cluster. All the remote mirror relationships are defined in a consistency group.
 - d. Run the setup script to configure a dedicated device class for the snapshot backups on the remote cluster. When you configure the new **DEVICE_CLASS** section with the setup script, look for the following prompt:

Is the FlashCopy/Snapshot taken from the mirror volumes {COPYSERVICES_REMOTE}.

Enter *yes*. The **COPYSERVICES_REMOTE_SERVERNAME**, **COPYSERVICES_REMOTE_USERNAME**, and **TAKEOVER_HOST_NAME** parameters are also required for remote mirroring.
 - e. On the remote cluster of the SAN Volume Controller or Storwize family, specify for each source the corresponding FlashCopy target volumes. To specify the FlashCopy target volumes, use one of the following options:
 - Parameter **TARGET_SETS** with **VOLUMES_FILE**. For example:


```
TARGET_SETS VOLUMES_FILE
VOLUMES_FILE /db2/DS0/acs/volumes/STANDARD_gm.fct
```
 - Parameter **TARGET_SETS** with **TARGET_NAMING**. For example:


```
TARGET_SETS dc2 dc3 dc4 dc5
TARGET_NAMING %SOURCEx%TARGETSET
```
2. To configure Tivoli Storage FlashCopy Manager with XIV Synchronous Remote Mirroring and Asynchronous Remote Mirroring, complete the following steps:
 - a. Define a coupling between peer volumes on the master and subordinate XIV systems, which creates a mirror relationship between the two.
 - b. Activate the XIV remote mirror couplings.
 - c. Define a coupling between peer consistency groups on the master and subordinate XIV systems, which creates a mirror relationship between the two.
 - d. Add volume mirror couplings to the consistency group couplings.

- e. Run the setup script to configure a dedicated device class for the snapshot backups on the remote cluster. When you configure the new `DEVICE_CLASS` section with the setup script, look for the following prompt:

Is the FlashCopy/Snapshot taken from the mirror volumes {`COPYSERVICES_REMOTE`}.

Enter *yes*. The `COPYSERVICES_REMOTE_SERVERNAME`, `COPYSERVICES_REMOTE_USERNAME`, and `TAKEOVER_HOST_NAME` parameters are also required for remote mirroring.

3. At the end of the setup script configuration process, verify the user name and password. When you see the following prompt, enter *yes*:

Do you want to continue by specifying passwords for the defined sections?

Example

The following information is provided as an example of how a team can complete asynchronous remote mirror configuration across two sites:

To configure Tivoli Storage FlashCopy Manager with IBM XIV Storage System with Asynchronous Remote Mirroring at both sites, certain ports must be open within the firewalls:

- On the production system, the production host, backup host, and primary XIV system must have ports open within the firewall.
- On the takeover system, the takeover host, backup host, and secondary XIV system must have ports open within the firewall.

For both the primary and secondary sites, the following ports must be open within the firewall:

- TCP port 3260 (iSCSI) open within firewalls for iSCSI replication
- Ports: http, https, ssh, and telnet
- TCP/IP ports: 55697, 5997, 5998, and 7778

All ports must be bidirectional.

Setting up the daemons on the production and backup systems

Before manually starting the Tivoli Storage FlashCopy Manager daemon processes, identify the daemons that must run on the production, backup, and cloning systems.

Procedure

You can manually set up the daemon processes. The following list specifies where the daemons can run.

- Run the following daemons on the production system only:
 - `INSTANCE_DIR/acsd` (management agent)
 - `INSTANCE_DIR/acsgen -D` (generic device agent)
- If offloaded backups are configured, run the following daemon on the production server:
`INSTANCE_DIR/fcmcli -D` (offload agent)
- Run the mount agent on all backup servers or cloning servers:
`INSTANCE_DIR/acsgen -D -M [-s deviceclass[,deviceclass]] [-H hostname]`

Postinstallation and configuration

After you install and configure Tivoli Storage FlashCopy Manager, you can set up extra backup and clone servers.

You can use the setup script to update the profile and configure Tivoli Storage FlashCopy Manager on multiple backup servers from the production server when you install Open Secure Shell (OpenSSH) to enable backup servers for remote installation and configuration from the production server. NFS shares between the production server and backup server are not required for this type of remote installation.

In a physically partitioned DB2 environment, installation and configuration are only required on one node of the production server, the master production server.

Upgrades and reconfiguration must be run only from the master production server node.

If OpenSSH is not available, follow the instructions for “Installing separately on backup or clone servers” on page 42 and run the setup script. Choose **On-site Backup server configuration** as the configuration type. Before you run the setup script on a backup or clone server, stop Tivoli Storage FlashCopy Manager on the production server. For details about how to stop an activated Tivoli Storage FlashCopy Manager instance, see Tivoli Storage FlashCopy Manager commands and scripts.

Typically, it is not necessary to run the setup script on the backup server after the initial configuration. Exceptions to this rule include:

- The use of alternative storage hardware might require a reconfiguration of Tivoli Storage FlashCopy Manager on the backup server.
- Changes to the scheduling policy for offloaded Tivoli Storage Manager backups might require you to configure the backup server again.
- If self-signed certificates are used, all changes to the certificates require a reconfiguration of the backup server.
- If OpenSSH is not used, you must copy the `fcmselcert.arm` file to the backup server before the setup script is run to configure the backup server again.

In these cases, stop Tivoli Storage FlashCopy Manager on the production server before reconfiguration of the backup server. Otherwise, you are prompted to stop Tivoli Storage FlashCopy Manager on the production server.

Related tasks:

Commands and scripts

Chapter 5. Backing up data

Instructions about how to back up DB2 (including SAP on DB2), Oracle, SAP® with Oracle databases, and custom applications using FlashCopy Manager for Custom Applications product are provided.

About this task

While Tivoli Storage FlashCopy Manager focuses on snapshot backups, the software can be integrated with Tivoli Storage Manager clients for offloaded backups to Tivoli Storage Manager.

Backup commands for DB2 databases

When you are backing up DB2 databases, use specific commands for your database configuration and backup type.

The following table summarizes the commands that are needed for backing up DB2 databases for different database configurations and corresponding backup types.

Table 5. Summary of backup commands for DB2 databases

Database configuration	Snapshot backup (disk only)	Back up to Tivoli Storage Manager		
		From production database (tape only)	Integrated with snapshot	From existing snapshot
DB2	<code>db2 backup ... use snapshot ...</code>	<code>db2 backup ... use tsm</code>	<code>db2 backup ... use snapshot ...¹</code>	<code>fmccli -f tape_backup²</code>
DB2 in an SAP environment	<code>db2 backup ... use snapshot ...</code>	<code>db2 backup ... load <library> or backom</code>	<code>db2 backup ... use snapshot ...¹</code>	<code>fmccli -f tape_backup²</code>
<p>Note:</p> <ol style="list-style-type: none">1. The profile parameter TSM_BACKUP is set to YES, MANDATE, or LATEST, and the offload agent (fmccli) is running in daemon mode on the production server.2. The profile parameter TSM_BACKUP is set to YES, MANDATE, or LATEST, and the offload agent (fmccli) is not running in daemon mode.				

The **db2 backup database** command with the use snapshot option is described in the *DB2 Command Reference* guide.

When you restore a backup image, the whole backup image is restored. Therefore, any data on the file system that is updated or created after the backup is taken is overwritten. To ensure that nothing is overwritten unintentionally, do not store any other data in the data and log volume groups. Any other data that is stored on the volume groups is processed by Tivoli Storage FlashCopy Manager and included in the backup image.

For DB2 pureScale, any additional files that are stored in log file sets and data file sets are included in the backup. When you restore a backup image, extra files and nested file sets are overwritten. To avoid overwriting, do not store any other files

in log file sets or database data file sets. Ensure that you do not link independent file sets containing unrelated data in file sets that participate in snapshots.

Extra files that are not associated with the database backup operation but are stored in the volume groups can cause the backup to fail. Use the **NEGATIVE_LIST** parameter in the Tivoli Storage FlashCopy Manager profile to control the processing of these files. For information about this parameter, see the “CLIENT” on page 143 profile section for details.

You can start a backup operation from any member of the DB2 pureScale instance. The Tivoli Storage FlashCopy Manager management agent *acsd* coordinates the backups and communicates between the application and device agents. The management agent is started automatically after the installation. If you are required to start the agent manually, this agent must not be started on more than one member. DB2 pureScale database is regarded as a single partitioned database.

Backing up DB2 databases

To protect data against the possibility of loss, ensure that you back up the DB2 database. Back up single partition, multi-partition, and pureScale databases with DB2 backup commands.

Procedure

1. Use the **db2 backup** commands when you are backing up DB2 databases with Tivoli Storage FlashCopy Manager.
2. Log on to one of the production hosts and use the DB2 instance owner ID.
3. Depending on the database you are backing up, type in one of the following commands:
 - Single partition database: **db2 backup db *dbname* use snapshot**
 - Multi-partition database: **db2 backup db *dbname* on all dbpartitionnums use snapshot**
 - DB2 pureScale database: **db2 backup db *dbname* use snapshot**
4. (Optional) To specify a different profile when you back up the database, enter the following command: **db2 backup db *dbname* on all dbpartitionnums use snapshot options "PROFILE=*path to new profile or name of new profile*"**

Serial and parallel backup modes for multi-partition DB2 database

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:

Serial mode

In serial mode that is used for non-SAP DB2 database, the partitions are processed sequentially. The following sequence of events is followed. Each partition is suspended. The snapshot is created and the partition is resumed before the next partition is processed. Tivoli Storage FlashCopy Manager returns an error during a backup if multiple partitions share a physical volume. A restore operation is always performed on a single partition.

Parallel mode

In parallel mode that is the 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. Tivoli Storage FlashCopy Manager allows multiple logical partitions to share a physical volume when these logical partitions are grouped in a **PARTITION_GROUP**. In this situation, **fcmccli** must be used to perform the restore. The restore proceeds in parallel for all the logical partitions that are specified in **PARTITION_GROUP**.

Related reference:

Appendix D, “Backup, restore, cloning commands, and utilities,” on page 265
“The fcmcli offload agent” on page 259

Backing up DB2 to a Tivoli Storage Manager server

Tivoli Storage FlashCopy Manager relies on standard DB2 mechanisms to back up a snapshot image to Tivoli Storage Manager.

Tivoli Storage FlashCopy Manager uses the following products to offload backups to Tivoli Storage Manager:

- IBM Tivoli Storage Manager for Enterprise Resource Planning in an SAP environment. This agent is not used in an IBM DB2 pureScale environment.
- DB2 Tivoli Storage Manager agent in a DB2 and DB2 pureScale environment.

Note: In an SAP environment, Tivoli Storage FlashCopy Manager can be configured to use the DB2 Tivoli Storage Manager agent. See the Tivoli Storage FlashCopy Manager **VENDOR_LIB** profile parameter in the offload section for details.

Use one of the following methods to offload a snapshot backup to Tivoli Storage Manager:

- When the offload agent (tsm4acs) is running, it queries periodically for snapshot backups where the **TSM_BACKUP** configuration parameter is set to YES, MANDATE, or LATEST, in the Tivoli Storage FlashCopy Manager profile file. The offload agent initiates a tape backup from the snapshot target set when the snapshot is created. The offload agent must be running in daemon mode on the production server.
- The **TSM_BACKUP** parameter is set to YES, MANDATE, or LATEST but the offload agent is not running then you must enter the following command **fcmccli -f tape_backup**. You must enter the command as the database instance owner on the production server. This command offloads a previously generated snapshot backup to Tivoli Storage Manager.

Tivoli Storage FlashCopy Manager, IBM Tivoli Storage Manager for Enterprise Resource Planning, and DB2 Tivoli Storage Manager agent, use their own profiles. To offload a backup to Tivoli Storage Manager, an OFFLOAD section must be present in the Tivoli Storage FlashCopy Manager profile file. This OFFLOAD section is created during the installation when the option to offload backups is selected.

When a profile is created or changed, the Tivoli Storage FlashCopy Manager configuration setup wizard, prompts you to specify whether offloaded backups are run. When YES is specified, the OFFLOAD section is added to the profile and the **TSM_BACKUP** parameter is added to the CLIENT section of the profile.

Back up commands for DB2 in a pureScale environment

When you are backing up DB2 databases in a DB2 pureScale environment, use specific commands for your database configuration and backup type.

To back up and restore a DB2 database in a DB2 pureScale environment, one of the following configurations must exist:

- The data and log files are in separate independent file sets within the same GPFS file system.
- The data and log files are in separate GPFS file systems.

The following table summarizes the commands that are needed, depending on the database configuration and the type of backup required.

Table 6. Summary of backup commands for DB2 in a pureScale environment. Summary of backup commands for DB2 in a pureScale environment

Database configuration	Snapshot backup (disk only)	Back up to Tivoli Storage Manager		
		From production database (tape only)	Integrated with snapshot	From existing snapshot
DB2 or DB2 in an SAP environment	<code>db2 backup use snapshot ...</code>	<code>db2 backup ...use tsm</code>	<code>db2 backup use snapshot¹</code>	<code>fmccli -f tape_backup²</code>
Note: 1. The profile parameter TSM_BACKUP is set to <i>YES</i> and the offload agent (fmccli) is running in daemon mode on the production server. 2. The profile parameter TSM_BACKUP is set to <i>YES</i> and the offload agent (fmccli) is not running in daemon mode.				

Any additional files that are stored in log file sets and data file sets are included in the backup. When you restore a backup image, extra files and nested file sets are overwritten. To avoid overwriting files, do not store any other files in log file sets or database data file sets. Ensure that you do not link independent file sets containing unrelated data in file sets that participate in snapshots.

Backing up DB2 (HADR) standby servers

You can use Tivoli Storage FlashCopy Manager to create snapshot backups of a DB2 High-Availability Disaster Recovery (HADR) standby server.

Although DB2 (HADR) standby server cannot be directly backed up to a Tivoli Storage Manager server, snapshot backups and subsequent backups of the snapshot files are possible. To ensure application consistency of the DB2 (HADR) standby database, the database must be deactivated or stopped before the snapshot is created. Then, after the snapshot is created the database must be reactivated or started again. Sample scripts that show you how to shut down and restart the DB2 (HADR) standby server are in the `INSTANCE_DIR` directory. You can customize these sample scripts. The scripts are available when Tivoli Storage FlashCopy Manager is configured for DB2 (HADR) standby server support. The sample scripts can be used as parameter values for the Tivoli Storage FlashCopy Manager profile **PRE_FLASH_CMD** and **POST_FLASH_CMD** parameters in the `DB2STANDBY` section of the profile file.

Enter the following commands to create snapshot backups of a DB2 (HADR) standby servers:

1. Log on to the DB2 (HADR) standby server and use the database instance owner user ID.
2. Change to the `INSTANCE_DIR` directory. For example, *DB2 instance owner* `$HOME/sql1lib/acs/`
3. Enter the following command:
`./fmccli -f backup_db2standby`

This command is a variant of the **fmccli -f backup** command that backs up custom database applications. Before Tivoli Storage FlashCopy Manager starts the backup process, Tivoli Storage FlashCopy Manager communicates with DB2 on the primary site to determine the list of database files that must be protected.

After a DB2 takeover, the DB2 (HADR) standby server becomes the DB2 (HADR) primary server. After this takeover, use the DB2 snapshot backup command for backup. Do not use the **backup_db2standby** command. Tivoli Storage FlashCopy Manager supports sharing the profile for both types of backups. You need only to use a different command to start your database backup that is dependent on the current DB2 HADR database role.

Use the same device classes for the DB2 snapshot backups, and for the DB2 (HADR) standby server backups.

Note: For DS8000 and SAN Volume Controller a DB2 snapshot backup can overwrite the backup from a DB2 (HADR) standby server backup. This situation occurs if there are different device classes for two backup types, but the same target volumes are used. The **inquire** command incorrectly indicates that both backups are valid.

Because Tivoli Storage FlashCopy Manager software cannot directly communicate with the standby server, Tivoli Storage FlashCopy Manager queries the DB2 instance that is running on the primary server by using DB2 remote connections. The software assumes that the file names for the production server database and the standby server database are identical. Tivoli Storage FlashCopy Manager can back up in situations where the DB2 automatic storage managed table spaces are in use, which can cause table space container IDs on the HADR primary and standby server not to match.

Although you cannot use DB2 commands to create a DB2 backup of the standby databases and offload directly to Tivoli Storage Manager, Tivoli Storage FlashCopy Manager starts a file-based Tivoli Storage Manager backup from the snapshot. You cannot use DB2 for a database restore from the file-based Tivoli Storage Manager backups. Use the Tivoli Storage Manager backup-archive client to restore the files that are backed up to the Tivoli Storage Manager server. Recover the database by using the DB2 **recover** command.

Backing up Oracle databases

Tivoli Storage FlashCopy Manager integrates with multiple components when you back up an Oracle database.

The following table summarizes the commands that are associated with backing up an Oracle database.

Table 7. Summary of Backup Commands for Oracle

Snapshot backup (disk only)	Back up to Tivoli Storage Manager		
	From production database (tape only)	Integrated with snapshot	From existing snapshot
acsora -f backup	RMAN by using Data Protection for Oracle	acsora -f backup ¹	fcmccli -f tape_backup ²
Note: 1. The Tivoli Storage FlashCopy Manager profile parameter TSM_BACKUP is set to one of the following options: YES, MANDATE, or LATEST, and the offload agent (tsm4acs) is running in daemon mode on the production server. 2. The profile parameter TSM_BACKUP is set to one of the following options: YES, MANDATE, or LATEST, and the offload agent is not running in daemon mode.			

You must use the Oracle instance owner ID and go to the `INSTANCE_DIR` directory before you enter any backup commands. Tivoli Storage FlashCopy Manager backs up the database control file and the database profile on the production server to the Tivoli Storage FlashCopy Manager repository. These files are required by Tivoli Storage FlashCopy Manager on the backup server to start the database instance and to run the offloaded backup to the Tivoli Storage Manager server. Furthermore, the database control file can be optionally restored during a FlashCopy restore (profile parameter **DATABASE_CONTROL_FILE_RESTORE**).

By default, the Tivoli Storage FlashCopy Manager software does not back up the transaction logs of the Oracle database. The database administrator is responsible for backing up the Oracle database transaction logs. After every full database online backup, back up the transaction logs to the Tivoli Storage Manager server.

The same commands can be used to back up Oracle databases that use Oracle Automatic Storage Management (ASM) and Oracle Real Application Clusters (RAC) based on Oracle ASM. An Oracle recovery database is required for Tivoli Storage FlashCopy Manager snapshot backups. This recovery database is a requirement even if a disk only backup is requested.

Backing up an Oracle database to Tivoli Storage Manager server

Tivoli Storage FlashCopy Manager require specific software when you back up an Oracle database to Tivoli Storage Manager server.

Before you back up to Tivoli Storage Manager server, ensure that the following requirements are met:

- Data Protection for Oracle must be configured on the backup server.
- A RMAN backup script that is 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. See “Example of the RMAN backup script” on page 230.

Manually backing up Oracle databases

A manual backup performs a one time backup of an Oracle database.

Procedure

1. Log on to the production server and use the database instance owner user ID.
2. Change to the `INSTANCE_DIR` directory.
3. Enter the following command:
`acsora -f backup`

Table 8. Files used during a manual backup

File name	Description	Default location
acsora	Tivoli Storage FlashCopy Manager production system executable file	<i>INSTANCE_DIR</i>
fccli	Tivoli Storage FlashCopy Manager production and backup system executable file	<i>INSTANCE_DIR</i>
profile	Tivoli Storage FlashCopy Manager profile	<i>ACS_DIR</i>

Automating Oracle database backups

A fully automated backup uses a server script to fully automate online backups of Oracle databases.

Synchronous and asynchronous offloaded backups are different. Synchronous means that the backup on the backup host starts as soon as a FlashCopy is started. In this case, the offload agent, `tsm4acs`, is started as a daemon by the `init` process. Asynchronous means that offloaded backups are triggered manually or triggered by another scheduler by starting the `fccli` agent. This type of backup is useful if the backup must be delayed until the required resources are available. During the configuration on the production server, you determine when to run the offloaded backups.

Backing up Oracle in an SAP environment databases

IBM Tivoli Storage FlashCopy Manager integrates with multiple components when you back up an Oracle in an SAP environment database.

The following table summarizes the commands that are associated with backing an SAP database with Oracle.

Table 9. Summary of backup commands (SAP with Oracle)

Snapshot backup (disk only)	Back up to Tivoli Storage Manager		
	From production database (tape only)	Integrated with snapshot	From existing snapshot
<code>brbackup -d util_vol ...</code>	<code>brbackup -d util_file ...</code>	<code>brbackup -d util_vol¹</code>	<code>fccli -f tape_backup²</code>

Table 9. Summary of backup commands (SAP with Oracle) (continued)

Snapshot backup (disk only)	Back up to Tivoli Storage Manager		
	From production database (tape only)	Integrated with snapshot	From existing snapshot
<p>Note:</p> <ol style="list-style-type: none"> 1. The Tivoli Storage FlashCopy Manager profile parameter TSM_BACKUP is set to one of the following options: YES, MANDATE, or LATEST, and the offload agent (tsm4acs) is running in daemon mode on the production server. 2. The profile parameter TSM_BACKUP is set to one of the following options: YES, MANDATE, or LATEST, and the offload agent is not running in daemon mode. 			

The following parameters are used in the SAP BR*Tool configuration files `initDBSID.sap` in the following scenarios. These configuration files are only needed on the production server.

backup_dev_type

Determines the backup medium that is used. The default is tape. To create a snapshot backup by using Tivoli Storage FlashCopy Manager, this parameter must be set to `util_vol` or to `util_vol_online`. Creating snapshot backups, minimizes the time during which the database is degraded by the Oracle begin backup command.

backup_mode

Identifies the scope of the backup. This parameter is only used by `brbackup`. The default is `all`; however, if the parameter is set to `all` and Oracle RMAN is used, an incremental offload to Tivoli Storage Manager backup cannot be created. When the **backup_mode** parameter is set to `all`, a backup of all data files is completed by using the `backint` interface.

For an incremental offload to Tivoli Storage Manager backup of an SAP with Oracle database by using Oracle RMAN, set the BR*Tools option for the **backup_mode** parameter to `full`.

util_par_file

Specifies the path to the profile (sent to **backint** by using the `-p` parameter). Typically this profile is the Tivoli Storage Manager for ERP `.utl` file.

util_path

Specifies the path to the **backint** executable file. If not specified, the **backint** executable file in `/usr/sap/SID/SYS/exe/run` directory is used.

util_options

Specifies the option argument, which is appended to the **backint** call.

util_vol_unit

Specifies the smallest unit that can be backed up with a snapshot or clone.

util_vol_nlist

Specifies a list of non-database files or directories that are on the database disk volume. To disable SAP BR*Tools from checking for more files, specify `util_vol_nlist = no_check`. However, when you specify `util_vol_nlist = no_check`, SAP BR*Tools not only copies those files during backup, but also overwrites those files during restore processing.

Backup scenario 1: Tivoli Storage FlashCopy Manager snapshot backup (disk-only)

This scenario demonstrates how the SAP BR*Tool brbackup interacts with Tivoli Storage FlashCopy Manager during backup operations. The SAP BR*Tool brbackup calls backint with these command-line parameters:

-t volume, -t volume_online

Tivoli Storage FlashCopy Manager (backint) uses the snapshot technology available on the FlashCopy device.

-t file, -t file_online

Tivoli Storage FlashCopy Manager (backint) transfers the Oracle control files into the Tivoli Storage FlashCopy Manager repository. Because Tivoli Storage Manager for ERP is not installed in this scenario, backint is not available in the `/usr/sap/SID/SYS/exe/run` directory. Therefore, the **util_path** parameter must specify the Tivoli Storage FlashCopy Manager `INSTANCE_DIR` in the SAP BR*Tools profile (`initDBSID.sap`).

An SAP BR*Tools backup run is split into three phases:

1. Back up Oracle database files by using the **-t volume | -t volume_online** option.
2. Back up Oracle control files by using the **-t file | -t file_online** option.
3. Back up the configuration and log files by using the **-t file | -t file_online** option.

When Tivoli Storage FlashCopy Manager is configured for stand-alone disk-only backup, Tivoli Storage FlashCopy Manager creates a disk-only snapshot backup of the database files on the storage system. Similarly, a disk-only backup for phase 2 and phase 3 is created by copying the requested files into the Tivoli Storage FlashCopy Manager repository. The configuration in this scenario is for a disk-only backup.

Contents of the SAP BR*Tools profile (`initDBSID.sap`):

```
backup_dev_type = util_vol | util_vol_online
util_par_file = ACS_DIR/profile
util_path = INSTANCE_DIR
```

Settings of the Tivoli Storage FlashCopy Manager profile `ACS_DIR/profile`:

```
TSM_BACKUP NO
```

However, such an operation must not be run unless necessary because the Oracle control files and other files are transferred into the repository. These additional files in the Tivoli Storage FlashCopy Manager repository can cause performance issues that are related to back up, restore, and space availability. Even for disk-only backups, an integration with Tivoli Storage Manager or a third-party tape backup product is the preferred solution. For more information about this solution, see the following backup scenarios.

Backup scenario 2: Tivoli Storage FlashCopy Manager and Tivoli Storage Manager for ERP installed

This scenario demonstrates how the same backint profile (`initDBSID.utl`) and SAP BR*Tools profile (`.sap`) can be used for a disk-only backup and a dual backup.

The SAP BR*Tools profile (`.sap`), is only needed on the production server. A *backint* profile, `initDBSID.utl`, is needed on the production and backup server. The content

of the *backint* profiles can be the same on both servers. A Tivoli Storage FlashCopy Manager profile *ACS_DIR/profile* is needed on the production and backup server. Both files are created by using the profile wizard. The following figure illustrates how the different profiles work together.

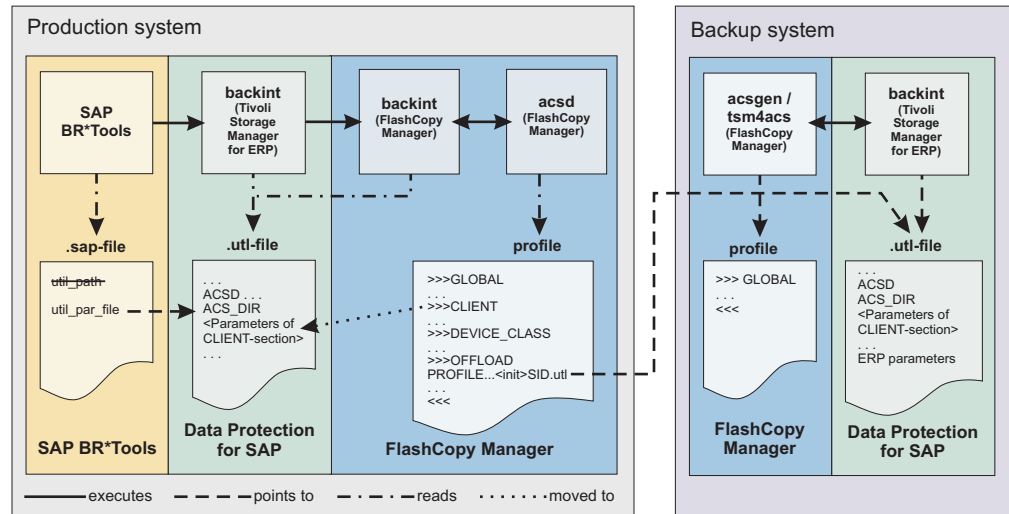


Figure 8. The backup profiles on the production and backup systems

A disk-only backup is a backup that is created by using snapshot technology with Tivoli Storage FlashCopy Manager. The backup is not copied to Tivoli Storage Manager.

A Tivoli Storage Manager only backup is a snapshot that is created for the sole purpose of creating a Tivoli Storage Manager backup from it. The snapshot is mounted on a secondary system and copied to Tivoli Storage Manager for that purpose.

A dual backup is a hybrid of a disk-only and a Tivoli Storage Manager only backup. A dual backup is a disk-only backup that is also copied to Tivoli Storage Manager. At least two device classes are needed in the Tivoli Storage FlashCopy Manager profile.

One device class is used for disk-only backups and one device class is used for dual backups. The **TSM_BACKUP_FROM_SNAPSHOT** parameter value depends on the device class because of the **USE_FOR** settings. The profile is configured so that it can be used for a disk-only backup and a dual backup.

Important: For this configuration, the Tivoli Storage FlashCopy Manager profile has no **CLIENT** section. You must add the **CLIENT** section parameters manually to the **.utl** file. After you add, the **TSM_BACKUP** parameter to the **.utl** file, you must rename the parameter to **TSM_BACKUP_FROM_SNAPSHOT**. Also, after you add the **MAX_VERSIONS** parameter you must rename the parameter to **MAX_SNAPSHOT_VERSIONS**. For a complete list of profile parameters to add to the **.utl** file, see the “BACKINT configuration file” on page 207 in the configuration files section.

Note: Ensure that the added parameters are placed before the first **SERVER** statement in the **.utl** file.

The following two links are automatically created during the installation and configuration of Tivoli Storage FlashCopy Manager and are used in this scenario:

- A link that is named *backint* in `/usr/sap/SID/SYS/exe/run` points to backint that is in the Tivoli Storage Manager for ERP installation directory.
- A link that is named *backint_volume* in `/usr/sap/SID/SYS/exe/run` points to backint that is in the Tivoli Storage FlashCopy Manager installation directory.

Settings of the common Tivoli Storage FlashCopy Manager .utl file (commonprofile.utl):

```
TSM_BACKUP_FROM_SNAPSHOT NO USE_FOR DISKONLY
TSM_BACKUP_FROM_SNAPSHOT LATEST USE_FOR DUAL
DEVICE_CLASS DISKONLY USE_AT Mon Wed Fri
DEVICE_CLASS DUAL USE_AT Sun Tue Thu Sat
```

Note: The use of multiple device classes and **TSM_BACKUP_FROM_SNAPSHOT** parameters in the SAP backint profile requires Tivoli Storage Manager for ERP 6.1.1 or later. For earlier releases of Tivoli Storage Manager for ERP, control the device class by defining multiple BR*Tools configuration profiles (.sap) in your environment.

Contents of the common SAP BR*Tools profile (initDBSID.sap):

```
backup_dev_type = util_vol | util_vol_online
util_par_file = ORACLE_HOME/dbs/initDBSID.utl
```

- Tivoli Storage FlashCopy Manager is called with **-t volume** or **-t volume_online** to run the snapshot part of the backup.
- The SAP control files are backed up to the Tivoli Storage Manager server for disk-only and dual backups. Use this backup location for the control files. To back up the control files into the Tivoli Storage FlashCopy Manager repository, specify the Tivoli Storage FlashCopy Manager installation directory with the `util_path` option in the SAP BR*Tools profile (initDBSID.sap).

The Tivoli Storage Manager for ERP executable file is called from `/usr/sap/SID/SYS/exe/run` and calls the **backint_volume**, which links to Tivoli Storage FlashCopy Manager to run the snapshot part of the backup. Calling Tivoli Storage FlashCopy Manager with the options `-t file` | `-t file_online` fails when the parameter **TSM_BACKUP_FROM_SNAPSHOT=YES** is specified. This failure occurs because, during dual backups, the Oracle control files must be backed up to Tivoli Storage Manager.

During the restore operation, the same `initDBSID.sap` files that are used during the original backup operation must be specified. For dual backups with Tivoli Storage FlashCopy Manager and Tivoli Storage Manager for ERP, use the `initDBSID.sap` file to restore both disk-only and dual backups. Tivoli Storage Manager for ERP delegates the restore of the snapshot backup to Tivoli Storage FlashCopy Manager.

Incremental backups of an SAP with Oracle database using Oracle RMAN

IBM Tivoli Storage Manager for Enterprise Resource Planning provides incremental backups that allow only the blocks that changed in the database to be offloaded to a Tivoli Storage Manager backup. This method reduces the required space for the backend storage dramatically.

A full backup must exist before an incremental backup can be created. If there is no full backup, it is created automatically by RMAN when called by Tivoli Storage Manager for ERP.

RMAN incremental backups are enabled by using profile parameters in the Tivoli Storage Manager for ERP configuration file (.utl file).

To run an incremental level 1 backup on weekdays and a level 0 full backup on Sunday, the following parameters must be added to the Tivoli Storage Manager for ERP configuration file (.utl file):

```
INCREMENTAL_LEVEL      1 USE_AT MON TUE WED THU FRI SAT
INCREMENTAL_LEVEL      0 USE_AT SUN
```

In this scenario, an Oracle recovery catalog database is required. This action must be run on the production and on the backup host. The recovery catalog database requires a password. This password can be set by entering the following command:

```
backint -p profile -f catalog_password
```

Backup scenario 3: Tivoli Storage FlashCopy Manager and third-party tape backup product

This scenario demonstrates how Tivoli Storage FlashCopy Manager and a third-party tape backup product are used in parallel. To run disk-only backups, the contents of the SAP BR*Tools profile (initDBSID.sap) and the Tivoli Storage FlashCopy Manager profile (ACS_DIR/profile) are the same as shown in the first scenario.

The following two alternative methods can be used to run a tape backup:

1. Offload the snapshot that is managed by Tivoli Storage FlashCopy Manager to tape from a backup server with a third-party product. In this case, you must mount the snapshot to a backup server by using the **fcmlcli -f mount** command. You can offload the mounted backup to tape and unmount the snapshot by using **fcmlcli -f unmount**. In this scenario, your tape backup product must be able to do a redirected restore to the production system.
2. Complete a tape backup from the production system with a third-party product and use Tivoli Storage FlashCopy Manager to create complementary snapshot backups for faster recovery.

In this case, you can use the third-party tool configuration as-is without any changes because the Tivoli Storage FlashCopy Manager installation does not replace the backint executable file. This file is in /usr/sap/SID/SYS/exe/run directory that is provided by the third-party vendor. For this Tivoli Storage FlashCopy Manager configuration, you can proceed exactly as described in the first scenario.

Related reference:

“Oracle in an SAP environment BR*Tools configuration profile (.sap)” on page 218

Automate backups of Oracle in an SAP environment

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.

The SAP® DBA Planning Calendar (either transaction DB13 or DBACOCKPIT) can be used to schedule backups with Tivoli Storage FlashCopy Manager when the SAP® BR*Tools profile (initDBSID.sap) is set up correctly.

Backing up file systems or custom applications

Tivoli Storage FlashCopy Manager software provides an application agent, the FlashCopy Manager for Custom Applications to back up file systems and custom applications.

You can use Tivoli Storage FlashCopy Manager to create a consistent snapshot image of a file system and custom application on a production system. Custom applications are applications that are on file systems that are supported by Tivoli Storage FlashCopy Manager and that are not explicitly supported. Examples of custom applications are Domino®, MAX DB, and WebSphere®. The snapshots are managed as backup versions by using the version management policies of Tivoli Storage FlashCopy Manager. The snapshots can be used as a source for snapshot restore operations.

You can mount these snapshot backups on a secondary server. In a Tivoli Storage Manager environment, you can use the Tivoli Storage Manager backup archive client to initiate a subsequent backup to a Tivoli Storage Manager server.

You can use the `fcmlcli -f backup` command to protect any application on a file system that is supported by Tivoli Storage FlashCopy Manager.

The following scenario explains the backup of a Tivoli Storage Manager server. In this scenario, the custom application is the Tivoli Storage Manager server:

1. Create a list of files and directories that you want to back up. Save the list to a file that is later used by Tivoli Storage FlashCopy Manager as an input *infile* file. This file can contain a list of the directories for the DB2 table spaces, and the online redo logs. If the storage device supports space-efficient snapshots, include the Tivoli Storage Manager disk storage pools. For example, include file pools and the active storage pool. This solution provides you with a consistent image of the system as of the time when the snapshot is created.
2. Create a `preflash.sh` and `postflash.sh` script files to shut down and restart the Tivoli Storage Manager server. Use the Tivoli Storage FlashCopy Manager configuration setup script to add these scripts to the CLIENT section of the Tivoli Storage FlashCopy Manager profile as values for the **PRE_FLASH_CMD** and **POST_FLASH_CMD** parameters.
3. Enter the following command to create a snapshot backup of the environment:

```
fcmlcli -f backup -I infile -p profile
```

Tivoli Storage FlashCopy Manager calls the `preflash.sh` script. After Tivoli Storage FlashCopy Manager creates the snapshot on the storage system it calls the `postflash.sh` script to restart the Tivoli Storage Manager server. The

snapshot represents an offline backup of the Tivoli Storage Manager database. The Tivoli Storage Manager server is offline only for a short time.

4. Depending on the value of the parameter **TSM_BACKUP** in the Tivoli Storage FlashCopy Manager profile file, Tivoli Storage FlashCopy Manager can start a Tivoli Storage Manager backup of the snapshot image by using the backup-archive client.

The snapshot must be backed up to another Tivoli Storage Manager server to obtain a useful backup.

FlashCopy backup of individual mirrors

Tivoli Storage FlashCopy Manager supports mirroring.

Mirroring using the AIX logical volume manager (LVM mirroring)

Tivoli Storage FlashCopy Manager provides LVM mirroring support for DS8000, IBM XIV Storage System, Storwize family, SAN Volume Controller, IBM System Storage N series, and NetApp. For those devices, Tivoli Storage FlashCopy Manager creates a FlashCopy backup where only one of the mirrors is copied during the backup. When LVM is used to mirror the database across sites, you can create offloaded tape backups on either site with Tivoli Storage FlashCopy Manager. In this situation, you do not have to transfer the backup image across sites. To complete this task, a backup server is required on either site where backup images can be mounted to transfer them to secondary backup media. For DS8000, you can create at most one INCREMENTAL FlashCopy per source volume. However, in LVM environments, each source volume is mirrored. Therefore, Tivoli Storage FlashCopy Manager can create two INCREMENTAL FlashCopy backups for DS8000.

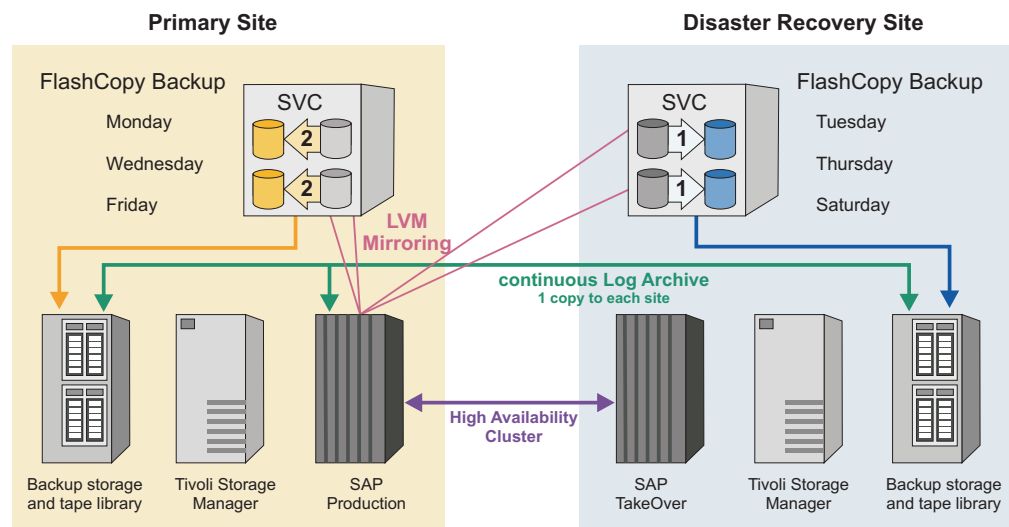


Figure 9. Cross-site mirrored SAP® database protected with Tivoli Storage FlashCopy Manager and Tivoli Storage Manager.

Support of AIX enhanced concurrent capable volume groups

To support high-availability environments, Tivoli Storage FlashCopy Manager supports enhanced concurrent capable volume groups.

Support of Oracle Automatic Storage Management (ASM) Failure Groups

Oracle ASM organizes data in disk groups that consist of a collection of disk drives that are in the same loop as configured by the storage subsystem. Tivoli Storage FlashCopy Manager uses an ASM instance to map these disk groups to physical disks. Each disk group can have multiple failure groups that are redundant copies of each other. These failure groups can be used as a technique to mirror storage volumes. To use this technique, define disk groups with normal redundancy that are composed of two failure groups, and place the volumes for each of the failure groups on a dedicated storage cluster. Alternatively, define disk groups with high redundancy that are composed of three failure groups. Although the default Oracle System ID (SID) for the ASM instance is +ASM, other SIDs are supported.

In such a configuration, Tivoli Storage FlashCopy Manager can create FlashCopy backups of an individual failure group for all of the following supported storage devices:

- DS8000
- Storwize family
- SAN Volume Controller
- IBM XIV Storage System
- IBM System Storage N series
- NetApp

Heterogeneous device mirroring

Tivoli Storage FlashCopy Manager does not require the storage devices of different mirrors to be at the same version level.

Backing up data with remote mirroring

When you back up data with remote mirroring, you can create local and remote snapshot backups.

About this task

The local and remote snapshot backups can be created for the following databases and applications:

- Oracle databases.
- Oracle in an SAP environment databases.
- DB2 databases.
- Custom applications that use a generic backup agent. This agent creates snapshots of other applications or databases that are on file systems that are supported by Tivoli Storage FlashCopy Manager.

The instructions that are provided can be applied to the following scenarios:

- SAN Volume Controller FlashCopy backup at the auxiliary cluster with either Metro Mirror or Global Mirror
- XIV system snapshot backup at the remote site with either Synchronous Remote Mirroring or Asynchronous Remote Mirroring

To create local application-consistent snapshot backups with the source volumes of the system that is running remote mirroring, verify that one `DEVICE_CLASS` section

is configured for the primary cluster. The production volumes are on the primary cluster. You can run the setup script to create or change `DEVICE_CLASS` sections. From the production host, start the local snapshot backup. There are no additional requirements.

To create application-consistent remote snapshot backups with the target volumes of the storage system that is running remote mirroring, complete the following steps. The first few steps do not include all details that are needed to complete the step. These steps are usually completed before you start the following procedure. The information is provided for your convenience. You can verify that you have the environment set up completely before the backup begins.

Procedure

1. Verify Tivoli Storage FlashCopy Manager is installed in an environment where you have either a supported database or custom application that is running on the primary cluster. The primary cluster is mirrored to a remote cluster with the storage feature for remote mirroring.
2. Use the setup script wizard to configure Tivoli Storage FlashCopy Manager for remote mirroring. When configuring for remote mirroring, the following parameters are set in the `DEVICE_CLASS` section:
 - `COPYSERVICES_REMOTE YES`
 - `COPYSERVICES_REMOTE_SERVERNAME SERVER_NAME`
 - `COPYSERVICES_REMOTE_USERNAME USER_NAME`
 - `TAKEOVER_HOST_NAME HOST_NAME`
3. At the end of the setup script wizard, the following question is displayed:
Do you want to continue by specifying passwords for the defined sections?
Enter *y* for yes.
4. Verify that the `DEVICE_CLASS` section, created for remote mirroring during the configuration process, is selected. To verify, go to the `CLIENT` section of the profile. In the `CLIENT` section, the `DEVICE_CLASS` to use is selected. When backing up data stored on Oracle in an SAP environment databases, the `DEVICE_CLASS` is specified in the SAP backup `.utl` file.
5. From the production host, use one of the following commands to start the remote snapshot backup:

DB2 database, remote FlashCopy backup, single partition database

```
db2 backup db dbname use snapshot
```

DB2 database, remote FlashCopy backup, multi-partition database

```
db2 backup db dbname on all dbpartitionnums use snapshot
```

Oracle database, remote FlashCopy backup

```
acsora -f backup
```

Oracle in an SAP environment, remote FlashCopy backup

```
brbackup -p /oracle/SID/dir/initSID.sap -t online -d  
util_vol_online -c
```

Custom application agent, remote FlashCopy backup

```
fccli -f backup
```

When a FlashCopy backup is attempted, but the remote mirroring relationships are not synchronized, the backup fails and an error message is displayed. Before you can back up data, the mirroring relationships must be in the consistent synchronized state.

There is a FlashCopy consistency group created in the remote cluster. The target of the mirroring relationships is the source of this new FlashCopy consistency group.

6. To verify that the backup is complete, from a command prompt window, enter the following command:

```
fcmcli -f inquire_detail
```

You can also run the following commands:

- To mount the backup, from a command prompt window, enter the following command: **fcmcli -f mount**
- To unmount the backup, from a command prompt window, enter the following command: **fcmcli -f unmount**

Usability states of snapshot backup operations

To view the usability states of a snapshot backup, use the **-f inquire_detail** command option with the application-specific commands for example **fcmcli**, **acsora**, or **backint**.

To see the states of a DB2 snapshot backup for example, enter the following command: `./fcmcli -f inquire_detail`. The output from this command shows a comma-separated list of the current usability states.

```
...
Type      Partition Backup-ID      TSM Backup-ID  State      DevClass TargetSet BackgroundCopy
BytesToBeFlashCopied

#BACKUP NODE0000 20130827214721 -          IN_PROGRESS MIRROR1 1          3.000 GB of 3.000 GB
3.000 GB
UsabilityStates: REMOTELY_MOUNTABLE,REPETITIVELY_RESTORABLE,SWAP_RESTORABLE,PHYSICAL_PROTECTION,FULL_COPY,
TAPE_BACKUP_PENDING,TAPE_BACKUP_FAILED
...
```

A snapshot backup generation can have one or more of the following states to indicate how it can or must be used by other Tivoli Storage FlashCopy Manager functions.

Table 10. Usability states

Usability state value	Meaning
REMOTELY_MOUNTABLE	Backup data can be mounted from a remote system.
REPETITIVELY_RESTORABLE	Backup data can be restored. The image can be used multiple times.
DESTRUCTIVELY_RESTORABLE	Data can be restored. After the restore, other backups and possible the backup to be restored can potentially be deleted.
SWAP_RESTORABLE	Restore is possible by using the backup volumes directly rather than copying the data back to the source volumes.
PHYSICAL_PROTECTION	The snapshot ensures protection from physical failures on the source volumes, there is no longer a dependency on the source volumes. This state does not necessarily mean that a FULL_COPY must be created with each snapshot. For example, block-level continuous data protection (CDP) mechanisms typically replicate the data only once, and then record changes only.
FULL_COPY	A full copy of the data was generated.

Table 10. Usability states (continued)

Usability state value	Meaning
INCOMPLETE	A portion of the data that was backed up is deleted and can no longer be restored. This situation can happen, for example, after a partial restore of an old backup that is only DESTRUCTIVELY_RESTORABLE .
MOUNTING	A mount operation was requested on the backup server.
MOUNTED	This backup is mounted on a backup server.
DELETING	Indicates that a backup is marked for deletion. The deletion was requested.
DELETED	Indicates that the backup was deleted.
BACKGROUND_MONITOR_PENDING	Indicates that a required background copy process is not yet active or not yet finished. The device agent checks for backups with this state and monitors the associated volumes until the background copy is finished. This state is then replaced by FULL_COPY .
TAPE_BACKUP_PENDING	Indicates that a requested tape backup is not yet started or is not yet finished successfully. The offload agent checks for backups with this state, and runs the requested tape backup. After the tape backup finishes successfully, this state is reset. If the tape backup stops with an error, the TAPE_BACKUP_PENDING state remains set, TAPE_BACKUP_IN_PROGRESS is reset, and a <i>retry</i> counter is incremented.
TAPE_BACKUP_IN_PROGRESS	Indicates that the requested tape backup was started by the Tivoli Storage FlashCopy Manager offload agent. If the backup fails, this state is reset. In a DB2 DPF environment, this state is used to indicate that some partitions are successfully backed up and others are still pending backup to tape.
TAPE_BACKUP_COMPLETE	Indicates that the requested tape backup is finished by the Tivoli Storage FlashCopy Manager offload agent. In a DB2 DPF environment, the TAPE_BACKUP_COMPLETE state is set when all the partitions of the database are successfully backed up to tape.
TAPE_BACKUP_FAILED	Indicates that the tape backup of the Tivoli Storage FlashCopy Manager offload agent was not successful. In a DB2 DPF environment, the TAPE_BACKUP_FAILED state is set when at least one partition of the database failed during tape backup.
CLONE_DATABASE	Indicates that a Tivoli Storage FlashCopy Manager cloning operation was run.
RESTORING	Indicates that a Tivoli Storage FlashCopy Manager restore operation was run.

Usability state diagrams

The following usability state diagrams show the state changes during different operations. The green arrows are used for actions that you can start. The blue arrows are used for actions that are done automatically by Tivoli Storage FlashCopy Manager. The black arrows indicate Tivoli Storage FlashCopy Manager operations that you can use to change usability states.

Snapshot backup

The first state diagram shows the usability state changes during a Tivoli Storage FlashCopy Manager snapshot backup operation. Depending on the storage system (DS8000, SAN Volume Controller, XIV system, IBM System Storage N series, and NetApp) some states differ.

For example, on XIV system, IBM System Storage N series, and NetApp, the snapshot backup is immediately restorable and the restore can be repeated multiple times. On DS8000 and SAN Volume Controller the snapshot backup requires a background monitoring operation (**acsngen -D**) that removes the **BACKGROUND_MONITOR_PENDING** state and instead sets the **FULL_COPY** and **PHYSICAL_PROTECTION** state. This requirement depends on the FlashCopy type that was used for the snapshot backup. Background monitoring operations (**acsngen -D**) are automatically running.

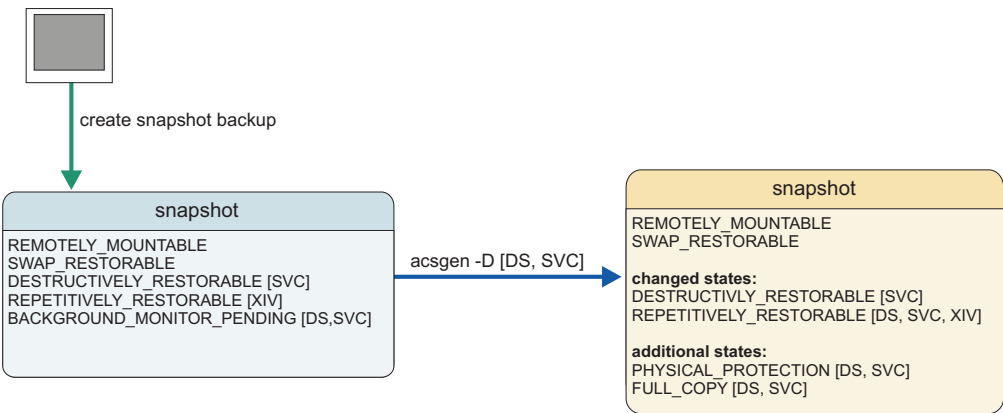


Figure 10. Usability States during snapshot backup

Snapshot restore

The second state diagram shows the usability state changes during a Tivoli Storage FlashCopy Manager snapshot restore operation. On the DS8000 and SAN Volume Controller storage systems, the usability states change during a snapshot restore operation.

For DS8000 and SAN Volume Controller systems, the **BACKGROUND_MONITOR_PENDING** state is turned on and in a **RESTORING** state. The background monitor process (**acsngen -D**) resets both states when the copy process in the storage system finishes. Background monitoring operations (**acsngen -D**) are automatically running.

For XIV system, IBM System Storage N series, and NetApp, there is no usability state change. However, in IBM System Storage N series, and NetApp environments, when you use an existing snapshot in a restore operation more recent existing snapshots become unusable. The reconcile process detects the

unusable snapshots and removes the backups from the repository.

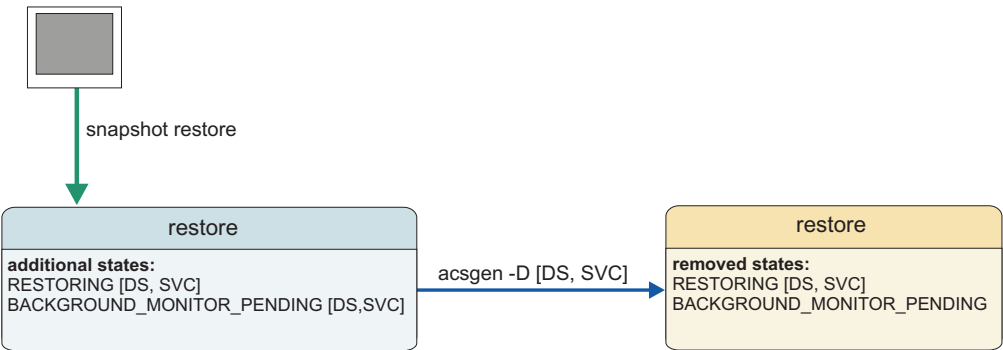


Figure 11. Usability states during snapshot restore

Snapshot delete

The next state diagram shows the usability state changes during a Tivoli Storage FlashCopy Manager snapshot delete operation. There are two types of delete operations: delete and delete with force option. For both types, the snapshot backup is marked with the **DELETING** state and a background monitoring operations (**acsgen -D**), which is running automatically in background, switches the states to **DELETED**. On the XIV system, IBM System Storage N series, and NetApp storage solutions the snapshot in the XIV system, IBM System Storage N series, and NetApp is deleted by the background monitor agent and the snapshot backup is also deleted from the Tivoli Storage FlashCopy Manager repository.

On the DS8000 and SAN Volume Controller storage systems, the FlashCopy relations are not deleted by the background monitor operation unless the delete force option was used on the delete command. On the DS8000 and SAN Volume Controller systems, the snapshot backup is not deleted from the Tivoli Storage FlashCopy Manager repository. Instead, a deleted snapshot backup can be reused by a new creation of a snapshot backup.

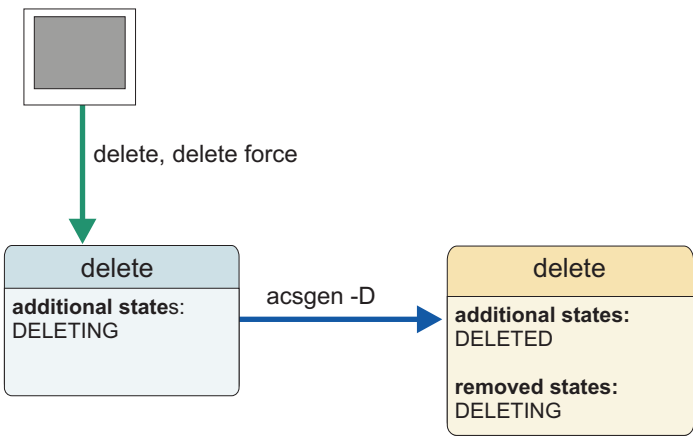


Figure 12. Usability states during snapshot delete

Snapshot mount

The next state diagram shows the usability state changes during a Tivoli Storage FlashCopy Manager snapshot mount operation. You can start a snapshot mount

operation by using the mount function of the FlashCopy Manager command-line interface or start it automatically during the creation of a snapshot backup. In the latter case, it is named a forced mount operation. In either case, the mount operation first changes the state to **MOUNTING**. If the mount operation finishes successfully, the state changes from **MOUNTING** to **MOUNTED**. If the mount operation fails, the state stays **MOUNTING**. The only operation that is allowed to remove a **MOUNTING** or **MOUNTED** state is a successful Tivoli Storage FlashCopy Manager unmount operation. If the unmount operation finishes successfully, the **MOUNTING** or **MOUNTED** state is removed. If the unmount operation fails, the state remains as **MOUNTING** or **MOUNTED**. An unmount force operation is not needed for unmounting unless an offloaded tape backup is in progress.

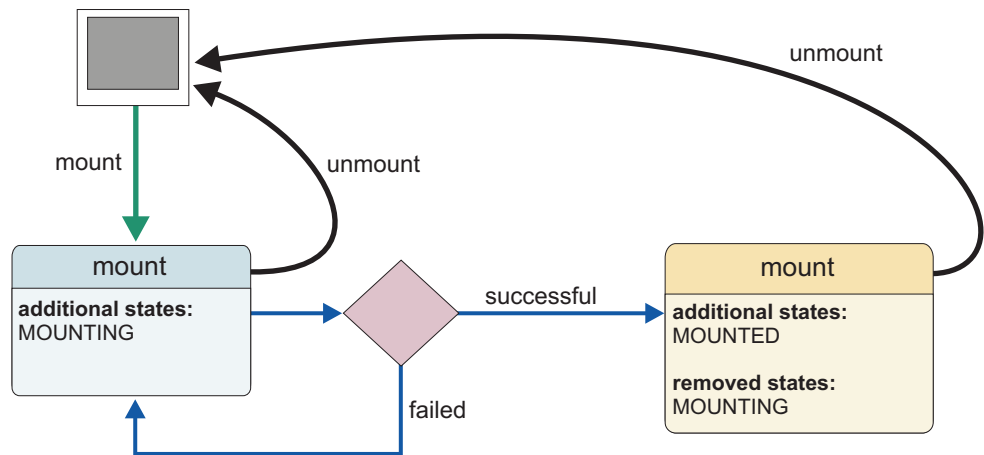
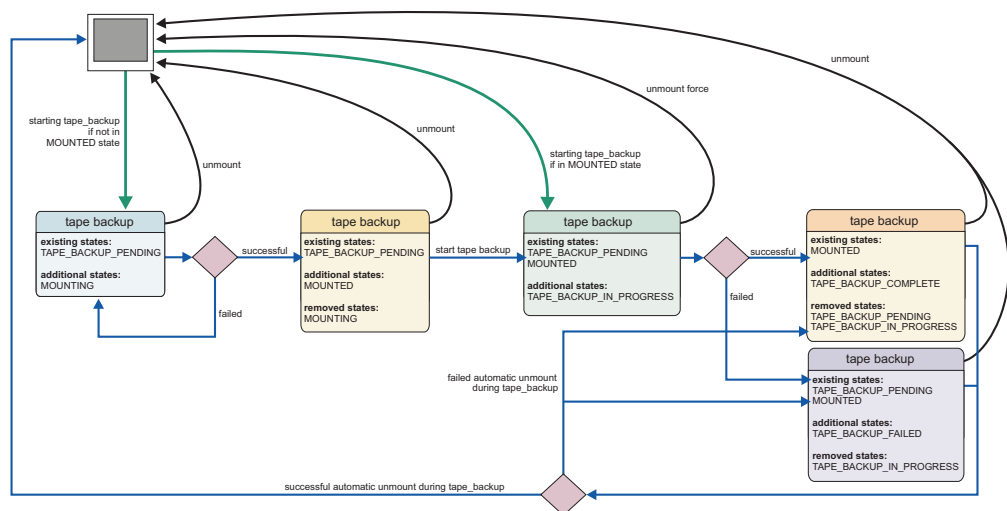


Figure 13. Usability states during snapshot mount

Snapshot offload

The last state diagram shows the usability state change during a Tivoli Storage FlashCopy Manager snapshot offload operation. You can start a snapshot offload operation with the **tape_backup** function of the FlashCopy Manager command-line interface. Alternatively, run it automatically with the offload agent that is running in the background (**fcmccli -D**). If the snapshot backup is not already mounted successfully, a mount operation is started automatically. The mount operation changes the state first to **MOUNTING** and then to **MOUNTED**. After that or in case that the snapshot backup was already mounted, the offload operation adds the state **TAPE_BACKUP_IN_PROGRESS** and runs the offloaded tape backup. If this operation is successful, the state switches from **TAPE_BACKUP_IN_PROGRESS** to **TAPE_BACKUP_COMPLETE**. Otherwise, the **TAPE_BACKUP_IN_PROGRESS** state switches to a **TAPE_BACKUP_FAILED** state and the **TAPE_BACKUP_PENDING** state persists. In either case, the automatic unmount operation is started and the **MOUNTED** state is removed when the operation completes successfully. If the mount operation fails, or the tape backup operation stops then the **MOUNTED** or **MOUNTING** state remains. The only operation that can remove these states is a successful Tivoli Storage FlashCopy Manager unmount operation. If the unmount operation finishes successfully, the **MOUNTED** or **MOUNTING** state is removed. If the unmount operation fails, the states are not removed. An unmount force operation is only needed for unmounting when an offloaded tape backup is in progress (**TAPE_BACKUP_IN_PROGRESS** is still set). The unmount force operation resets the **TAPE_BACKUP_IN_PROGRESS** state when it successfully completes the unmount operation.



The usability state **TAPE_BACKUP_PENDING** can be removed by using the Tivoli Storage FlashCopy Manager function **update_status** with the option **-S TSM_BACKUP=NO**. This state is also removed by starting a new snapshot backup with the option **TSM_BACKUP[_FROM_SNAPSHOT] LATEST**. This option automatically removes the usability state **TAPE_BACKUP_PENDING** from all snapshot backups that exist in the Tivoli Storage FlashCopy Manager repository.

Chapter 6. Restoring data

Detailed instructions about how to restore DB2 (native and SAP® on DB2), Oracle (native), SAP with Oracle databases, and custom applications (using FlashCopy Manager for Custom Applications) are provided.

About this task

Tivoli Storage FlashCopy Manager provides two basic restore methods:

- Restoring data from a snapshot on the storage subsystem.
- Restoring data from Tivoli Storage Manager.

Restoring DB2 databases

To restore a DB2 database, open a command-line window.

The following table summarizes the command entries according to the database configuration and type of restore:

Table 11. Summary of Restore Commands for DB2

Database configuration	Snapshot restore	Restore from Tivoli Storage Manager
DB2	db2 restore ... use snapshot ...	db2 restore ... or db2 recover ...
DB2 in an SAP environment	db2 restore ... use snapshot ...	db2 restore ... or db2 recover ... or backom

Depending on the options that are specified in the **db2 backup ... use snapshot ...** command when the snapshot is created, both backup types (snapshot and Tivoli Storage Manager) can be restored. A snapshot backup type might not be eligible for restore, even though the snapshot backup request completed successfully, because the background copy is not yet complete. When you restore from snapshots, all objects that are created in the backup snapshot process are restored.

The default behavior when you restore data from a snapshot image is a full database offline restore of all paths that make up the database. This restore includes all containers, the local volume directory, and the database path but does not include the database log files. To restore a snapshot, type the following command:

```
db2 restore db DBNAME use snapshot taken at TIMESTAMP
```

Where *TIMESTAMP* is a string that represents the time stamp of the backup image and is optional if there is only one backup image in the source specified. The log files are excluded by default from the restore unless you specify the *logtarget include* option. To restore log files, table spaces, and directories, type the following command:

```
db2 restore db DBNAME use snapshot taken at TIMESTAMP logtarget include
```

To restore a Tivoli Storage FlashCopy Manager snapshot backup in a DB2 pureScale environment, use the same commands as defined in table summary of restore commands for DB2. Issue the command from any of the pureScale member nodes.

In a more complex environment, use the following commands to restore a DB2 multi-partition snapshot:

```
(catalog node first)
db2_all "<+0< db2 restore db H80 use snapshot without prompting"
(remaining nodes)
db2_all "<-0< db2 restore db H80 use snapshot without prompting"
```

For DB2 in an SAP environment only, if the **PARTITION_GROUP** parameter was specified when the snapshot was created, you cannot use the **db2 restore** command to restore the snapshot. For this scenario, use the Tivoli Storage FlashCopy Manager **fcmlcli** command with the following syntax:

```
fcmlcli -f restore -d <dbname> -B <backupID> -P <partition group name>
```

If more than one partition group is used during the backup, the restore operation must be completed for all partition groups.

Restoring DB2 HADR and DB2 standby server environments

Use the `fcmlcli -f restore_db2standby` command to restore a Tivoli Storage FlashCopy Manager snapshot backup of a DB2 HADR standby server. Before, you restore ensure that you stop the DB2 HADR function and deactivate the DB2 database. Tivoli Storage FlashCopy Manager stops the DB2 manager before the restore operation. If the DB2 HADR is still running or the database is still active, Tivoli Storage FlashCopy Manager cannot stop the DB2 manager and the restore is not successful.

A restore operation of an offloaded tape backup from Tivoli Storage Manager can be performed by running Tivoli Storage Manager backup-archive client commands on the DB2 HADR standby server. A proxy node setup can be used.

Tivoli Storage FlashCopy Manager maintains a backup ID that can uniquely identify any snapshot backup. Backup-archive client backups are not associated with backup IDs. Therefore, there is no correlation between a snapshot backup and its corresponding Tivoli Storage Manager backup, other than the time when either backup was created. In configurations where the offloaded Tivoli Storage Manager backup is scheduled at a different time from the snapshot backup, this correlation can be difficult to achieve. If you want to maintain that relationship explicitly in the offload section of the Tivoli Storage FlashCopy Manager profile configuration file, set the **MODE** parameter to ARCHIVE. This way, Tivoli Storage FlashCopy Manager can correlate both backup methods by using the snapshot backup ID as the archive description for the offloaded backup.

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 Oracle databases

Specific command entries are used when restoring Oracle databases.

The following table summarizes the command entries according to the type of restore:

Table 12. 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.

This section describes how to restore your Oracle database using the snapshot restore feature.

Restoring snapshots for Oracle databases

This scenario demonstrates how to restore a snapshot of the Oracle database myDB. The **FLASHCOPY_TYPE COPY** is specified in the Tivoli Storage FlashCopy Manager profile file. In addition, no new file systems or logical volumes were created on the LUNs that myDB is on since the database was originally backed up.

Before you begin

The following conditions are assumed:

- The redo logs for myDB database is in a volume group that is not shared with any Oracle data files.
- The Oracle control files are created in volume groups that are not shared by Oracle data files.
- The Oracle data files are created on LUNs that are on the storage system.

Procedure

1. Ensure that the database to be restored is stopped. Log on to the production server and use the Oracle instance owner user ID.
2. Issue the following command:

```
acsora -f restore
```

This command restores the latest snapshot backup. To restore an older snapshot backup, the backup ID of this backup must be specified.

```
acsora -f restore -b backup ID
```

Where the *backup ID* is ID of the snapshot backup that you want to restore.

The following command can be used to query for existing backup IDs: `acsora -f inquire` (or `acsutil`).

3. After snapshot restore processing completes, you must recover the database.
 - If the **DATABASE_CONTROL_FILE_RESTORE YES** is specified in the Tivoli Storage FlashCopy Manager profile file, you must perform an incomplete recovery.
 - If the **DATABASE_CONTROL_FILE_RESTORE NO** is specified in the Tivoli Storage FlashCopy Manager profile file, you must perform a complete recovery.

Results

After snapshot restore processing completes, you are now able to start the recovery of the restored database myDB database and when complete open the database. If your snapshot restore was not successful and you receive an error message, see the log file for assistance.

Restoring Oracle databases from Tivoli Storage Manager

Tivoli Storage Manager 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.

Restoring the entire database

Perform these tasks to restore Tivoli Storage Manager backups as an entire database.

Procedure

To restore an entire database backup, complete the following steps:

1. If the database is running, enter the following command to stop the database:
`shutdown;`
2. Enter the following command to mount the database:
`startup mount;`
3. Enter the following command to start RMAN and connect to the target database and the recovery catalog:
`rman target username/password rcvcat username/password@connect_string`
4. Issue the RMAN **run** command by specifying the allocation of channels and the restoration of the database. The following example is from an AIX installation:

```
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;
}
```

The previous example also applies to Linux, Solaris, and HP-UX, except that the path to the `tdpo.opt` file differs. On Linux, Solaris and HP-UX, the path is likely to start with `/opt/tivoli`.

5. Recover the database by entering the following command to connect to the target database:
`recover database;`

What to do next

If your restore is not successful and you receive an error message, see the default `tdpoerror.log` error log file for assistance.

Restoring files

To restore Tivoli Storage FlashCopy Manager backups by restoring specific files, complete the following steps.

Procedure

1. If the database is running, enter the following command to stop the database:
`shutdown;`
2. Enter the following command to mount the database:
`startup mount;`
3. Enter the following command to start RMAN and connect to the target database and the recovery catalog. Enter the command on one line.
`rman target username/password rcvcat username
/password@connect_string`

The RMAN command in the preceding example is divided to accommodate page formatting. The actual RMAN command string is on one line.

4. Issue a RMAN **run** command by specifying the allocation of channels and the restoration of the data file *n*, where *n* is the number of the data file. The following example is from an AIX installation:

```
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;
}
```

This example can also apply to Linux, Solaris and HP-UX platforms, except that the path to the `tdpo.opt` file differs. On Linux, Solaris and HP-UX platforms, the path is likely to start with `/opt/tivoli`.

5. Enter the following SQL command to bring the data file online. The *n* variable is the number of the data file.
`alter database datafile n online;`
6. Recover the data file by connecting to the target database and entering the following command:
`recover datafile n;`

What to do next

If your restore is not successful and you receive an error message, see the error log file for assistance.

Restoring Oracle in an SAP environment databases

Specific command entries are used when you restore an Oracle in an SAP environment database.

The SAP BR*Tools BRRECOVER for Oracle databases is used as a database administration tool to help recover your database. BRRECOVER can be used from these interfaces:

- BRRECOVER command-line interface
- BRTOOLS with character-based menus or GUI

BRRECOVER can be used for these tasks:

- Complete database recovery
- Database point-in-time (PIT) recovery
- Tablespace PIT recovery
- Whole database reset
- Restore of individual backup files
- Restore and application of offline redo log files
- Disaster recovery

See the SAP BR*Tools documentation for information about restore and recovery strategies.

The following table summarizes the command entries according to the type of restore:

Table 13. Summary of Restore Commands for Oracle in an SAP environment

Snapshot Restore	Restore from Tivoli Storage Manager
brrestore -d util_vol	brrestore -d util_file
brrecover	brrecover

Restoring file systems or custom applications

You can use the `fccli -f restore` command to restore a file system or custom application that you backed up.

The following examples illustrate the processes that are involved in restoring file systems and custom applications.

Before you begin a restore operation, query Tivoli Storage FlashCopy Manager for all of the snapshot backups that are taken, use the `fccli -f inquire` command. To restore a file system or custom application, complete the following steps:

1. Specify what data you want to query. Use one of the following methods:
 - Specify `#NULL` to query Tivoli Storage FlashCopy Manager for a list of all backups.
 - Specify a backup ID to query the details of a particular snapshot backup.
 - Use the `fccli -f inquire_detail` function to query extra information about the backup. For example, the type of snapshot or the background copy progress.
2. After you run the query, use the `fccli -f restore` command to perform a full or partial snapshot restore of the data that was backed up.

- To perform a full snapshot restore, provide Tivoli Storage FlashCopy Manager with a backup ID from the query that you ran. If you want to restore the latest backup, you can specify #NULL.
- To restore only a portion of the data, specify a list of files explicitly by using the `-I <infile>` option, where the *infile* file contains a list of files or directories that you want to restore. Although Tivoli Storage FlashCopy Manager performs restores at a volume level, extra data might be restored as part of the volume restore operation. You can use the **NEGATIVE_LIST** parameter to specify what actions Tivoli Storage FlashCopy Manager takes in these situations.

You can use the backup-archive client to query and restore data from the Tivoli Storage Manager server. Although Tivoli Storage FlashCopy Manager assists in creating a Tivoli Storage Manager backup from a snapshot, Tivoli Storage FlashCopy Manager cannot be used for the restore operation. You can use the following options to facilitate the restore:

MODE FULL or MODE DIFF

You can correlate a Tivoli Storage Manager backup with the corresponding FlashCopy backup. Compare the Tivoli Storage FlashCopy Manager backup ID with the name of the file list that is backed up as part of the Tivoli Storage Manager backup.

MODE ARCHIVE

You can correlate a Tivoli Storage Manager backup with the corresponding FlashCopy backup. Compare the Tivoli Storage FlashCopy Manager backup ID with the name of the archive description of the Tivoli Storage Manager backup.

Restoring data with remote mirroring

Tivoli Storage FlashCopy Manager software can be used to complete a remote FlashCopy restore of database or custom application data.

About this task

The instructions that are provided assume the following environment:

- Data is successfully backed up and the backup copy of data is accessible.
- A take over host is running with the same operating system level as the production host. In addition, the take over host is configured on the remote side.
- (Databases only) The database instance is created on the take over host.
- Tivoli Storage FlashCopy Manager software is installed on the take over host. The software level on the production host and take over host match.

The instructions for restoring data with remote mirroring slightly vary, depending on the database or custom application. Use the instructions that match your environment.

Restore DB2 database data

The Tivoli Storage FlashCopy Manager snapshot local repository is restored to the take over host at a point in time after the remote backup. The database is restored to the take over host by using the Tivoli Storage FlashCopy Manager snapshot local repository after the remote backup. The database instance is created on the take over host. Complete the following steps:

1. Start the DB2 database manager with the following command: **db2start**

2. Update the Tivoli Storage FlashCopy Manager configuration parameters with the setup script wizard. Specifically, in the GLOBAL section, set the **ACSD** parameter to use the acsd on the take over host. Do not use the acsd of the production host.
3. Stop the Tivoli Storage FlashCopy Manager acsd daemon on the primary production host. Transfer all the repository files from the primary production host to the take over host. The repository files are in the directory that is defined by the parameter **ACS_REPOSITORY** in the ACSD section of the profile.
4. Start the Tivoli Storage FlashCopy Manager acsd daemon on the take over host.
5. From the backups that are displayed, select the remote backup to use for the restore. The backups are displayed when you enter the query command on the take over host. For example: **db2acsutil query show details**
6. Start the restore by entering the following command:
`db2 restore db <db_name> use snapshot taken at <backup_timestamp>`

Restore Oracle database data

The Tivoli Storage FlashCopy Manager snapshot local repository is restored to the take over host at a point in time after the remote backup. The database is restored to the take over host by using the Tivoli Storage FlashCopy Manager snapshot local repository after the remote backup. Complete the following steps:

1. Update the Tivoli Storage FlashCopy Manager configuration parameters with the setup script wizard. Specifically, in the GLOBAL section, set the **ACSD** parameter to use the host name on the take over host. Do not use the acsd of the production host.
2. Stop the Tivoli Storage FlashCopy Manager acsd daemon on the primary production host. Transfer all the repository files from the primary production host to the take over host. The repository files are in the directory that is defined by the parameter **ACS_REPOSITORY** in the ACSD section of the profile.
3. Start the Tivoli Storage FlashCopy Manager acsd daemon on the take over host.
4. From the backups that are displayed, select the remote backup to use for the restore. The backups are displayed after you enter the query command on the take over host. For example: **acsora -f inquire_detail**
5. Start the restore by entering the following command:
`acsora -f restore -b <backup_id>`

Restore Oracle in an SAP environment database data

The Tivoli Storage FlashCopy Manager snapshot local repository and the SAP backup directory, `/oracle/<SID>/sapbackup`, is restored to the take over host at a point in time after the remote backup. When you are restoring data in a maintenance scenario, not a disaster recovery scenario, the Tivoli Storage FlashCopy Manager repository and the SAP backup repository can be shared by NFS. Complete the following steps:

1. Update the Tivoli Storage FlashCopy Manager configuration parameters with the setup script wizard. Specifically, in the GLOBAL section, set the **ACSD** parameter to use the acsd on the take over host. Do not use the acsd of the production host.

2. In the `init<SID>.utl` file, set the **ACSD** parameter to use the acsd on the take over host. Do not use the acsd of the production host.
3. Stop the Tivoli Storage FlashCopy Manager acsd daemon on the primary production host. Transfer all the repository files from the primary production host to the take over host. The repository files are in the directory that is defined by the parameter **ACS_REPOSITORY** in the ACSD section of the profile.
4. Start the Tivoli Storage FlashCopy Manager acsd daemon on the take over host.
5. From the backups that are displayed, select the remote backup to use for the restore. The backups are displayed when you enter the query command on the take over host. For example: **fcmccli -f inquire_detail**
6. Start the restore by entering the following command:

```
BR_NSC=1 brrestore -m full -p <dir>/init<SID>.sap -b <sap backup log id>
-d util_vol -r <dir>/init<SID>.utl
```

Restore custom application agent data

The Tivoli Storage FlashCopy Manager snapshot local repository is restored to the take over host at a point in time after the remote backup. When you are recovering data for maintenance, not disaster recovery, the Tivoli Storage FlashCopy Manager repository can be shared by NFS. Complete the following steps:

1. Update the Tivoli Storage FlashCopy Manager configuration parameters with the setup script wizard. Specifically, in the GLOBAL section, set the **ACSD** parameter to use the host name on the take over host. Do not use the acsd of the production host.
2. Stop the Tivoli Storage FlashCopy Manager acsd daemon on the primary production host. Transfer all the repository files from the primary production host to the take over host. The repository files are in the directory that is defined by the parameter **ACS_REPOSITORY** in the ACSD section of the profile.
3. Start the Tivoli Storage FlashCopy Manager acsd daemon on the take over host.
4. From the backups that are displayed, select the remote backup to use for the restore. The backups are displayed when you enter the query command on the take over host. For example: **fcmccli -f inquire_detail**
5. Start the restore by entering the following command:

```
fcmccli -f restore -b <backup_id>
```

Results

The remote mirroring relationships are stopped. The volume groups with the file systems that contain the table spaces are restored from the FlashCopy targets to the remote mirroring targets. The file systems that contain the table spaces are mounted.

For IBM System Storage SAN Volume Controller all versions, starting with 6.2, the remote relationships are stopped. You must restart the remote relationships before another snapshot of targets of remote mirroring can be run. For IBM XIV Storage System and IBM System Storage SAN Volume Controller before version 6.2, the remote relationships are removed. You must re-create the remote relationships before another snapshot of targets of remote mirroring can be run.

Chapter 7. Cloning databases

Tivoli Storage FlashCopy Manager uses the FlashCopy or snapshot function of the storage solutions for database cloning. This method eliminates downtime and minimizes the impact on the production database.

For FlashCopy backup, the physical volume identification numbers (PVIDs) are not changed. For FlashCopy cloning, the PVIDs of the FlashCopy target disks are automatically changed by the Tivoli Storage FlashCopy Manager software. You can have several cloned databases of one source database running on one host.

With Tivoli Storage FlashCopy Manager, a cloning process can be started with an online or offline source database (DB2 or Oracle). For online Tivoli Storage FlashCopy Manager cloning, the source database is suspended for a short time. The suspension occurs when the storage system creates its FlashCopy or snapshot of the source database.

The cloned database (target database) can have the same database name as the source database. The cloned database can also be renamed to any valid database name during the Tivoli Storage FlashCopy Manager cloning process. Tivoli Storage FlashCopy Manager requires the cloned database to be created on a different database server than the source database server regardless of whether the clone database name is changed.

When you clone databases and use IBM System Storage SAN Volume Controller, the space-efficient disks can be used as a target for FlashCopy cloning operations. However, when you use SAN Volume Controller space-efficient disks as a target for FlashCopy cloning, there are restrictions on the FlashCopy backups. You can complete cloning operations from the cloning source volumes. If you want to complete FlashCopy backup and FlashCopy cloning from the same source disks, use full target disks.

To use SAN Volume Controller space-efficient disks, in the **DEVICE_CLASS** that is used for cloning operations, set the **ALLOW_NOCOPY_FLASHCOPY** parameter to YES.

Tivoli Storage FlashCopy Manager cloning process

Information about the Tivoli Storage FlashCopy Manager cloning process is provided.

The Tivoli Storage FlashCopy Manager cloning process is initiated by either of the following commands, with the appropriate command-line options:

- `fccli -f create_clone`
- `fccli -f refresh_clone`

The following processing occurs:

1. The selected preprocessing scripts are run, including stopping the clone database. This step only occurs when using the `refresh_clone` command with the `-X pre-processing_configuration_file` option.
2. The FlashCopy clone is unmounted on the clone system. This step occurs only when using `refresh_clone` function.

3. A new FlashCopy clone is created, including the suspension and resumption of the source database, and mounted on the clone system.
4. The cloned database is recovered.
5. The cloned database is renamed to the target database name.
6. Tivoli Storage FlashCopy Manager starts the cloned database.
7. The selected postprocessing scripts are run to clean up the clone database. This step occurs only when the *-Y post-processing_configuration_file* option is used.

Cloning an Oracle Data Guard standby database

Tivoli Storage FlashCopy Manager can clone an Oracle Data Guard standby database.

To clone an Oracle Data Guard standby database, on the Oracle Data Guard standby server complete the following steps:

- Shut down the Oracle Data Guard standby instance.
- Log on to the Oracle Data Guard standby server and use the Oracle instance user ID.
- To create a clone, enter the following command:

```
./fcmcli -f create_clone -C CLONE_ORACLE_SID -u CLONE_ORACLE_USER
```

This clone is a stand-alone Oracle database that can be opened in read and write mode. You can use the cloning command optional function *-X preprocessing-configuration-filename* and *-Y postprocessing-configuration-filename* to run preprocessing and postprocessing scripts on the cloned target system. You can use shell or sql scripts.

Tip: If the Tivoli Storage FlashCopy Manager profile parameter **OVERWRITE_DATABASE_PARAMETER_FILE** is set to YES, the `initDBSID.ora` file is copied from the Oracle Data Guard standby server to the clone target system. This file contains Data Guard configuration information that is not required by the clone instance and can cause problems. Therefore, create a customized `initDBSID.ora` file for the Oracle clone instance and set the Tivoli Storage FlashCopy Manager **OVERWRITE_DATABASE_PARAMETER_FILE** profile parameter to NO. You can copy the `initDBSID.ora` file and remove any specific Data Guard configuration information.

Typically Oracle temporary tablespace files are not present in the Data Guard standby server. If the temporary tablespace files are on the same file systems as the Oracle data files, no additional configuration is required by Tivoli Storage FlashCopy Manager. If the temporary tablespace files are on a dedicated file system or volume group, use the **FLASH_DIR_LIST** parameter in the cloning section of Tivoli Storage FlashCopy Manager profile to include these files. Use the **FLASH_DIR_LIST** parameter to specify a fully qualified directory name and file name. This file contains the mount points where the Oracle temporary files are located. Use a separate line for each mount point. Then, Tivoli Storage FlashCopy Manager includes the mount points and the corresponding volume groups in the FlashCopy cloning operation.

Database cloning preprocessing and postprocessing

Repetitive processing steps that occur before and after database cloning can be automated by scripts.

The required functions in the automated scripts depend largely on the cloning environment. Because all possible environments cannot be covered by one package, preprocessing and postprocessing must be considered outside the scope of Tivoli Storage FlashCopy Manager cloning.

Tivoli Storage FlashCopy Manager provides a framework in which you can run shell scripts and DB2 or Oracle SQL scripts on the clone system. Run the shell scripts before a clone database is unmounted and after a new clone database is created. With this capability, you gain the ability and flexibility to fully automate the cloning process.

Configuration files used for cloning

Information is provided about configuration files for use with FlashCopy cloning.

Tivoli Storage FlashCopy Manager uses preprocessing and postprocessing configuration files during cloning operations (for example `/oracle/P01/acs/preprocessing.ini`). The functions that are provided by the processing scripts depend on the cloning environment where they are issued. All processing configuration files and the scripts that are defined in the configuration files must meet the following requirements:

- Files and scripts are stored on the clone system.
- Files and scripts have permissions for read and write access for the clone database instance owner. The preprocessing and postprocessing scripts have permissions for read and write access for the user who updates and runs the scripts. If the scripts are run by any user registered on the system, the scripts are owned by the root user. The root user has permission to read and write for the User, Group, and World user groups.
- Files and scripts have permission for read access for the production database instance owner.

Attention: If a write access level for the World user group is given, there is a security risk.

When adding processing configuration files, place each script on a separate line as shown in the following example:

```
/oracle/P01/acs/scripts/PreProcessing_stopsap.sh
/oracle/P01/acs/scripts/PreProcessing_stopdb.sh
```

Both processing configuration files support embedded user comments. A comment line in the configuration file is denoted by the number sign character: `#`. The scripts are specified with fully qualified file names. Each line of the processing configuration file represents one processing script. The Tivoli Storage FlashCopy Manager Offload Agent, `tsm4acs`, uses these arguments and their values when calling the scripts:

DBNAME_PROD

The database name on the production system.

DBNAME_CLONE

The database name on the cloning system.

DBHOST_PROD

The host name of the production system.

DBHOST_CLONE

The host name of the cloning system.

CLONE_TIMESTAMP

The timestamp when the clone was created. This entry is also the time when the production database is suspended and the FlashCopy operation begins. The timestamp format is YYYYMMDDhhmmss. During preprocessing, the timestamp identifies when the previous FlashCopy clone is created. During postprocessing, the timestamp identifies when the current FlashCopy clone was created.

SCHEMA

The database schema of the production database as specified by the profile parameter **DATABASE_SCHEMA**. Depending on SAP® Kernel release, this schema is SAPR3 or SAPDBname.

You can use the following processing scripts:

- SQL scripts (DB2 in an SAP environment or Oracle in an SAP environment) with the extension .sql.
- Shell scripts with the extension .sh. Shell scripts can be started by a database user who is different from the clone database user. For example, when installing the SAP license for the cloned SAP system, start the postprocessing shell script as the SAP administration user *sidadm*:

```
scripts/PostProcessing_saplicense.sh:c01adm
```

By adding `:c01adm` to the script file name, the script runs as user `c01adm` instead of user `orac01` or `db2c01`. This addition requires that the owner of the script to be identical to the user who is intended operator of the script. In this example, `c01adm` is the owner of the script. There is one exception. If a preprocessing or postprocessing script is owned by the root user, the script can be run by any user registered on the system.

The processing scripts that are defined in the processing configuration files run sequentially. The return code of each script is validated. The following values are used:

- RC=0** Processing ends successfully. If this script is the last script to be run, continue cloning. If this script is not the last script, continue with the next script.
- RC=1** Processing ends successfully with warning. If this script is the last script to be run, continue cloning. If this script is not the last script, continue with the next script.
- RC=2** Processing ends with an error. Cloning immediately stops. No additional scripts run.

The return code for each script is written to the cloning log files. The output is written to dedicated log files with the following file names:

```
clone_preproc.<timestamp>
clone_postproc.<timestamp>
```

Processing example: Cloning configuration files

In the following processing example, the production database is named P01, and the clone database is named C01:

```
./fcmcli -f preproc_clone -u db2c01 -C C01 -X /oracle/C01/acs/preprocessing.ini
./fcmcli -f postproc_clone -u db2c01 -C C01 -Y /oracle/C01/acs/postprocessing.ini
```

If a processing script needs additional command-line options, add these options to each line of the configuration file. In this example, the additional command-line argument LC01 is added to the script entry in the configuration file:

```
/oracle/C01/acs/scripts/PostProcessing_startListener.sh LC01
```

The Tivoli Storage FlashCopy Manager command-line interface issues a call to the processing script with the six default arguments. After these arguments are provided, additional command-line options are sent. In this example, the additional command-line argument LC01 is passed to the PostProcessing_startListener.sh script as the seventh argument:

```
#!/bin/ksh
# FOLLOWING ACTIONS ARE PERFORMED -----
# start the Oracle Listener

DBNAME_PROD=$1
DBNAME_CLONE=$2
DBHOST_PROD=$3
DBHOST_CLONE=$4
CLONE_TIMESTAMP=$5

# ${SCHEMA} is schema owner (for SAP Kernel > 6.10, for userid other than SAPR3)
SCHEMA=$6
SCHEMA=$(echo ${SCHEMA} | tr [a-z] [A-Z])

# ${LISTENER} is the name of the listener to be started (taken from listener.ora)
LISTENER=$7

lsnrctl start ${LISTENER}
```

If a DB2 SQL script needs additional command-line options, use a shell script as a wrapper with the DB2 SQL commands. Tivoli Storage FlashCopy Manager requires that the DB2 SQL script use a semicolon delimiter: ;. If another delimiter character is specified, use another shell script wrapper that calls the DB2 SQL script with the correct delimiter character in the command-line entry. This example shows a shell script wrapper that specifies the correct delimiter character:

```
#!/bin/ksh
DELIMITER=#
db2 -td${DELIMITER} -svf PostProcessing_script1.sql
```

Chapter 8. Troubleshooting

There are multiple resources for support.

The following list identifies the various ways that you can find information online:

- Tivoli Storage FlashCopy Manager wiki on the developerWorks® site at [https://www.ibm.com/developerworks/community/wikis/home?lang=en#/wiki/Tivoli Storage FlashCopy Manager](https://www.ibm.com/developerworks/community/wikis/home?lang=en#/wiki/Tivoli%20Storage%20FlashCopy%20Manager).
- Service Management Connect site at <https://www.ibm.com/developerworks/servicemanagement/sm/index.html>.
- Tivoli Storage FlashCopy Manager product support at <http://www.ibm.com/software/tivoli/products/storage-flashcopy-mgr/>. Enter the search term, such as an authorized program analysis report (APAR) number, release level, or operating system to narrow the search criteria for your support need.

General troubleshooting procedure

This procedure is valid for all Tivoli Storage FlashCopy Manager applications.

The starting point for problem determination is the summary log file located in the <ACS_DIR>/logs directory. The summary log file name is summary.<timestamp>.log where <timestamp> is an entry that represents the four-digit year, month, and day (for example, summary.20090817.log). A new log file is created each day. This file contains a list of all operations and the most important messages. Each line begins with one of these prefixes to indicate the type of operation:

Table 14. Message prefixes used in the summary log file

Prefix	Operation
GEN	Generic message
DB	Database backup or restore; inquire or delete of FlashCopy backups
MON	Monitoring of the background copy that is performed by the storage device
TSM	Off-loaded backup to Tivoli Storage Manager
MNT	Mount and unmount services
CLO	FlashCopy cloning operations

The summary log file only contains the information about operations that were performed and whether they completed successfully. Error messages are also logged when they occur. A dedicated log file is created for each operation in the <ACS_DIR>/logs/details. These files should be checked for detailed information when an error occurs.

This summary log file example shows a FlashCopy backup of a database. Messages with the DB prefix are issued by the database client. This is the application that requests the backup operation.

GEN 00:10:00 (70a)

=====

New backup operation started for database instance db2h51, database H51.

```

=====
DB 00:10:00 (70a) FMM1510I New connection received.
DB 00:10:00 (70a) FMM1513I ***** Database client connected: db2s95, database S95,
partition NODE0000
DB 00:10:00 (70a) FMM1574I Backup for db2s95.S95.DEVICE_CLASS:STANDARD.NODE0000 is
created using DEVICE_CLASS
DEVICE_CLASS:STANDARD.
DB 00:10:01 (80c) FMM1510I New connection received.
DB 00:10:01 (80c) FMM1514I ***** Device client connected.
DB 00:10:01 (80c) FMM6219I Backup to TSM: NO
DB 00:10:01 (80c) FMM1582I The target set 1 will be used for the current backup.
DB 00:10:44 (70a) FMM1014I Operation backup completed successful.
GEN 00:12:28 (70e)
=====

```

Logging and tracing files

Log and trace files are updated during Tivoli Storage FlashCopy Manager operations.

Log and trace files are written to during backup and restore processing by these products:

- DB2
- Oracle
- Tivoli Storage FlashCopy Manager
- Storage system
- CIM
- IBM General Parallel File System (GPFS) for DB2 pureScale.
- Tivoli Storage Manager for ERP
- Operating system

The following figure illustrates a sample sequence for examining log and trace files when troubleshooting SAP with Oracle Tivoli Storage FlashCopy Manager.

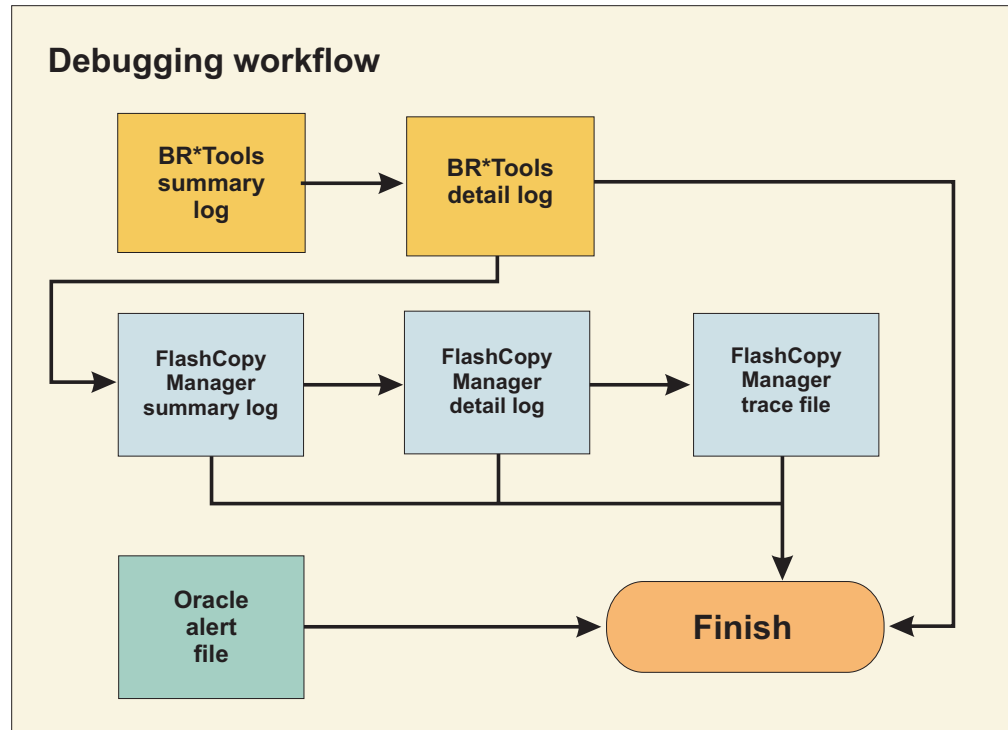


Figure 15. Debugging workflow for SAP with Oracle Tivoli Storage FlashCopy Manager

The following figure illustrates a sample sequence for examining log and trace files when troubleshooting SAP with Oracle Tivoli Storage FlashCopy Manager with Tivoli Storage Manager.

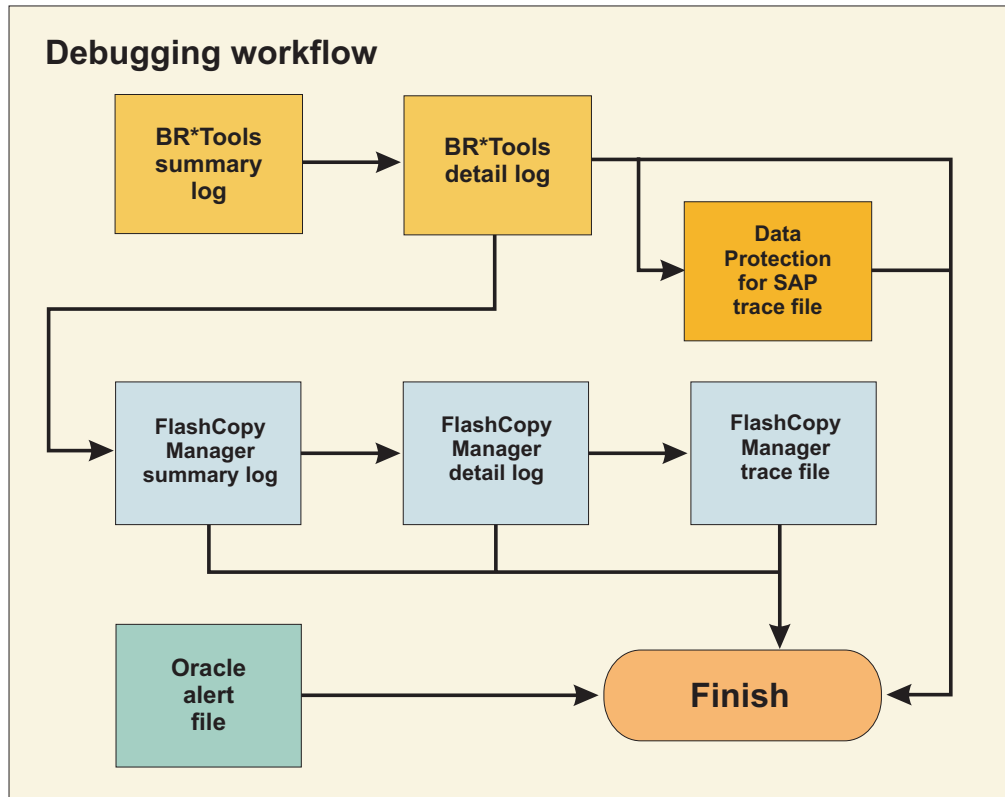


Figure 16. Debugging workflow for SAP with Oracle Tivoli Storage FlashCopy Manager with Tivoli Storage Manager

Tivoli Storage FlashCopy Manager log and trace files

Refer to these examples of the log and trace files maintained by Tivoli Storage FlashCopy Manager.

Tivoli Storage FlashCopy Manager 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 requested by IBM Support. If TRACE is set to YES, each Tivoli Storage FlashCopy Manager component creates an additional trace file in the log directory.

The following tables list the log and trace files maintained by Tivoli Storage FlashCopy Manager. These files reside in `ACS_DIR/logs`.

Table 15. Tivoli Storage FlashCopy Manager log files

Purpose	File
Overview about performed operations and their result.	<code>summary.timestamp.log</code>
Overview about the monitoring of the background copy that is performed by the storage device.	<code>monitor.timestamp.log</code>
Detailed log of a particular operation.	<code>details/function.longtimestamp</code>

Table 15. Tivoli Storage FlashCopy Manager log files (continued)

Purpose	File
Note: <ul style="list-style-type: none"> <i>timestamp</i> is the date (yyyymmdd) <i>longtimestamp</i> is the date and time (yyyymmddHHMMSS) <i>function</i> is a value of backup, restore, inquire, delete, mount, unmount, tsm, or clone <p>The summary log file is always used as an entry point. All major events, such as the start of a new operation or errors, are recorded in this file. A new summary log file is created for every day and records all operations of one day within a single file.</p>	

Table 16. Tivoli Storage FlashCopy Manager trace files

Component	File
Management Agent (acsd)	acsd.id.trace
Application client (for DB2, the Snapshot Backup Library)	client.instance.db name.node.id.trace
Generic Device Agent (acsgen)	acsgen.hostname.device class.node num.id.trace acsgen.hostname.function.id.trace acsgend.hostname.id.trace
Device Agent for IBM XIV® Storage System Devices	xivadapter_id_function.trace
Device Agent for IBM System Storage N series and NetApp storage solutions	fmna.hostname.function.id.trace fmna.hostname.device class.node num.id.trace
Device Agent for CIM Devices (DS8000, SAN Volume Controller, Storwize family)	fmcima.hostname.function.id.trace fmcima.hostname.device class.node num.id.trace
Offload Agent (tsm4acs)	tsm4acs. host.id.trace
fcmcli	fcmcli.host.id.trace
RMAN (when invoked by Tivoli Storage FlashCopy Manager)	rman.SID.id.log
Notes: <ul style="list-style-type: none"> Names ending in -d are daemon processes (started with -D option). <i>id</i> 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. <i>device class</i> 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. <i>instance</i> and <i>db hostname</i> can be <i>undef</i> for query and delete requests started with db2acsutil. <i>node num</i> 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. <i>function</i> is backup, delete, restore, mount, unmount, or reconcile. 	

Table 17. Tivoli Storage FlashCopy Manager return codes

Reason code	Explanation	User response
0	Operation is successful	None

Table 17. Tivoli Storage FlashCopy Manager return codes (continued)

Reason code	Explanation	User response
1	Operation terminated successfully with warnings	The Tivoli Storage FlashCopy Manager operation was successful but warning messages were reported. Check the Tivoli Storage FlashCopy Manager summary log file and the therein referenced detail log files for more information.
2	Operation terminated with error	The Tivoli Storage FlashCopy Manager operation failed. Check the Tivoli Storage FlashCopy Manager summary log file and the therein referenced detail log files for more information.

Table 18. Tivoli Storage FlashCopy Manager installer exit codes

Exit Code	Explanation	User Response
0	The operation completed successfully	The installation completed successfully without any warnings or errors.
1	The operation completed successfully with warnings.	The installation completed successfully, but one or more of the actions from the installation sequence caused a warning or a non-fatal error. See the Tivoli Storage FlashCopy Manager installer log file installation.log in the installation directory for details.
-1	The operation terminated with error	One or more of the actions from the installation sequence caused a unrecoverable error. See the Tivoli Storage FlashCopy Manager installer log file installation.log in the installation directory for details.
>=1000	The operation terminated with error Note: There more error codes with numbers greater than or equal to 1000 which all mean that some kind of error occurred.	One or more of the actions from the installation sequence caused a unrecoverable error. See the Tivoli Storage FlashCopy Manager installer log file installation.log in the installation directory for details.

Table 19. DB2 vendor reason codes

Reason Code	Explanation	User Response
0	The operation is successful.	None
2	Communication error with device	TheTivoli Storage FlashCopy Manager operation failed. Check the db2diag.log and the Tivoli Storage FlashCopy Manager summary log file for details.

Table 19. DB2 vendor reason codes (continued)

Reason Code	Explanation	User Response
3	The DB2 and vendor products are incompatible	The Tivoli Storage FlashCopy Manager operation failed during initialization of the Tivoli Storage FlashCopy Manager vendor library. The DB2 API version does not match the Tivoli Storage FlashCopy Manager vendor library version. Check the db2diag.log for details.
6	Object specified cannot be found	The Tivoli Storage FlashCopy Manager operation failed because the requested object cannot be found in the Tivoli Storage FlashCopy Manager repository. Check the db2diag.log and the Tivoli Storage FlashCopy Manager summary log file for details.
8	Invalid user ID specified	The Tivoli Storage FlashCopy Manager operation failed because an invalid user ID was specified on the db2 command line. Check the db2diag.log.
9	Invalid password provided	The Tivoli Storage FlashCopy Manager operation failed because an invalid password was specified on the db2 command line. Check the db2diag.log.
10	Invalid options specified	The Tivoli Storage FlashCopy Manager operation failed because an invalid db2 command-line option was specified. Check the db2diag.log.
11	Initialization failed	The Tivoli Storage FlashCopy Manager operation failed because the Tivoli Storage FlashCopy Manager vendor library cannot be initialized. Check the db2diag.log and the Tivoli Storage FlashCopy Manager summary log file for details.
14	End of data reached	Not an error condition.
18	Device error	The Tivoli Storage FlashCopy Manager operation failed. Check the Tivoli Storage FlashCopy Manager summary log file for details.
19	Warning	The Tivoli Storage FlashCopy Manager operation is successful with warning messages. Check the Tivoli Storage FlashCopy Manager summary log file for details.
21	More data to come	Not an error condition.
26	Delete object fails	The Tivoli Storage FlashCopy Manager delete operation failed. Check the Tivoli Storage FlashCopy Manager summary log file for details.

Table 19. DB2 vendor reason codes (continued)

Reason Code	Explanation	User Response
29	Abort request failed	The Tivoli Storage FlashCopy Manager abort request failed. Check the Tivoli Storage FlashCopy Manager summary log file for details.
30	Unexpected Error	The Tivoli Storage FlashCopy Manager operation failed. Check the Tivoli Storage FlashCopy Manager summary log file for details.
31	No data has been returned	Not an error condition.
32	Object not under Backup Adapter control	The Tivoli Storage FlashCopy Manager operation failed because the object specified for a restore or query is not under the control of Tivoli Storage FlashCopy Manager. It might be under control of Tivoli Storage Manager for ERP, for example. Check the db2diag.log and the Tivoli Storage FlashCopy Manager summary log file for details.
34	Another database or application is using the same storage groups	The Tivoli Storage FlashCopy Manager snapshot backup operation failed because another database or application is using the same storage group. Check the db2diag.log and the Tivoli Storage FlashCopy Manager summary log file for details.

Storage system log and trace files

Storage system log and trace files are updated during Tivoli Storage FlashCopy Manager operations.

Consult the documentation for the configured storage system.

CIM log and trace files

CIM log and trace files are updated during Tivoli Storage FlashCopy Manager operations.

For more information about log and trace files for CIM, see the CIM documentation. The DS8000 Open API, SAN Volume Controller, and Storwize family master console produce log and trace output.

GPFS log files

IBM General Parallel File System (GPFS) log files are updated during DB2 pureScale Tivoli Storage FlashCopy Manager operations.

The GPFS log files are in /var/adm/ras directory on each GPFS node and start with the prefix mmfs.log. The most current GPFS log file can be found by using the symbolic link /var/adm/ras/mmfs.log.latest. See the information about GPFS log files and troubleshooting procedures in the *IBM General Parallel File System (GPFS) for Clusters: Problem Determination Guide (GA76-0415-08)*.

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.

Troubleshooting mirroring relationships

There are some questions that might arise when implementing Tivoli Storage FlashCopy Manager and storage systems with mirroring technologies. The following information is provided to help you answer questions unique to your environment.

Question

Why are some remote mirroring relationships missing?

Answer

The target volumes that are referenced in this solution are part of the remote mirror relationship. The target volumes are used as the source for the snapshot operation.

Before you start the snapshot backup that uses the target volumes, verify that the remote mirroring relationships are established. You can verify the relationships by using either the graphical user interface or the command-line interface. For example, if using SAN Volume Controller global mirror, you can enter the following command to verify the mirroring relationship:

```
ssh -i/<dir>/ssh-identity <username>@<hostname>
svctask mkrcrelationship -master <vdiskname local> -aux <vdiskname remote>
-cluster <clusterid> -name <relation name> -consistgrp <consgrp name>
-global
```

Question

The remote mirroring relationships are not in the state consistent_synchronized. How does the state for remote mirroring relationship get updated?

Answer

Go to the storage solution. Synchronize the consistency groups. For more

information about synchronizing consistency groups, see the documentation that is provided with the storage hardware.

Question

(SAN Volume Controller only) One or more of the FlashCopy target volumes for the remote site are missing. Where is the FlashCopy target volume?

Answer

Use either the graphical user interface or command-line interface to start the Metro Mirror or Global Mirror consistency group. For example, you can enter the following command from the command-line interface:

```
ssh -i/<di>ssh-identity <username>@<hostname of the cluster> svctask  
starttrconsistgrp consist group id>
```

Question

(XIV only) One of the following issues exists.

- The remote mirroring is not operational.
- For XIV system synchronous mirroring, the state of the consistency group is not consistent synchronized.
- For XIV system asynchronous mirroring, the state of the consistency group is not RPO_OK.

How are these issues resolved?

Answer

Verify that the consistency groups meet the following requirements:

- Consistency groups need to be enabled and synchronized.
- The volumes that are assigned to the consistency groups need to be correctly identified and enabled.

One consistency group per database partition is needed.

Troubleshooting storage solutions

There are some common problems that might occur when using Tivoli Storage FlashCopy Manager and storage solutions. These problems and the solutions are provided to help you complete problem determination activities.

Question

During the backup or cloning on a storage solution running a supported AIX operating system, the mount of one or more file systems fails on the auxiliary host with the following message:

```
FMM0644E Error on running command: mount: 0506-334  
/oracle/C21/mirrlog2 is not a known file system.
```

How can this error be resolved?

Answer

When the storage solution running a supported AIX operating system imports a volume group, use the label of the logical volume for the new mount point. Check the production system to determine the labels of the logical volumes that support backup and clone operations. The fields **mount point** and **label** should have identical values. For example:

```
# lslv lvDS1data1  
LOGICAL VOLUME: lvDS1data1 VOLUME GROUP: DS1data1vg  
...  
MOUNT POINT: /db2/DS1/db2ds1/NODE0001 LABEL: /db2/DS1/db2ds1/NODE0001
```

Problem

In an environment with an IBM System Storage N series and NetApp storage system and Tivoli Storage FlashCopy Manager, the performance seems to lag. What could be the problem?

Solution

The primary variable that affects the performance of the Tivoli Storage FlashCopy Manager is the number of volumes and LUNs that are backed up with a FlashCopy.

Problem

As an administrator using Tivoli Storage FlashCopy Manager, how do I mount a backup that resides on a SAN-attached IBM System Storage N series or NetApp storage system?

Answer

After the backup is created, run the following commands:

```
fccli -f mount
```

Verify that the snapshot is mounted on the backup system.

Problem

As an administrator using Tivoli Storage FlashCopy Manager, how do I complete an offloaded backup of a database that resides on a SAN-attached IBM System Storage N series or NetApp storage system? This backup copy is used to recover from disasters.

Answer

After the backup is created, run the following commands:

```
fccli -f tape_backup
```

Verify that the snapshot is mounted on the backup system.

Problem

As an administrator using Tivoli Storage FlashCopy Manager, how do I restore disk backups that reside on a SAN-attached IBM System Storage N series or NetApp storage system? The goal is to integrate recovery into established workflows.

Answer

For the configured application, run one of the following commands to restore:

- `db2 restore db <id> use snapshot`
- `acsora -f restore`
- `brrestore`
- `tsm4acs -f restore`

Verify that the data can be used by the respective application.

Troubleshooting connectivity problems

This information covers a problem that can occur with connectivity. The problem and the solution are provided to help you complete problem determination activities.

When the production server and backup server are separated by a firewall, socket connections might time out

Question

After a successful snapshot backup operation, why is it not possible to mount or unmount this snapshot backup on a backup or clone server?

Answer

The socket connection failure can result from a mismatch between the firewalls connection timeout setting and the operating systems frequency of sending keep alive network packets. When a firewall or other network devices such as a router or switch exists between the production and backup server, the daemon connection can time out. A similar situation can exist between a production and clone server. To prevent connections from timing out, the management agent acsd on the production server, requests that the operating system sends out network packets. These packets keep the connection between the servers alive.

The **tcp_keepidle** operating system parameter specifies the interval of inactivity. Depending on the operating system, this parameter might vary. After this interval of inactivity, the TCP generates a keep alive transmission for the application that requests it. This interval is measured in half seconds. For AIX operating systems, the keep alive default value for this parameter is 14400 (2 hours). This frequency is sufficient for many environments. Decrease this value when the following conditions exist:

- A firewall or other network device exists between the production and backup or clone server.
- If the device connection timeout is less than 2 hours.

For AIX operating systems, issue the following network command to reduce the **tcp_keepidle** parameter value and send a keep alive transmission every 5 minutes:

```
no -o tcp_keepidle=600
```

This change remains in effect until you restart the production server. To permanently modify this parameter, add the command to the `/etc/rc.net` file.

Troubleshooting tips for Tivoli Storage FlashCopy Manager for Oracle

Resolving problems encountered when using Tivoli Storage FlashCopy Manager requires tasks specific to the native Oracle database environment.

If an error condition occurs during a Tivoli Storage FlashCopy Manager event, there are several sources of information you can view to help determine what the problem might be. 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 Tivoli Storage FlashCopy Manager 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 server must be in “startup mount” state at the time **acsora** is issued. Otherwise it 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 chl 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 chl;
}
```

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

When the SQL*Plus or Oracle Net configuration files do not reside in their default location, set the **TNS_ADMIN** environment variable.

To run offloaded backups of Oracle databases, a recovery catalog database is needed. The database must be accessible by RMAN from the production host and the backup host. On the production host, use the following command to verify if the connection can be established. Before entering the command, log on as the database instance owner.

```
rman target / catalog catalog_db_user/catalog_user_password@catalog_db_connect_string
```

On the backup host, log on as the root user and enter the following command:

```
su - oracle_instance_owner -c rman target / catalog catalog_db_user/  
catalog_user_password@catalog_db_connect_string
```

If you receive errors that say RMAN is unable to connect to the catalog database, verify the configuration of the `tnsnames.ora` on the host where the command was run. In addition, verify the listener configuration on the host where the catalog database runs. For details about the setup of the catalog database and the listener configuration, see documentation provided by Oracle.

Tivoli Storage FlashCopy Manager for Oracle miscellaneous errors

Certain unique errors might occur when you use Tivoli Storage FlashCopy Manager for native Oracle.

If you receive the following errors:

Tivoli Storage FlashCopy Manager fails on the backup server in DBCS locales when the datafile or the path to the datafile contains a DBCS name.

This error is an Oracle problem that was reported to the Oracle development team. The Oracle Technical Assistance Request (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 Tivoli Storage FlashCopy Manager supports table spaces that are named with DBCS, datafiles or paths to the datafiles that contain DBCS must be renamed to English before running Tivoli Storage FlashCopy Manager.

Internet Protocol Version 6 (IPv6) support

The Tivoli Storage FlashCopy Manager for UNIX and Linux software operates in IPv4, IPv6, and mixed environments.

The network configuration determines which protocol is used by the Tivoli Storage FlashCopy Manager software. The acsd service listens for IPv4 and IPv6 connection requests. Connection requests to the acsd service are made for the addresses that are returned by the system for the respective port on the local host. Connection requests to other systems are made for the addresses that are specified by the user. When TCP/IP addresses are set from a command-line interface, or when you are setting configuration parameters with the setup script, IPv6 addresses are supported. When an IP address and a port are specified in the following format:

<IPv4 address>:<service or port>

the format needs to be changed for IPv environments only:

<service or port>@<IP address>

|

In pure IPv4 environments, the traditional format can be used.

Appendix A. Configuration files

When you complete the setup script, the information you enter is used to configure Tivoli Storage FlashCopy Manager.

Tivoli Storage FlashCopy Manager uses the following configuration files:

- Profile
- Target volumes
- Password
- (Oracle in an SAP environment) Backint for SAP database
- (Oracle in an SAP environment) BR*Tools
- (Native Oracle) Tivoli Storage Manager options

The parameter and option information provided for the Tivoli Storage FlashCopy Manager configuration files is for reference only. Do not edit these configuration files. The configuration files are updated when you use the setup script.

Profile overview

When you complete the setup script, the information you enter is used to create the profile configuration file. Each section of the profile includes parameters and options that determine how the Tivoli Storage FlashCopy Manager backs up and restores data in your environment. For references, the following information explains the various parameters and options.

In the Tivoli Storage FlashCopy Manager executable files, the profile is identified by the value specified for option -p. For DB2 databases, the profile is identified by the PROFILE vendor option. The elements of the profile are not case sensitive. By convention, section and parameter names are indicated with uppercase letters.

The profile is divided into the following sections:

- GLOBAL
- ACSD
- CLIENT
- DEVICE_CLASS *device*
- OFFLOAD
- OFFLOAD_DB2STANDBY
- ORACLE
- CLONING
- DB2STANDBY

There can be multiple DEVICE_CLASS sections. Each DEVICE_CLASS section must have a unique *device* instance name.

The profile must be available on all database nodes and on the system where the management agent, acsd, is running. In addition, the GLOBAL section of the profile is required on the host where the clone databases reside.

To overwrite Tivoli Storage FlashCopy Manager profile parameters for DB2 and for Oracle in an SAP environment, use vendor options.

GLOBAL The GLOBAL section contains information that is required and used by all Tivoli Storage FlashCopy Manager components. The section is used by all database nodes, and the management, device, and offload agents. The components reference the information in the GLOBAL section during the start up process. Changes to this section require a restart of Tivoli Storage FlashCopy Manager.

Tivoli Storage FlashCopy Manager can be installed on multiple systems within an environment. For example, when a database is distributed among multiple application hosts or when a backup server is used to transfer snapshot backups to Tivoli Storage Manager. When Tivoli Storage FlashCopy Manager is installed on multiple systems within an environment, there is only one active management agent. The location of this management agent is specified in GLOBAL section using the **ACSD** parameter.

Other parameters in the GLOBAL section specify the location for logging, tracing, and password files. On the backup server, the only section of profile that is referenced is GLOBAL.

ACSD The ACSD section contains information that is used exclusively by the management agent, acsd. This section includes the **ACS_REPOSITORY** parameter. The **ACS_REPOSITORY** parameter specifies the directory where the management agent stores its backup repository. This repository is the most important collection of Tivoli Storage FlashCopy Manager data. If the repository is lost, any previously created backup cannot be restored.

CLIENT The CLIENT section contains all parameters relating to backup operations, including parameters for 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_CLASS** 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.

(Oracle in an SAP environment only) When configuring offloaded backups, the profile does not contain a CLIENT section. The information that is usually referenced in the CLIENT section is stored in the .utl file. For more information about the .utl file, see “BACKINT configuration file” on page 207.

DEVICE_CLASS *device*

The **DEVICE_CLASS** section contains parameters that are related to the storage solution or file system (file system snapshots). At least one **DEVICE_CLASS** section is required for the configuration of the management agent. A **DEVICE_CLASS** section describes the characteristics of a storage device or file system that can be used to create a snapshot backup. The parameters and options that are used in the **DEVICE_CLASS** section depend on the storage solution.

Each storage solution that is used in the environment must have a **DEVICE_CLASS** section and must have a unique *device* instance name.

The **DEVICE_CLASS** section that is used is determined by the value of the **DEVICE_CLASS** parameter in the CLIENT section of the profile for backup operation. For cloning operations, this value is determined by the

DEVICE_CLASS parameter in the CLONING section of the profile. If the same value is specified for the DEVICE_CLASS parameter in both the CLIENT and CLONING sections, an error is reported.

The value of DEVICE_CLASS *device* is recorded in the Tivoli Storage FlashCopy Manager repository to identify the appropriate DEVICE_CLASS section during the restore process. Therefore, use caution when you delete or rename DEVICE_CLASS sections. If the appropriate section cannot be found, then the data that is backed up cannot be restored.

For each DEVICE_CLASS section, a password is required and can be set by running the setup script without the -a action option. For example:

```
setup_type.sh -d <Instance owner $HOME directory>
```

The password can be set in a batch processing mode using the following **fcmccli** command: **fcmccli -f password**

These passwords are used by Tivoli Storage FlashCopy Manager to authenticate to the storage solution represented by the DEVICE_CLASS section.

OFFLOAD

The parameters and options in the OFFLOAD section determine how a snapshot is transferred to Tivoli Storage Manager. The information is sent to the offload agent, tsm4acs.

To configure Tivoli Storage FlashCopy Manager for protection of both active and standby nodes of a DB2 high-availability disaster recovery (HADR) environment, have two OFFLOAD sections in the profile: OFFLOAD and OFFLOAD_DB2STANDBY.

When the offload agent is started, it connects to the management agent and queries for snapshot backups that have been backed up with the **TSM_BACKUP** parameter that is set to YES. For Oracle in an SAP environment systems, the **TSM_BACKUP_FROM_SNAPSHOT** parameter is used instead of the **TSM_BACKUP** parameter. If this parameter and option is found, the offload agent mounts the snapshot and initiates a Tivoli Storage Manager backup using one of the following applications:

- (DB2) The DB2 built-in Tivoli Storage Manager agent
- (Oracle in an SAP environment or DB2) IBM Tivoli Storage Manager for Enterprise Resource Planning (Tivoli Storage Manager for ERP)
- (Oracle) Oracle RMAN and Data Protection for Oracle
- (FlashCopy Manager for Custom Applications) Tivoli Storage Manager backup-archive client

If one of the following conditions exists, the OFFLOAD section is required. If neither condition exists, the OFFLOAD section is optional.

- (Oracle in an SAP environment) Tivoli Storage Manager for ERP is used for an offload tape backup. In this scenario, the OFFLOAD section includes at least the **PROFILE** parameter.
- One or more of the default values must be overridden.

OFFLOAD_DB2STANDBY

The OFFLOAD_DB2STANDBY section uses the same semantics as the OFFLOAD section, except that the section is evaluated when an offloaded backup from a DB2 HADR secondary occurs. In most environments, the profile also includes an OFFLOAD section to protect databases when the DB2 HADR primary and secondary have switched roles.

ORACLE As the name implies, the ORACLE section is only used to identify parameters and options that describe the Oracle database. The ORACLE section is not needed for Oracle in an SAP environment configurations.

CLONING

The CLONING section contains the parameters used for cloning operations. The section is ignored for all other operations.

DB2STANDBY

As the name implies, the DB2STANDBY section is used when backing up the standby node of a DB2 HADR environment. Although Tivoli Storage FlashCopy Manager also evaluates all parameters specified within the CLIENT section during HADR operations, some parameters specified in the DB2STANDBY section override the corresponding parameters specified in the CLIENT section.

Examples

All parameters in a section are indicated by a section start notation, `>>>` *section_name*, and a section end notation, `<<<` *section_name*. The name is optional on the section end notation. Comments can be used at any place within the profile. Comments start with a # character and extend to the end of the line. Tab characters are permitted. The following example provides an example of the profile configuration file:

```
# Global section
>>> GLOBAL
parametername1 value1
parametername2 value1 value2
....
<<<
# ACSD section
>>> ACSD
parametername1 value1
parametername2 value1 value2
....
<<<
# CLIENT section
>>> CLIENT
parametername1 value1
parametername2 value1 value2
....
<<<
# DEVICE_CLASS device section
>>> DEVICE_CLASS device
parametername1 value1
parametername2 value1 value2
....
<<<
# DEVICE_CLASS device2 section
>>> DEVICE_CLASS device2device2
parametername1 value1
parametername2 value1 value2
....
<<<
# OFFLOAD section
>>> OFFLOAD
parametername1 value1
parametername2 value1 value2
....
<<<
# ORACLE section
>>> ORACLE
parametername1 value1
```

```

parametername2 value1 value2
....
<<<
# CLONING section
>>> CLONING
parametername1 value1
parametername2 value1 value2
....
<<<
# DB2STANDBY section
>>> DB2STANDBY
parametername1 value1
parametername2 value1 value2
....
<<<

```

The following example is a sample profile for DB2 including cloning and backup of a standby node of a DB2 HADR environment.

```

>>> GLOBAL
ACS_DIR /db2/AS1/acs
ACSD auntmathilda 54331
# TRACE NO
<<<

>>> ACSD
ACS_REPOSITORY /db2/AS1/acs/acsrepository
# ADMIN_ASSISTANT levi 5126
# REPOSITORY_LABEL TSM
<<<

>>> CLIENT
# BACKUPIDPREFIX DB2_____
APPLICATION_TYPE SAP
# PARTITION_GROUP
TSM_BACKUP YES
# MAX_VERSIONS ADAPTIVE
# LVM_FREEZE_THAW AUTO
# NEGATIVE_LIST no_check
# TIMEOUT_FLASH 120
# GLOBAL_SYSTEM_IDENTIFIER
# DEVICE_CLASS STANDARD
<<<

>>> OFFLOAD
BACKUP_METHOD DB2
OPTIONS @/db2/AS1/dbs/vendor.env.%DB2NODE
# PARALLELISM AUTO
# NUM_SESSIONS 1
# NUM_BUFFERS AUTO
# BUFFER_SIZE AUTO
<<<

>>> DB2STANDBY
DB2_PRODUCTIVE_SERVER akuma DB2_db2as1_svc
DB2_ALIAS AS1
PRE_FLASH_CMD /db2/AS1/acs/db2_pre_flash_script.cmd
POST_FLASH_CMD /db2/AS1/acs/db2_post_flash_script.cmd
DB2_USERNAME db2as1
DB2_AUTH_TYPE SERVER
<<<

>>> OFFLOAD_DB2STANDBY
BACKUP_METHOD TSM_CLIENT
# MODE FULL
ASNODENAME AS1TEST
# DSM_DIR

```

```

# DSM_CONFIG
# VIRTUALFSNAME fcm
<<<

>>> CLONING
DEVICE_CLASS CLONE1 USE_FOR_CLONING AS2
<<<

>>> DEVICE_CLASS STANDARD
COPYSERVICES_HARDWARE_TYPE DS8000
COPYSERVICES_PRIMARY_SERVERNAME uncltetus
# COPYSERVICES_SECONDARY_SERVERNAME
COPYSERVICES_USERNAME tsmuser
# COPYSERVICES_COMMPROTOCOL HTTPS
# COPYSERVICES_CERTIFICATEFILE NO_CERTIFICATE
# COPYSERVICES_SERVERPORT 5989
FLASHCOPY_TYPE NOCOPY
# COPYSERVICES_TIMEOUT 6
# RESTORE_FORCE NO
# STORAGE_SYSTEM_ID
TARGET_SETS VOLUMES_FILE
VOLUMES_FILE /db2/AS1/acs/acsvolumes/fct.file
<<<

>>> DEVICE_CLASS CLONE1
COPYSERVICES_HARDWARE_TYPE DS8000
COPYSERVICES_PRIMARY_SERVERNAME uncltetus
# COPYSERVICES_SECONDARY_SERVERNAME
COPYSERVICES_USERNAME tsmuser
# COPYSERVICES_COMMPROTOCOL HTTPS
# COPYSERVICES_CERTIFICATEFILE NO_CERTIFICATE
# COPYSERVICES_SERVERPORT 5989
# FLASHCOPY_TYPE COPY
# COPYSERVICES_TIMEOUT 6
# RESTORE_FORCE NO
# STORAGE_SYSTEM_ID
TARGET_SETS VOLUMES_FILE
VOLUMES_FILE /db2/AS1/acs/acsvolumes/fct.file.cloning
CLONE_DATABASE YES
<<<

```

GLOBAL

The profile parameters in the GLOBAL section contain basic configuration information. Examples of the type of information that is specified by the parameters are the port that is used by Tivoli Storage FlashCopy Manager and the location of log files. The parameters are independent of the storage solution, database application, and custom application.

The following list provides the parameters, a description of each parameter, and default values for the GLOBAL section of the profile configuration file.

ACS_DIR

Path to the IBM Tivoli Storage FlashCopy Manager configuration directory. This parameter is required. The following subdirectories are included in this directory:

logs The subdirectory contains all log and trace information for Tivoli Storage FlashCopy Manager.

shared The subdirectory contains information that is shared among all Tivoli Storage FlashCopy Manager components.

When the subdirectory is initially created, the only file that is stored in the directory is the password file: `pwd.acsd`. This file contains the

passwords for all devices that are specified within the profile. The file also contains a master password that is used from all components for authentication when they are connecting to the management agent. When you are running remote configuration tasks from the production system with SSH, the information in these directories is promoted to all systems that belong to the instance where Tivoli Storage FlashCopy Manager is configured.

Default

user_home/acs

Advanced mode only

Yes

ACSD

The host name and port of the system where the management agent is running. The following format is used for **ACSD**: *hostname port*

This parameter must be identical on all systems where Tivoli Storage FlashCopy Manager is installed for a database instance. While the parameter must be identical, each database instance can be managed by an individual management agent.

Default

hostname 57328

Advanced mode only

Yes

ENFORCE_TLS12

Tivoli Storage FlashCopy Manager uses the security suite, IBM Global Security Kit (GSKit) for Secure Socket Layer / Transport Layer Security (SSL/TLS) TCP/IP connections. GSKit is able to provide SP800-131 compliant encryption by using the TLS protocol V1.2. To enforce the use of this protocol, select the option YES, otherwise the TLS version 1.0 and 1.1 is enabled by default.

Default

NO

Advanced mode only

Yes

TRACE

There are two options for **TRACE**: YES and NO. YES means that tracing is enabled. NO means that tracing is disabled.

This parameter can also be set in the .utl file. For more information about the .utl file, see "BACKINT configuration file" on page 207.

Default

NO

Advanced mode only

Yes

ACSD

Except where noted, the profile parameters in the ACSD section are independent of the storage device or application.

ACS_REPOSITORY

This parameter sets the path to the IBM Tivoli Storage FlashCopy Manager repository. This directory is used during restore operations and must be in a secure location. If the repository is lost, all backups are not available.

The directory that is referenced by the **ACS_REPOSITORY** parameter cannot be in a file system that participates in snapshot backup operations. If the directory is part of a file system that is used for snapshot backup operations, Tivoli Storage FlashCopy Manager reports a failure. The Tivoli Storage FlashCopy Manager repository cannot be in the main Tivoli Storage FlashCopy Manager directory that is specified by the **ACS_DIR** parameter. Ideally, the **ACS_REPOSITORY** directory is a subdirectory of the **ACS_DIR** directory. For example:

```
<ACS_DIR>/acsrepository
```

Before you configure Tivoli Storage FlashCopy Manager, the path to the **ACS_REPOSITORY** is set, but the directory does not exist. The **ACS_REPOSITORY** directory is created during the configuration process. If the directory specified for the **ACS_REPOSITORY** parameter exists, the setup script, used to configure Tivoli Storage FlashCopy Manager, reports an error.

Default

user_home/acs/acsrepository.

Advanced mode only

Yes.

ADMIN_ASSISTANT

In non-SAP environments, this parameter is ignored. If Tivoli Storage Manager for ERP and the Administration Assistant component are installed, when this parameter is set, Tivoli Storage FlashCopy Manager sends backup and restore information to the Administration Assistant.

```
<server> <port>
```

Server and port where the Tivoli Storage Manager for ERP Administration Assistant server component is listening.

NO Do not send data to the Administration Assistant.

Default

NO

Advanced mode only

Yes.

REPOSITORY_LABEL

When this parameter is set, a prefix is added to each volume name on the IBM XIV Storage System, IBM System Storage N series, and NetApp Storage System. The prefix contains 3 characters in one of the following ranges:

[a-z]
[A-Z]
[0-9]

Note: If the repository label changes, backups that are created with the prior repository label are excluded from reconciliation.

Default

TSM

Advanced mode only

Yes.

SYNCHRONOUS_RECONCILE

This parameter is used to configure Tivoli Storage FlashCopy Manager to synchronously reconcile and delete snapshot backups. If the `RESTORE_AND_DELETE` option is specified for this parameter, a delete and restore operation also starts a synchronous delete and reconcile operation. This process can be useful for storage systems that can delete snapshot backups during a Tivoli Storage FlashCopy Manager snapshot restore process. Deletion can occur on N series, NetApp, Storwize family, or SAN Volume Controller storage systems. Also, this process is useful if you manually delete snapshot backups and use the force option (`-f`) on DS8000, SAN Volume Controller, or Storwize family storage systems.

If the `YES` option is specified in addition to the delete and restore operation, a backup operation also starts a synchronous delete and reconcile process. This process can be useful for storage systems that delete snapshot backups during a Tivoli Storage FlashCopy Manager backup or cloning operation. Deletion can occur on SAN Volume Controller or Storwize family storage systems. The following list identifies the possible options:

NO Use this option not to start a synchronous delete and reconcile operation.

YES

Use this option to start a synchronous delete and reconcile process as part of a backup, restore, and delete operation.

RESTORE_AND_DELETE

Use this option to start a synchronous delete and reconcile process as part of a restore and delete operation.

Default

`RESTORE_AND_DELETE`

Advanced mode only

`YES`

CLIENT

The `CLIENT` section of the Tivoli Storage FlashCopy Manager profile file contains parameters that relate to database and custom applications. The parameters do not depend on the storage solution. The client section is required for all database and custom applications except for Oracle in an SAP environment. When you use Oracle in an SAP environment databases and Tivoli Storage FlashCopy Manager with IBM Tivoli Storage Manager for Enterprise Resource Planning, the Tivoli Storage FlashCopy Manager profile does not contain a `CLIENT` section.

CLIENT parameters for DB2 databases

Tivoli Storage FlashCopy Manager uses the DB2 specific parameters to configure DB2 backup and restore operations. These parameters are defined in the client section of the Tivoli Storage FlashCopy Manager profile configuration file.

The ability to create a Tivoli Storage Manager backup from a snapshot requires a Tivoli Storage FlashCopy Manager license.

APPLICATION_TYPE

This parameter specifies the environment. The following list identifies the possible options:

DB2

Use as a DB2 database.

SAP

Use as a DB2 in an SAP environment database.

BACKUPIDPREFIX

This parameter specifies a string that is added before the backup ID that is generated by Tivoli Storage FlashCopy Manager. This parameter is used to separate the backups within the same repository. When you use this parameter, other clients are not able to query, restore, or delete these backups.

The string can contain letters, digits, or the underscore character (_). Except in DB2 environments, the string must be exactly 6 characters.

Default

None

Advanced mode only

Yes

DEVICE_CLASS

This parameter specifies the device classes to use. The following sample identifies the syntax that can be used with the **DEVICE_CLASS** parameter:

`DEVICE_CLASS list_of_device_classes [conditions]`

When a list of device classes is specified, the software determines which device class matches the device class in the environment. When multiple device classes are specified, separate the device classes names with a space. The condition statement is optional. When you use the condition statement, use the following syntax:

`[USE_AT days of week] [FROM time TO time]
(partitioned DB2 databases) [ON_DBPARTITIONNUMS list of partitions]`

Note: The time period that is specified cannot span midnight for a device class. If a device class time period is required to span midnight, you must specify two time periods for the device class. The first time period must end with a value 1 minute before midnight and the second time period must start at midnight. The following example shows how to specify a time period that spans midnight for a device class:

`DEVICE_CLASS myClass FROM 20:00 TO 23:59
DEVICE_CLASS myClass FROM 00:00 TO 06:00`

When there are different devices, multiple sections can be used. Each section provides information about a particular device. To select a particular section, use the **DEVICE_CLASS** parameter. When the software restores data, the software uses the **DEVICE_CLASS** value that is specified when the data was backed up.

The configuration wizard (the setup script) automatically adds **DEVICE_CLASS** sections to the Tivoli Storage FlashCopy Manager profile when you add more instances of the **DEVICE_CLASS** parameter to the CLIENT section of the profile.

Default

STANDARD

Advanced mode only

No

GLOBAL_SYSTEM_IDENTIFIER

This parameter specifies a string to be used in the IBM Tivoli Storage Manager for Enterprise Resource Planning Administration Assistant that uniquely

identifies a DB2 or Oracle database in the system landscape. This parameter is only valid when the **ADMIN_ASSISTANT** parameter is specified in the ACSD section of the profile.

Default

Depending on the environment, the default value is either *DB2_<DBname>* or *ORA_<DBname>*.

Advanced mode only

Yes

LVM_FREEZE_THAW

This parameter specifies when to enable file system freeze and thaw actions. The following list identifies the possible options:

YES

Enable file system freeze before the snapshot operation and the thaw after the snapshot operation. For AIX, the YES value can be used only when all file systems included in the backup are JFS2 file systems.

NO Do not freeze the file system. To set this parameter to NO, a licensed version of Tivoli Storage FlashCopy Manager is needed and a backup server is required for mounting the snapshot to ensure file system consistency.

The value NO is required if at least one file system that does not support freeze or thaw actions, such as JFS, is involved.

AUTO

If the **TARGET_DATABASE_SUSPEND** parameter is YES, then this parameter is set with the following option: **LVM_FREEZE_THAW YES**. If the file system does not support freeze actions, the AUTO value is NO.

For more information, see “Interdependency of **LVM_FREEZE_THAW** and **TARGET_DATABASE_SUSPEND**” on page 199.

Default

AUTO

Advanced mode only

Yes

MAX_VERSIONS

This parameter specifies the number of snapshot versions to store. The following list identifies the possible options:

ADAPTIVE

The maximum number varies depending on the available space. Tivoli Storage FlashCopy Manager reuses the oldest target set as the target for the current backup. You cannot use the ADAPTIVE value in a DB2 pureScale environment, you must specify the maximum number of snapshots to be stored (*n*).

n Where *n* is the maximum number of snapshot versions to be stored. In a DB2 pureScale environment, the file system must have sufficient free space for all snapshots. The amount of space that is required depends on the following factors:

- The number of snapshots.
- For each snapshot, the number of changes to the file system content since the snapshot was taken.

When this limit is reached, the oldest version is deleted.

Default

ADAPTIVE

Advanced mode only

No

NEGATIVE_LIST

This parameter is used to control file processing. This processing occurs when files not associated with the database are stored within the same file system that is used for the backup and restore operations. This parameter is required. The following list identifies the possible options:

NO_CHECK

Use this option to not check for extra files. The operation ignores any additional files that are identified. When you use this option and data is restored, all files on the file system or volume group are overwritten.

WARN

Use this option to receive a warning message for each file that is identified on the volume, but not part of the FlashCopy operation. The processing continues. When you use this option and data is restored, all files on the file system or volume group are overwritten.

ERROR

Use this option to receive an error message for each file that is discovered on the volume, but not part of the FlashCopy operation. The processing ends.

filename

Where *filename* is a name of a file that contains a list of fully qualified names of files and directories, each name requires a new line. Only files or directories that are not associated with the database but are stored within the file system that is used for backup operations are listed. Any file that is identified by Tivoli Storage FlashCopy Manager that is not part of the database files or is not in the **NEGATIVE_LIST** file, causes processing to end. Any directory that is listed in the **NEGATIVE_LIST** file is processed recursively. For example, all files within the directory, including subdirectories, are processed during a backup or restore request.

Default

None

Advanced mode only

No

PARTITION_GROUP

This parameter is used in multi-partition DB2 in SAP environments, when multiple partitions are in the same volume group for volume sharing. Use this parameter to specify all partitions that have the same volume group. This parameter can be specified multiple times. When a **PARTITION_GROUP** parameter is specified, the **VOLUMES_FILE** parameter must be used to specify the .fct file. In a DB2 pureScale environment, there is one data partition and therefore this parameter is not used. The following list identifies the possible options:

<group name>

The name of the partition group.

<db2 node>

The name of the DB2 node. When multiple entries are specified, each entry is separated by a space character.

The following sample is an example of how to use the **PARTITION_GROUP** parameter:

```
>>> CLIENT
...
PARTITION_GROUP ONE 0 1
PARTITION_GROUP TWO 2 3
...
<<<
```

For an example of an .fct file in this scenario, see “Target set definition file for multi-partition DB2 databases” on page 70.

Default

None

Advanced mode only

Yes

TIMEOUT_FLASH

This parameter specifies the maximum time, in seconds, that the database agent waits for a response to the management agent call during the *flash* phase. If the database agent does not receive a response within the specified time, an error message is displayed. This parameter allows the maximum time to be specified for a database to be suspended. This parameter also implies the maximum time when JFS2 file systems can be frozen. When the timeout is reached, the file systems thaw, the database is resumed, and the backup operation ends with an error. If the **LVM_FREEZE_THAW** parameter is set to either **AUTO** or **YES**, the minimal value for **TIMEOUT_FLASH** is 5 seconds. In other scenarios, the minimal value is 1 second.

Default

The default value is 120 seconds.

Advanced mode only

Yes

TIMEOUT_PHASE

This parameter specifies the maximum time, in seconds, that the database agent waits for a response to the management agent call during a specific operation phase. If the database agent does not receive a response within the specified time, either the backup or restore operation ends and an error message is shown.

Specify one of the following phase values for a FlashCopy backup:

- **PARTITION**
- **PREPARE**
- **FLASH** (this parameter has a separate description)
- **VERIFY**
- **CLOSE**

For example, **TIMEOUT_PREPARE**.

Specify one of the following phase values for a FlashCopy restore:

- **PREPARERESTORE**
- **FLASHRESTORE**
- **COMPLETERESTORE**
- **CLOSE**

For example, **TIMEOUT_FLASHRESTORE**.

Default

The default value is 3600 seconds.

Advanced mode only

Yes

TSM_BACKUP

This parameter specifies whether to create a Tivoli Storage Manager backup from a snapshot. Tivoli Storage FlashCopy Manager must be installed on a backup server. When the **TSM_BACKUP** parameter is set to YES, MANDATE, or LATEST, and after the offload agent runs, a Tivoli Storage Manager backup is created from the snapshot. The following list identifies the possible options:

YES

This option creates a Tivoli Storage Manager backup from a snapshot. If the Tivoli Storage Manager backup operation does not successfully complete, the target set can be reused.

MANDATE

This option creates a Tivoli Storage Manager backup from a snapshot. However, the target set cannot be reused until the Tivoli Storage Manager backup successfully completes.

LATEST

This option removes a backup request to Tivoli Storage Manager from a previous backup. When a new snapshot with **TSM_BACKUP** set to LATEST, YES, or MANDATE is created, Tivoli Storage FlashCopy Manager removes any unsuccessful backup request that were previously created with the **TSM_BACKUP** option set to LATEST. This option prevents backup requests to Tivoli Storage Manager from queuing if they are not completed in time.

NO Keeps the snapshot backup but the snapshot is not used as a source for a subsequent tape backup operation.

TSM_ONLY

After the Tivoli Storage Manager backup is completed, during the unmount operation, the backup is automatically marked for deletion. This action occurs regardless of whether the backup is successful or not.

USE_FOR *list of device classes*

To create a Tivoli Storage Manager backup from snapshots that are run with particular device classes, as specified in the profile, combine this attribute with other options. When you list device classes, separate device classes with the space character. There is no limit of the number of device classes.

Default

None

Advanced mode only

No

CLIENT parameters for Oracle databases

Tivoli Storage FlashCopy Manager uses the Oracle specific parameters to configure Oracle backup and restore operations. These parameters are defined in the client section of the Tivoli Storage FlashCopy Manager profile configuration file.

Oracle databases

When using Oracle databases, in addition to the CLIENT section, an ORACLE section is included in the profile configuration file. For more information about the ORACLE section, see "ORACLE" on page 164.

APPLICATION_TYPE

This parameter specifies the environment. There is only one option:

ORACLE

Use as an Oracle system.

BACKUPIDPREFIX

This parameter specifies a string that is added before the backup ID that is generated by Tivoli Storage FlashCopy Manager. This parameter is used to separate the backups within the same repository. When you use this parameter, other clients are not able to query, restore, or delete these backups.

The string can contain letters, digits, or the underscore character (_). Except in DB2 environments, the string must be exactly 6 characters.

Default

None

Advanced mode only

Yes

DEVICE_CLASS

This parameter specifies the device classes to use. The following sample identifies the syntax that can be used with the **DEVICE_CLASS** parameter:

```
DEVICE_CLASS list_of_device_classes [conditions]
```

When a list of device classes is specified, the software determines which device class matches the device class in the environment. When multiple device classes are specified, separate the device classes names with a space. The condition statement is optional. When you use the condition statement, use the following syntax:

```
[USE_AT days of week] [FROM time TO time]
```

Note: The time period that is specified cannot span midnight for a device class. If a device class time period is required to span midnight, you must specify two time periods for the device class. The first time period must end with a value 1 minute before midnight and the second time period must start at midnight. The following example shows how to specify a time period that spans midnight for a device class:

```
DEVICE_CLASS myClass FROM 20:00 TO 23:59  
DEVICE_CLASS myClass FROM 00:00 TO 06:00
```

When there are different devices, multiple sections can be used. Each section provides information about a particular device. To select a particular section, use the **DEVICE_CLASS** parameter. When the software restores data, the software uses the **DEVICE_CLASS** value that is specified when the data was backed up.

The configuration wizard (the setup script) automatically adds **DEVICE_CLASS** sections to the Tivoli Storage FlashCopy Manager profile when you add more instances of the **DEVICE_CLASS** parameter to the **CLIENT** section of the profile.

Default

STANDARD

Advanced mode only

No

GLOBAL_SYSTEM_IDENTIFIER

This parameter specifies a string to be used in the IBM Tivoli Storage Manager for Enterprise Resource Planning Administration Assistant that uniquely identifies a DB2 or Oracle database in the system landscape. This parameter is only valid when the **ADMIN_ASSISTANT** parameter is specified in the **ACSD** section of the profile.

Default

Depending on the environment, the default value is either *DB2_<DBname>* or *ORA_<DBname>*.

Advanced mode only

Yes

LVM_FREEZE_THAW

This parameter specifies when to enable file system freeze and thaw actions. The following list identifies the possible options:

YES

Enable file system freeze before the snapshot operation and the thaw after the snapshot operation. For AIX, the YES value can be used only when all file systems included in the backup are JFS2 file systems.

NO Do not freeze the file system. To set this parameter to NO, a licensed version of Tivoli Storage FlashCopy Manager is needed and a backup server is required for mounting the snapshot to ensure file system consistency.

The value NO is required if at least one file system that does not support freeze or thaw actions, such as JFS, is involved.

AUTO

If the **TARGET_DATABASE_SUSPEND** parameter is YES, then this parameter is set with the following option: **LVM_FREEZE_THAW YES**. If the file system does not support freeze actions, the AUTO value is NO.

For more information, see “Interdependency of **LVM_FREEZE_THAW** and **TARGET_DATABASE_SUSPEND**” on page 199.

Default

AUTO

Advanced mode only

Yes

MAX_VERSIONS

This parameter specifies the number of snapshot versions to store. The following list identifies the possible options:

ADAPTIVE

The maximum number varies depending on the available space. Tivoli Storage FlashCopy Manager reuses the oldest target set as the target for the current backup.

- n* This number specifies the maximum number of snapshot versions to be stored. When this limit is reached, the oldest version is deleted.

Default

ADAPTIVE

Advanced mode only

No

NEGATIVE_LIST

This parameter is used to control file processing. This processing occurs when files not associated with the database are stored within the same file system that is used for the backup and restore operations. This parameter is required. The following list identifies the possible options:

NO_CHECK

Use this option to not check for extra files. The operation ignores any additional files that are identified. When you use this option and data is restored, all files on the file system or volume group are overwritten.

WARN

Use this option to receive a warning message for each file that is identified on the volume, but not part of the FlashCopy operation. The processing continues. When you use this option and data is restored, all files on the file system or volume group are overwritten.

ERROR

Use this option to receive an error message for each file that is discovered on the volume, but not part of the FlashCopy operation. The processing ends.

filename

Where *filename* is a name of a file that contains a list of fully qualified names of files and directories, each name requires a new line. Only files or directories that are not associated with the database but are stored within the file system that is used for backup operations are listed. Any file that is identified by Tivoli Storage FlashCopy Manager that is not part of the database files or is not in the **NEGATIVE_LIST** file, causes processing to end. Any directory that is listed in the **NEGATIVE_LIST** file is processed recursively. For example, all files within the directory, including subdirectories, are processed during a backup or restore request.

Default

None

Advanced mode only

No

TARGET_DATABASE_SUSPEND

This parameter determines if the activity is suspended on the target database until the FlashCopy operation completes. The following list identifies the possible options:

Yes

This option suspends the target database until the FlashCopy operation completes. When there are many transactions processing, use this option.

- NO** This option means that the target database is available while FlashCopy operations run.

OFFLINE

All backups must be offline for the FlashCopy operations to run. When

either `acsora` or `acsutil` is issued, the target database on the production system must be in a *startup mount* state. If the state is not *startup mount*, recovery is necessary to restore the database.

Default

Yes.

Advanced mode only

Yes.

For more information about the **TARGET_DATABASE_SUSPEND**, see “Interdependency of **LVM_FREEZE_THAW** and **TARGET_DATABASE_SUSPEND**” on page 199.

TIMEOUT_FLASH

This parameter specifies the maximum time, in seconds, that the database agent waits for a response to the management agent call during the *flash* phase. If the database agent does not receive a response within the specified time, an error message is displayed. This parameter allows the maximum time to be specified for a database to be suspended. This parameter also implies the maximum time when JFS2 file systems can be frozen. When the timeout is reached, the file systems thaw, the database is resumed, and the backup operation ends with an error. If the **LVM_FREEZE_THAW** parameter is set to either **AUTO** or **YES**, the minimal value for **TIMEOUT_FLASH** is 5 seconds. In other scenarios, the minimal value is 1 second.

Default

The default value is 120 seconds.

Advanced mode only

Yes

TIMEOUT_PHASE

This parameter specifies the maximum time, in seconds, that the database agent waits for a response to the management agent call during a specific operation phase. If the database agent does not receive a response within the specified time, either the backup or restore operation ends and an error message is shown.

Specify one of the following phase values for a FlashCopy backup:

- **PARTITION**
- **PREPARE**
- **FLASH** (this parameter has a separate description)
- **VERIFY**
- **CLOSE**

For example, **TIMEOUT_PREPARE**.

Specify one of the following phase values for a FlashCopy restore:

- **PREPARERESTORE**
- **FLASHRESTORE**
- **COMPLETERESTORE**
- **CLOSE**

For example, **TIMEOUT_FLASHRESTORE**.

Default

The default value is 3600 seconds.

Advanced mode only

Yes

TSM_BACKUP

This parameter specifies whether to create a Tivoli Storage Manager backup from a snapshot. Tivoli Storage FlashCopy Manager must be installed on a backup server. When the **TSM_BACKUP** parameter is set to YES, MANDATE, or LATEST, and after the offload agent runs, a Tivoli Storage Manager backup is created from the snapshot. The following list identifies the possible options:

YES

This option creates a Tivoli Storage Manager backup from a snapshot. If the Tivoli Storage Manager backup operation does not successfully complete, the target set can be reused.

MANDATE

This option creates a Tivoli Storage Manager backup from a snapshot. However, the target set cannot be reused until the Tivoli Storage Manager backup successfully completes.

LATEST

This option removes a backup request to Tivoli Storage Manager from a previous backup. When a new snapshot with **TSM_BACKUP** set to LATEST, YES, or MANDATE is created, Tivoli Storage FlashCopy Manager removes any unsuccessful backup request that were previously created with the **TSM_BACKUP** option set to LATEST. This option prevents backup requests to Tivoli Storage Manager from queuing if they are not completed in time.

NO Keeps the snapshot backup but the snapshot is not used as a source for a subsequent tape backup operation.

TSM_ONLY

After the Tivoli Storage Manager backup is completed, during the unmount operation, the backup is automatically marked for deletion. This action occurs regardless of whether the backup is successful or not.

USE_FOR *list of device classes*

To create a Tivoli Storage Manager backup from snapshots that are run with particular device classes, as specified in the profile, combine this attribute with other options. When you list device classes, separate device classes with the space character. There is no limit of the number of device classes.

Default

None

Advanced mode only

No

VOLUME_MGR

The following list identifies the possible options:

ASM

When this option is selected, the option that is set for the **LVM_FREEZE_THAW** parameter is ignored. When this parameter is ignored, there is no file system, and the wizard does not query for data.

LVM

When this option is selected, the ASM-related options in the **DEVICE_CLASS** section is ignored and not queried by the wizard software.

Default*LVM***Advanced mode only**

No.

CLIENT parameters for Oracle in an SAP environment databases

When Tivoli Storage FlashCopy Manager is used with IBM Tivoli Storage Manager for Enterprise Resource Planning, and Oracle in an SAP environment, the client parameters are included in the IBM Tivoli Storage Manager for Enterprise Resource Planning configuration file, *.utl* file.

For information about the IBM Tivoli Storage Manager for Enterprise Resource Planning configuration file, see “BACKINT configuration file” on page 207. In addition, parameters must be specified in the SAP BRTOOLS configuration file, *.sap* file. For more information, see “Oracle in an SAP environment BR*Tools configuration profile (*.sap*)” on page 218.

APPLICATION_TYPE

This parameter specifies the environment. There is only one option:

SAP_ORACLE

Use as an Oracle system.

BACKUPIDPREFIX

This parameter specifies a string that is added before the backup ID that is generated by Tivoli Storage FlashCopy Manager. This parameter is used to separate the backups within the same repository. When you use this parameter, other clients are not able to query, restore, or delete these backups.

The string can contain letters, digits, or the underscore character (*_*). Except in DB2 environments, the string must be exactly 6 characters.

Default

None

Advanced mode only

Yes

DEVICE_CLASS

This parameter specifies the device classes to use. The following sample identifies the syntax that can be used with the **DEVICE_CLASS** parameter:

```
DEVICE_CLASS list_of_device_classes [conditions]
```

When a list of device classes is specified, the software determines which device class matches the device class in the environment. When multiple device classes are specified, separate the device classes names with a space. The condition statement is optional. When you use the condition statement, use the following syntax:

```
[USE_AT days of week] [FROM time TO time]
```

Note: The time period that is specified cannot span midnight for a device class. If a device class time period is required to span midnight, you must specify two time periods for the device class. The first time period must end with a value 1 minute before midnight and the second time period must start at midnight. The following example shows how to specify a time period that spans midnight for a device class:

```
DEVICE_CLASS myClass FROM 20:00 TO 23:59
DEVICE_CLASS myClass FROM 00:00 TO 06:00
```

When there are different devices, multiple sections can be used. Each section provides information about a particular device. To select a particular section, use the **DEVICE_CLASS** parameter. When the software restores data, the software uses the **DEVICE_CLASS** value that is specified when the data was backed up.

The configuration wizard (the setup script) automatically adds **DEVICE_CLASS** sections to the Tivoli Storage FlashCopy Manager profile when you add more instances of the **DEVICE_CLASS** parameter to the CLIENT section of the profile.

Default

STANDARD

Advanced mode only

No

GLOBAL_SYSTEM_IDENTIFIER

This parameter specifies a string to be used in the IBM Tivoli Storage Manager for Enterprise Resource Planning Administration Assistant that uniquely identifies a DB2 or Oracle database in the system landscape. This parameter is only valid when the **ADMIN_ASSISTANT** parameter is specified in the ACSD section of the profile.

Default

Depending on the environment, the default value is either *DB2_<DBname>* or *ORA_<DBname>*.

Advanced mode only

Yes

LVM_FREEZE_THAW

This parameter specifies when to enable file system freeze and thaw actions. The following list identifies the possible options:

YES

Enable file system freeze before the snapshot operation and the thaw after the snapshot operation. For AIX, the YES value can be used only when all file systems included in the backup are JFS2 file systems.

NO Do not freeze the file system. To set this parameter to NO, a licensed version of Tivoli Storage FlashCopy Manager is needed and a backup server is required for mounting the snapshot to ensure file system consistency.

The value NO is required if at least one file system that does not support freeze or thaw actions, such as JFS, is involved.

AUTO

If the **TARGET_DATABASE_SUSPEND** parameter is YES, then this parameter is set with the following option: **LVM_FREEZE_THAW YES**. If the file system does not support freeze actions, the AUTO value is NO.

For more information, see “Interdependency of **LVM_FREEZE_THAW** and **TARGET_DATABASE_SUSPEND**” on page 199.

Default

AUTO

Advanced mode only

Yes

MAX_VERSIONS

This parameter specifies the number of snapshot versions to store. The following list identifies the possible options:

ADAPTIVE

The maximum number varies depending on the available space. Tivoli Storage FlashCopy Manager reuses the oldest target set as the target for the current backup.

- n* This number specifies the maximum number of snapshot versions to be stored. When this limit is reached, the oldest version is deleted.

Default

ADAPTIVE

Advanced mode only

No

TARGET_DATABASE_SUSPEND

This parameter determines if the activity is suspended on the target database until the FlashCopy operation completes. The following list identifies the possible options:

Yes

This option suspends the target database until the FlashCopy operation completes. When there are many transactions processing, use this option.

- NO** This option means that the target database is available while FlashCopy operations run.

OFFLINE

All backups must be offline for the FlashCopy operations to run. If the SAP software requests an offline backup, this parameter is ignored.

Default

Yes.

Advanced mode only

Yes.

For more information about the **TARGET_DATABASE_SUSPEND**, see “Interdependency of **LVM_FREEZE_THAW** and **TARGET_DATABASE_SUSPEND**” on page 199.

TIMEOUT_FLASH

This parameter specifies the maximum time, in seconds, that the database agent waits for a response to the management agent call during the *flash* phase. If the database agent does not receive a response within the specified time, an error message is displayed. This parameter allows the maximum time to be specified for a database to be suspended. This parameter also implies the maximum time when JFS2 file systems can be frozen. When the timeout is reached, the file systems thaw, the database is resumed, and the backup operation ends with an error. If the **LVM_FREEZE_THAW** parameter is set to either **AUTO** or **YES**, the minimal value for **TIMEOUT_FLASH** is 5 seconds. In other scenarios, the minimal value is 1 second.

Default

The default value is 120 seconds.

Advanced mode only

Yes

TIMEOUT_PHASE

This parameter specifies the maximum time, in seconds, that the database agent waits for a response to the management agent call during a specific

operation phase. If the database agent does not receive a response within the specified time, either the backup or restore operation ends and an error message is shown.

Specify one of the following phase values for a FlashCopy backup:

- **PARTITION**
- **PREPARE**
- **FLASH** (this parameter has a separate description)
- **VERIFY**
- **CLOSE**

For example, **TIMEOUT_PREPARE**.

Specify one of the following phase values for a FlashCopy restore:

- **PREPARERESTORE**
- **FLASHRESTORE**
- **COMPLETERESTORE**
- **CLOSE**

For example, **TIMEOUT_FLASHRESTORE**.

Default

The default value is 3600 seconds.

Advanced mode only

Yes

TSM_BACKUP

This parameter specifies whether or not to create a Tivoli Storage Manager backup from a snapshot. For Oracle in an SAP environment, in the .utl file, this parameter is named **TSM_BACKUP_FROM_SNAPSHOT**. For more information about the Oracle in an SAP environment .utl file, see “BACKINT configuration file” on page 207.

When Tivoli Storage FlashCopy Manager is installed on a backup server, you can create a Tivoli Storage Manager backup from a snapshot. When the **TSM_BACKUP** parameter is set to YES, MANDATE, or LATEST, and after the offload agent runs, a Tivoli Storage Manager backup is created from the snapshot. The following list identifies the possible options:

YES

This option creates a Tivoli Storage Manager backup from this snapshot. If the Tivoli Storage Manager backup operation does not successfully complete, the target set can be reused.

MANDATE

This option creates a Tivoli Storage Manager backup but the target set cannot be reused until the Tivoli Storage Manager backup successfully completes.

LATEST

This option removes a backup request to Tivoli Storage Manager from a previous backup. When a new snapshot with **TSM_BACKUP** set to LATEST, YES, or MANDATE is created, Tivoli Storage FlashCopy Manager removes any unsuccessful backup request that were previously created with the **TSM_BACKUP** option set to LATEST. This option prevents backup requests to Tivoli Storage Manager from queuing if they are not completed in time.

NO Keeps the snapshot backup but the snapshot is not used as a source for a subsequent tape backup operation.

TSM_ONLY

After the Tivoli Storage Manager backup is completed, during the unmount operation, the backup is automatically marked for deletion. This action occurs regardless of whether the backup is successful or not.

USE_FOR *list of device classes*

To create a Tivoli Storage Manager backup from snapshots that are performed with particular device classes, as specified in the profile, combine this attribute with other options. When you list device classes, separate device classes with the space character. There is no limit of the number of device classes.

Default

None

Advanced mode only

No

CLIENT parameters for custom applications

Tivoli Storage FlashCopy Manager uses specific custom application parameters to configure custom application backup and restore operations. These parameters are defined in the client section of the Tivoli Storage FlashCopy Manager profile configuration file.

Custom applications**APPLICATION_TYPE**

For this parameter, specify the environment. The following list identifies the possible options:

GENERIC

This parameter specifies that the Tivoli Storage FlashCopy Manager backup is a custom application backup.

Default

None. When you use the setup script, the option for this parameter is entered.

Advanced mode only

No

BACKUPIDPREFIX

This parameter specifies a string that is added before the backup ID that is generated by Tivoli Storage FlashCopy Manager. This parameter is used to separate the backups within the same repository. When you use this parameter, other clients are not able to query, restore, or delete these backups.

The string can contain letters, digits, or the underscore character (_). Except in DB2 environments, the string must be exactly 6 characters.

Default

None

Advanced mode only

Yes

DEVICE_CLASS

This parameter specifies the device classes to use. The following sample identifies the syntax that can be used with the **DEVICE_CLASS** parameter:

`DEVICE_CLASS list_of_device_classes [conditions]`

When a list of device classes is specified, the software determines which device class matches the device class in the environment. When multiple device classes are specified, separate the device classes names with a space. The condition statement is optional. When you use the condition statement, use the following syntax:

[USE_AT *days of week*] [FROM *time* TO *time*]

Note: The time period that is specified cannot span midnight for a device class. If a device class time period is required to span midnight, you must specify two time periods for the device class. The first time period must end with a value 1 minute before midnight and the second time period must start at midnight. The following example shows how to specify a time period that spans midnight for a device class:

```
DEVICE_CLASS myClass FROM 20:00 TO 23:59
DEVICE_CLASS myClass FROM 00:00 TO 06:00
```

When there are different devices, multiple sections can be used. Each section provides information about a particular device. To select a particular section, use the **DEVICE_CLASS** parameter. When the software restores data, the software uses the **DEVICE_CLASS** value that is specified when the data was backed up.

The configuration wizard (the setup script) automatically adds **DEVICE_CLASS** sections to the Tivoli Storage FlashCopy Manager profile when you add more instances of the **DEVICE_CLASS** parameter to the CLIENT section of the profile.

Default

STANDARD

Advanced mode only

No

ENHANCED_PARTITIONING

The **ENHANCED_PARTITIONING** parameter is used to control processing of the application file systems during the backup or restore operation. Tivoli Storage FlashCopy Manager fails, when a file system contains symbolic links that point to a file system on a different volume group that is not part of the FlashCopy operation. Set the **ENHANCED_PARTITIONING** parameter to NO to ensure that symbolic links if present are not processed. With this setting, there is no check for additional files that are not associated with the application. If you use this setting, the run time of the backup operation is likely to decrease depending on the file system structure. The following list identifies the possible options:

YES

Use this option to ensure that Tivoli Storage FlashCopy Manager processes all symbolic links of files or directories.

NO Use this option to ensure that Tivoli Storage FlashCopy Manager does not process symbolic links of files or directories.

Default

YES

Advanced mode only

Yes.

INFILE

This parameter is used when the **APPLICATION_TYPE** parameter is set to

GENERIC. This parameter identifies the file that contains a list of all objects to be processed. The file must meet the following requirements:

- Each line specifies only one file or directory to be backed up.
- A directory, including all subdirectories, is recursively processed. When the directory is expanded, links are followed.
- When a link to a file is specified, Tivoli Storage FlashCopy Manager protects the file system where the file is located. However, the file system where the link is located is disregarded.

The **INFILE** parameter can be overridden by an entry from the command-line interface. If the **INFILE** parameter is not specified in the profile configuration file, the parameter must be specified from the command-line interface.

Default

There is no default for this required parameter.

Advanced mode only

Yes.

LVM_FREEZE_THAW

This parameter specifies when to enable file system freeze and thaw actions. The following list identifies the possible options:

YES

Enable file system freeze before the snapshot operation and the thaw after the snapshot operation. For AIX, the YES value can be used only when all file systems included in the backup are JFS2 file systems.

NO

Do not freeze the file system. To set this parameter to NO, a licensed version of Tivoli Storage FlashCopy Manager is needed and a backup server is required for mounting the snapshot to ensure file system consistency.

The value NO is required if at least one file system that does not support freeze or thaw actions, such as JFS, is involved.

AUTO

If the **TARGET_DATABASE_SUSPEND** parameter is YES, then this parameter is set with the following option: **LVM_FREEZE_THAW YES**. If the file system does not support freeze actions, the AUTO value is NO.

For more information, see “Interdependency of **LVM_FREEZE_THAW** and **TARGET_DATABASE_SUSPEND**” on page 199.

Default

AUTO

Advanced mode only

Yes

MAX_VERSIONS

This parameter specifies the number of snapshot versions to store. The following list identifies the possible options:

ADAPTIVE

The maximum number varies depending on the available space. Tivoli Storage FlashCopy Manager reuses the oldest target set as the target for the current backup.

- n* This number specifies the maximum number of snapshot versions to be stored. When this limit is reached, the oldest version is deleted.

Default

ADAPTIVE

Advanced mode only

No

NEGATIVE_LIST

This parameter is used to control file processing. This processing occurs when files not associated with the database are stored within the same file system that is used for the backup and restore operations. This parameter is required. The following list identifies the possible options:

NO_CHECK

Use this option to not check for extra files. The operation ignores any additional files that are identified. When you use this option and data is restored, all files on the file system or volume group are overwritten.

WARN

Use this option to receive a warning message for each file that is identified on the volume, but not part of the FlashCopy operation. The processing continues. When you use this option and data is restored, all files on the file system or volume group are overwritten.

ERROR

Use this option to receive an error message for each file that is discovered on the volume, but not part of the FlashCopy operation. The processing ends.

filename

Where *filename* is a name of a file that contains a list of fully qualified names of files and directories, each name requires a new line. Only files or directories that are not associated with the database but are stored within the file system that is used for backup operations are listed. Any file that is identified by Tivoli Storage FlashCopy Manager that is not part of the database files or is not in the **NEGATIVE_LIST** file, causes processing to end. Any directory that is listed in the **NEGATIVE_LIST** file is processed recursively. For example, all files within the directory, including subdirectories, are processed during a backup or restore request.

Default

None

Advanced mode only

No

POST_FLASH_CMD

This parameter identifies the command script or executable file that is used to resume the application after the snapshot operation. Arguments can be specified and are separated by blanks. This parameter is used when the **APPLICATION_TYPE** parameter is set to **GENERIC**.

This parameter can be set in the profile configuration file, or the parameter can be set from the command-line interface. If set from the command-line interface, the parameter setting overrides the corresponding parameter in the profile configuration file.

Default

There is no default for this required parameter.

Advanced mode only

Yes.

PRE_FLASH_CMD

This parameter identifies the command script or executable file that is used to immediately quiesce the application before the snapshot operation begins. Arguments can be specified and are separated by blanks. This parameter is used when the **APPLICATION_TYPE** parameter is set to **GENERIC**.

This parameter can be set in the profile configuration file, or the parameter can be set from the command-line interface. If set from the command-line interface, the parameter setting overrides the corresponding parameter in the profile configuration file.

Default

There is no default for this required parameter.

Advanced mode only

Yes.

TSM_BACKUP

This parameter specifies whether to create a Tivoli Storage Manager backup from a snapshot. Tivoli Storage FlashCopy Manager must be installed on a backup server. When the **TSM_BACKUP** parameter is set to **YES**, **MANDATE**, or **LATEST**, and after the offload agent runs, a Tivoli Storage Manager backup is created from the snapshot. The following list identifies the possible options:

YES

This option creates a Tivoli Storage Manager backup from a snapshot. If the Tivoli Storage Manager backup operation does not successfully complete, the target set can be reused.

MANDATE

This option creates a Tivoli Storage Manager backup from a snapshot. However, the target set cannot be reused until the Tivoli Storage Manager backup successfully completes.

LATEST

This option removes a backup request to Tivoli Storage Manager from a previous backup. When a new snapshot with **TSM_BACKUP** set to **LATEST**, **YES**, or **MANDATE** is created, Tivoli Storage FlashCopy Manager removes any unsuccessful backup request that were previously created with the **TSM_BACKUP** option set to **LATEST**. This option prevents backup requests to Tivoli Storage Manager from queuing if they are not completed in time.

NO Keeps the snapshot backup but the snapshot is not used as a source for a subsequent tape backup operation.

TSM_ONLY

After the Tivoli Storage Manager backup is completed, during the unmount operation, the backup is automatically marked for deletion. This action occurs regardless of whether the backup is successful or not.

USE_FOR *list of device classes*

To create a Tivoli Storage Manager backup from snapshots that are run with particular device classes, as specified in the profile, combine this attribute with other options. When you list device classes, separate device classes with the space character. There is no limit of the number of device classes.

Default

None

Advanced mode only

No

TIMEOUT_FLASH

This parameter specifies the maximum time, in seconds, that the database agent waits for a response to the management agent call during the *flash* phase. If the database agent does not receive a response within the specified time, an error message is displayed. This parameter allows the maximum time to be specified for a database to be suspended. This parameter also implies the maximum time when JFS2 file systems can be frozen. When the timeout is reached, the file systems thaw, the database is resumed, and the backup operation ends with an error. If the **LVM_FREEZE_THAW** parameter is set to either AUTO or YES, the minimal value for **TIMEOUT_FLASH** is 5 seconds. In other scenarios, the minimal value is 1 second.

Default

The default value is 120 seconds.

Advanced mode only

Yes

TIMEOUT_PHASE

This parameter specifies the maximum time, in seconds, that the database agent waits for a response to the management agent call during a specific operation phase. If the database agent does not receive a response within the specified time, either the backup or restore operation ends and an error message is shown.

Specify one of the following phase values for a FlashCopy backup:

- **PARTITION**
- **PREPARE**
- **FLASH** (this parameter has a separate description)
- **VERIFY**
- **CLOSE**

For example, **TIMEOUT_PREPARE**.

Specify one of the following phase values for a FlashCopy restore:

- **PREPARESTORE**
- **FLASHRESTORE**
- **COMPLETERESTORE**
- **CLOSE**

For example, **TIMEOUT_FLASHRESTORE**.

Default

The default value is 3600 seconds.

Advanced mode only

Yes

ORACLE

The ORACLE section is an extension to the CLIENT and CLONING sections for ORACLE environments. The parameters do not depend on the storage device.

CATALOG_DATABASE_CONNECT_STRING

The recovery catalog connect string. This parameter specifies the connect string of the Recovery catalog database that is used to catalog backup information. This value corresponds to the value defined in the `$ORACLE_HOME/network/admin/tnsnames.ora` file.

Default

There is no default value. This parameter is specified by the user.

Advanced mode only

No.

CATALOG_DATABASE_USERNAME

This parameter sets the user name that has the Oracle system database administrator privileges on the Recovery catalog database.

Default

There is no default value. This parameter is specified by the user.

Advanced mode only

No.

TARGET_DATABASE_PARAMETER_FILE

This parameter specifies the fully resolved path and file name of the Oracle parameter file for the target database. This file is a text-based Oracle parameter file (PFILE) and not an Oracle server file.

Default

`${ORACLE_HOME}/dbs/init${ORACLE_SID}.ora`

Advanced mode only

Yes.

DATABASE_BACKUP_SCRIPT_FILE

Name of the RMAN backup script that contains the Data Protection for Oracle environment variables.

Default

There is no default value. For offload configuration, this parameter is specified.

Advanced mode only

No.

DATABASE_CONTROL_FILE_RESTORE

This parameter specifies whether to restore Oracle control files after snapshot restore processing completes. There are two options:

- YES: A YES option restores Oracle control files and you complete the incomplete recovery up to the point when the control files were backed up.
- NO: A NO option does not restore Oracle control files and you complete the full recovery up to the current image of the Oracle database by using the existing control files in the system.

Default

NO

Advanced mode only

Yes.

ASM_INSTANCE_USER

This parameter specifies the user name of the ASM instance owner. This parameter is used when the target database and the ASM instance are running under different user IDs. The ASM instance has one of the following permissions:

- sysdba
- sysasm
- sysadm

When the parameter is set to AUTO, the database user who runs the process is used.

Default

AUTO

Advanced mode only

No.

ASM_INSTANCE_ID

This parameter sets the SID for the ASM instance.

Default

+ASM

Advanced mode only

No.

ASM_ROLE

This parameter specifies the role that is used when connecting to the ASM instance. There are two options:

- sysdba: This role is specified when using Oracle 10g.
- sysasm: This role is specified when using Oracle 11g.

Default

sysdba

Advanced mode only

No.

CLONING

The CLONING section of the Tivoli Storage FlashCopy Manager profile contains parameters that are used for cloning operations. The parameters are independent of the storage device or application.

The following lists provide the parameters, a description of each parameter, and default values for the CLONING section.

The following parameters apply only to DB2, Oracle, and Oracle in an SAP environment databases:

DEVICE_CLASS

This required parameter identifies the device class to use when you are cloning a database. The following code sample provides an example of how to specify options for this parameter:

```
DEVICE_CLASS device class USE_FOR_CLONING list of clone database names
```

There is an optional *conditions* statement that can be used. The following code sample includes an example of how to use the *conditions* statement:

(partitioned DB2 databases)
[ON_DBPARTITIONNUMS <list of partitions>]

Default

Not applicable.

Advanced mode only

No.

ENHANCED_PARTITIONING

The **ENHANCED_PARTITIONING** parameter is used to control processing when extra file systems that are not database files are specified by the **FLASH_DIR_LIST** parameter in a cloning operation. If VOLUME_MGR is set to ASM, you must remove **ENHANCED_PARTITIONING** from the profile. Tivoli Storage FlashCopy Manager fails, when a file system that is specified by the **FLASH_DIR_LIST** parameter contains symbolic links that point to a file system on a different volume group that is not part of the FlashCopy operation. Set the **ENHANCED_PARTITIONING** parameter to NO to ensure that symbolic links if present are not processed. You must manually add this parameter to the Tivoli Storage FlashCopy Manager profile file. The following list identifies the possible options:

YES

Use this option to ensure that Tivoli Storage FlashCopy Manager processes all symbolic links of files or directories that are specified in the **FLASH_DIR_LIST** profile parameter.

NO Use this option to ensure that Tivoli Storage FlashCopy Manager does not process symbolic links of files or directories that are specified in the **FLASH_DIR_LIST** profile parameter.

Default

YES

Advanced mode only

Yes.

FLASH_DIR_LIST

This parameter is used to include files systems that are not part of the database files in the FlashCopy operation. For example, when you are cloning an SAP Advanced Business Application Programming and Oracle Java™ system, the Java instance is not part of the database files. A clone of the Java instance is created along with the clone of the database. In this scenario, use the **FLASH_DIR_LIST** parameter to include the Java instance directories. If VOLUME_MGR is set to ASM, the **FLASH_DIR_LIST** is ignored.

Specify a fully qualified directory name and file name. For example:

[ON_DBPARTITIONNUM *list of partitions*] *fully qualified file name*

Inside the file, specify one fully qualified file or directory on each line. Tivoli Storage FlashCopy Manager uses the FlashCopy function to FlashCopy the complete volume groups where the specified files or directories are located.

In DB2 Data Partitioning Feature environments that contain multiple partitions, a different file name for each partition can be specified. In this scenario, because different file names are specified for different partitions, specify the **ON_DBPARTITIONNUM** parameter. Each partition number is separated by a space.

The default value is an empty list. This value prevents extra files or directories from participating in the FlashCopy operation.

Default

By default, no file name is specified.

Advanced mode only

Yes.

DATABASE_SCHEMA

When a clone database is created from the production database, the database schema does not change. The clone database uses the database schema that is used by the production database. The **DATABASE_SCHEMA** parameter is used to specify the database schema. For DB2 and Oracle databases, the **DATABASE_SCHEMA** parameter is required. For Oracle in an SAP environment databases, the **DATABASE_SCHEMA** parameter is optional. The default database schema is determined by the following environment variables. These environment variables are set on the production database instance owner environment.

DB2 `db2_db6_schema`

Oracle `db2_ora_schema`

If these environment variables are not set, the default database schema value is *SAPR3*. When the **DATABASE_SCHEMA** parameter is used for a Oracle in an SAP environment database, the specified database schema value overrides all default database schema values. The **DATABASE_SCHEMA** parameter is evaluated when the following conditions exist:

- A processing script is used with the **preproc_clone** or **postproc_clone** command.
- The **refresh_clone** command is entered with the **-X** or **-Y** cloning parameter.
- The **create_clone** command is entered with the **-Y** cloning parameter.

Default

The default value is determined by environment variables.

Advanced mode only

Yes.

NEGATIVE_LIST

The **NEGATIVE_LIST** parameter is used to control processing when files not associated with the database are stored within the same file system that is used for the backup and restore operations. This parameter is required. The following list identifies the options:

NO_CHECK

Use this option to not check for extra files. The operation ignores any additional files that are identified. When you use this option and data is restored, all files that are on the file system or volume group are overwritten.

WARN

Use this option to receive a warning message for each file that is identified on the volume, but not part of the FlashCopy operation. The processing continues. When you use this option and data is restored, all files that are on the file system or volume group are overwritten.

ERROR

Use this option to receive an error message for each file that is discovered on the volume, but not part of the FlashCopy operation. The processing ends.

filename

Use this option to back up and restore files that are not part of the database tablespace files. Using this option includes files in the FlashCopy operations. When you use this option, specify the fully qualified names of

the files and directories. Use one line for each entry. When these files are identified, processing continues. When other files are identified, but not part of the database tablespace files or identified in the **NEGATIVE_LIST** file, processing ends. Any directory that is listed in the **NEGATIVE_LIST** file is processed recursively. For example, all files within the directory, including subdirectories, are processed during a backup or restore request.

Default

There is no default for this required parameter.

Advanced mode only

Yes.

GLOBAL_SYSTEM_IDENTIFIER

Use this parameter to specify a string to be used in the IBM Tivoli Storage Manager for Enterprise Resource Planning Administration Assistant that uniquely identifies a DB2 or Oracle database in the system landscape. This parameter is only valid when the **ADMIN_ASSISTANT** parameter is specified in the ACSD section of the profile.

Default

Depending on the environment, the default value is either *DB2_<DBname>* or *ORA_<DBname>*.

Advanced mode only

Yes.

TIMEOUT_FLASH

This parameter specifies the maximum time, in seconds, that the database agent waits for a response to the management agent call during the *flash* phase. If the database agent does not receive a response within the specified time, an error message is displayed. This parameter allows the maximum time to be specified for a database to be suspended. This parameter also implies the maximum time when JFS2 file systems can be frozen. When the timeout is reached, the file systems thaw, the database is resumed, and the backup operation ends with an error. The minimum value for **TIMEOUT_FLASH** is 5 seconds.

Default

The default value is 120 seconds.

Advanced mode only

Yes

TIMEOUT_<PHASE>

Specify the maximum time (in seconds) that the database agent waits for a response to the management agent call during the *<phase>* phase. If the database agent does not receive a response within the specified time, the backup or restore operation ends and an error message is displayed. The default value is 3600 seconds.

You can specify one of these phase values for a FlashCopy backup. For example: **TIMEOUT_PREPARE**

- **PARTITION**
- **PREPARE**
- **VERIFY**
- **CLOSE**

You can specify one of these phase values for a FlashCopy restore. For example: **TIMEOUT_FLASHRESTORE**

- **PREPARERESTORE**
- **FLASHRESTORE**
- **COMPLETERESTORE**
- **CLOSE**

Advanced mode only

Yes.

The following parameters apply only to Oracle and Oracle in an SAP environment databases:

OVERWRITE_DATABASE_PARAMETER_FILE

This parameter is used only with Oracle and Oracle in an SAP environment databases. This parameter is also included in the OFFLOAD section of the configuration profile. The parameter specifies whether the database configuration file on the backup server is overwritten with the file from the production server. The parameter value in the OFFLOAD section is not applicable to cloning operations and is ignored.

To copy the database configuration file from the production system to the clone system, specify this parameter in the CLONING section of the configuration profile. The Tivoli Storage FlashCopy Manager software requires two database configuration files to be available in the clone instance on the clone system. The default database configuration file name is `${ORACLE_HOME}/dbs/init${ORACLE_SID}.ora`

In the scenario where the production system is `${ORACLE_SID}=P01` and the clone system is `${ORACLE_SID}=C01`, the following database configuration files are required:

```
/oracle/C01/102_64/dbs/initP01.ora
/oracle/C01/102_64/dbs/initC01.ora
```

The `initP01.ora` file is used during the cloning process to recover the database that is used in the FlashCopy operation on the clone system. The `initC01.ora` file is used to rename and start the clone database.

Specify one of the following values:

YES

Copy the database configuration file from the production system to the clone system. The following processes occur:

- The clone database configuration file `initP01.ora` is copied on the clone system. The existing file, `/oracle/C01/102_64/dbs/initP01.ora`, is overwritten.
- The clone database configuration file `/oracle/C01/102_64/dbs/initP01.ora` is copied to `/oracle/C01/102_64/dbs/initC01.ora`. The existing file, `/oracle/C01/102_64/dbs/initC01.ora`, is overwritten. All occurrences of `P01` in this file are renamed to `C01`.

NO Do not copy the database configuration file from the production system to the clone system. This value requires that the database configuration files `/oracle/C01/102_64/dbs/initP01.ora` and `/oracle/C01/102_64/dbs/initC01.ora` are available on the clone system. You must verify that these files are available and are valid.

If the name of the database configuration file on the production database is not the default file name, `${ORACLE_HOME}/dbs/init${ORACLE_SID}.ora`, use the **TARGET_DATABASE_PARAMETER_FILE** parameter, in the CLONING section, to specify

the correct name. In this scenario, the clone database configuration file name is created by replacing the `${ORACLE_SID}` value of the production database with the name of the clone database.

Default

YES

Advanced mode only

Yes.

TARGET_DATABASE_PARAMETER_FILE

This parameter is used only with Oracle and Oracle in an SAP environment databases. This parameter is also included in the ORACLE section of the configuration profile.

The parameter specifies the database configuration file name. The parameter value in the ORACLE section is not applicable to cloning operations and is ignored.

Specify this parameter in the CLONING section of the profile to identify the name of the Oracle parameter file for the production database. Enter the fully resolved path and file name of the Oracle parameter file for the production database. By default, the file name of the Oracle parameter file for the production database is `initSID.ora`. This file must be a text-based Oracle parameter file (PFILE) and not an Oracle server file. The default value is `${ORACLE_HOME}/dbs/init${ORACLE_SID}.ora`. If the production database is configured to use an Oracle server file, this parameter is ignored.

Default

`${ORACLE_HOME}/dbs/init${ORACLE_SID}.ora`

Advanced mode only

Yes.

VOLUME_MGR

The following list identifies the possible options:

ASM

When this option is selected, the option that is set for the **LVM_FREEZE_THAW** parameter is ignored. When this parameter is ignored, there is no file system, and the wizard does not query for data.

LVM

When this option is selected, the ASM-related options in the **DEVICE_CLASS** section is ignored and not queried by the wizard software.

Default

LVM

Advanced mode only

No.

DEVICE_CLASS *device*

The Tivoli Storage FlashCopy Manager profile configuration file can contain one or more **DEVICE_CLASS** sections. The device class section configures Tivoli Storage FlashCopy Manager for use with a particular storage or file system solution. The parameters do not depend on the database or custom application that is protected.

Use care when you rename or delete a **DEVICE_CLASS** section from the profile, as you cannot access backups that were taken with the original **DEVICE_CLASS** section. Therefore, first remove backups and clones that are associated with the **DEVICE_CLASS** before you rename or delete the **DEVICE_CLASS** section.

A *device* refers to supported IBM XIV Storage System , IBM Storwize family, IBM System Storage SAN Volume Controller, IBM System Storage DS8000 series, IBM System Storage N series, and NetApp storage systems. In addition to these storage systems, a device can also be a General Parallel File System (GPFS) file system.

DEVICE_CLASS DS8000 Storage System parameters

The parameters that are defined in the device class section of the Tivoli Storage FlashCopy Manager profile file, configure Tivoli Storage FlashCopy Manager for use with the IBM System Storage DS8000.

BACKUP_HOST_NAME

This parameter specifies the name of the backup host that is used during offloaded tape backups only. The following list identifies the possible options:

PREASSIGNED_VOLUMES

Specify this option when the target volumes are preassigned to a specific backup server.

None

This option is used if you do not have a backup server.

Default

None.

Advanced mode only

No.

CLONE_DATABASE

This parameter is preset by the setup script. If you use the setup script for configuration, it is not necessary to manually update any parameters. The following list identifies the possible options:

YES Use the device class for cloning. When the parameter is set to YES, the device class is unavailable for non-cloning backup or restore operations. The device class is ignored during backup expiration and reconciliation processing.

NO Do not use the device class for cloning. When the parameter is set to NO, any cloning request fails with an error message and return code 2.

Default

This parameter is not explicitly set. The setup script sets the value, depending on if the device class is specified in the **CLIENT** or **CLONING** section.

Advanced mode only

No.

COPYSERVICES_HARDWARE_TYPE

This parameter is required. Only one device can be specified.

DS8000

Specify the DS8000 option, when the database is stored on one of the following storage systems:

- IBM DS8100
- IBM DS8300
- IBM DS8700
- IBM DS8800
- IBM DS8870

Default

None.

Advanced mode only

No.

COPYSERVICES_USERNAME

This parameter identifies the user name, use the *cim user* of the CIM Agent for DS Open API. The CIM Agent for DS Open API manages the primary and secondary copy services servers of the DS8000 cluster.

Default

superuser

Advanced mode only

No.

RECON_INTERVAL

This parameter specifies the interval, in hours, between two subsequent reconciliation operations. The options are whole numbers between 0 and 24 inclusive.

Default

12

Advanced mode only

Yes.

STORAGE_SYSTEM_ID

Specify the storage system ID of the cluster where the storage system is used in the following mirrored environments:

- AIX Logical Volume Manager mirrored environment.
- Oracle ASM mirrored environment where the failure groups are distributed across multiple storage systems.

This parameter must not be specified in non-mirrored environments.

Note: For information about ASM failure group environments, see “LVM mirroring and ASM failure group environments” on page 72.

Default

None.

Advanced mode only

Yes.

COPYSERVICES_COMMPROTOCOL

This parameter identifies the protocol to be used for communication with the CIM Agent. The options are HTTP, for communication in a non-secure mode, and HTTPS, for communication in a secure mode.

Default

HTTPS

Advanced mode only

Yes.

COPYSERVICES_CERTIFICATEFILE

When **COPYSERVICES_COMMPROTOCOL** is set to HTTPS, there are two options:

certificate_filename

Name of a certificate file that is created for secure communication between the CIM Client and the CIM Agent.

NO_CERTIFICATE

Select for null trust provider mode.

By default, the CIM Agent for DS8000, which is preinstalled on the HMC, requires communication in secure mode. For this scenario, clients such as Tivoli Storage FlashCopy Manager must connect by using HTTPS instead of HTTP. This connection requires that the CIM Client obtain the public key that is used for encryption from the *truststore* certificate in the CIM Agent. After the client obtains the public key, the CIM Client is authenticated by using the user name and password.

To enable the HTTPS protocol, the Tivoli Storage FlashCopy Manager profile parameter **COPYSERVICES_COMMPROTOCOL** must specify HTTPS. For this scenario, the **COPYSERVICES_CERTIFICATEFILE** parameter can define a certificate file name, and Tivoli Storage FlashCopy Manager exports the certificate by using this file.

The CIM Agent also provides another communication mode that is known as *null trust provider*. In this scenario, 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 file name. To enable this mode, the value of **COPYSERVICES_CERTIFICATEFILE** must be **NO_CERTIFICATE**. This mode is used only if the production and backup systems, and the storage system, are protected by a firewall. If **NO_CERTIFICATE** is used, the `cimom.properties` parameter **DigestAuthentication** must be set to false.

Default

NO_CERTIFICATE

Advanced mode only

Yes.

COPYSERVICES_PRIMARY_SERVERNAME

This parameter identifies the server name or address that defines the TCP/IP address of the host that is running the CIM Agent for DS Open API. This host manages the primary and secondary copy services servers of the DS8000 cluster.

Default

localhost

Advanced mode only

No.

COPYSERVICES_SECONDARY_SERVERNAME

This parameter identifies the name of the backup Copy Services server that is located within a snapshot devices cluster. Specify either the IP address or the server DNS name. This parameter can be used only in environments with DS8000 in combination with the proxy CIM Agent.

Default

None

Advanced mode only

Yes.

COPYSERVICES_SERVERPORT

This parameter identifies the server port number of the host that is running the CIM Agent for DS Open API.

Default

The default port number depends on the settings of

COPYSERVICES_HARDWARE_TYPE and **COPYSERVICES_COMMPROTOCOL**:

COPYSERVICES_HARDWARE_TYPE	COPYSERVICES_COMMPROTOCOL	Default Port
DS8000	HTTPS	6989
	HTTP	6988

Advanced mode only

Yes.

COPYSERVICES_TIMEOUT

This parameter identifies the maximum length of time, in minutes, that the CIM Client waits for a response to a call sent to the CIMOM (CIM Agent). If the CIM Client does not receive a response within this time, an error message is sent.

Default

6

Advanced mode only

Yes.

FLASHCOPY_TYPE

This parameter specifies whether the storage solution does a bit-level copy of data from one logical volume to another. This parameter applies to any FlashCopy storage system. The following options are available:

COPY Directs the storage system to run a bit-level copy of the data from one physical volume to another. Specify this value when the following conditions are true:

- A fast snapshot restore of a backed-up database is required.
- A complete copy of the database data on the target volume is required.

NOCOPY Directs the storage system to run a bit-level copy of a track if the data is modified after the initial FlashCopy request. This technique is typically referred as copy-on-write. This option applies only to FlashCopy devices. Specify this value when the following conditions are true:

- A complete copy of the source volumes that contain the database files is not required on the target volumes.
- Backup time constraints are a concern.

INCR This option is similar to the COPY option but the INCR option copies only those tracks that were modified since the previous incremental FlashCopy was created. This option applies only to FlashCopy devices. Specify this value when the following conditions are true:

- Tivoli Storage Manager backups are taken from disk copies. This type of backup creates less burden on the storage system than for the COPY option.

- A snapshot restore operation of the backed up database is to be completed.
- More frequent backups for the database are scheduled.

There must be only one target set specified in the target volumes file (.fct) for incremental snapshots. CIM errors might occur when more than one target set is specified. A successful backup of the database to the Tivoli Storage Manager server is possible even if the parameter is set to NOCOPY.

Default

COPY

Advanced mode only

No.

RESTORE_FORCE

This parameter specifies whether to force a restore. During a rerun of a snapshot restore, the message FMM0200E can be generated. This problem occurs if the background copy process of the previous snapshot restore is still running and the **RESTORE_FORCE** parameter is set to NO. There are two ways to resolve the issue that is identified by the message:

- Wait until the background copy process ends.
- Set the **RESTORE_FORCE** parameter to YES in the profile configuration file and try the snapshot restore again. This option withdraws all existing source and target relationships, and creates new source and target relationships. A full copy is completed. If you want to set **RESTORE_FORCE** to YES for a specific restore, you can create a temporary profile configuration file.

Default

NO

Advanced mode only

Yes.

TARGET_SETS

This parameter specifies the target volumes to be used in the FlashCopy operation. The following list identifies the possible options:

VOLUMES_FILE

The name of the target volumes file (.fct).

Default

None.

Advanced mode only

No.

VOLUMES_FILE

This parameter specifies the name of the target volumes file (.fct).

Default

None.

Advanced mode only

No.

DEVICE_CLASS Storwize family and SVC Storage System parameters

The parameters that are defined in the device class section of the Tivoli Storage FlashCopy Manager profile file, configure Tivoli Storage FlashCopy Manager for use with the IBM Storwize family or IBM System Storage SAN Volume Controller storage systems.

CLONE_DATABASE

This parameter is preset by the setup script. If you use the setup script for configuration, it is not necessary to manually update any parameters. The following list identifies the possible options:

YES Use the device class for cloning. When the parameter is set to YES, the device class is unavailable for non-cloning backup or restore operations. The device class is ignored during backup expiration and reconciliation processing.

NO Do not use the device class for cloning. When the parameter is set to NO, any cloning request fails with an error message and return code 2.

Default

This parameter is not explicitly set. The setup script sets the value, depending on if the device class is specified in the CLIENT or CLONING section.

Advanced mode only

No.

COPYSERVICES_HARDWARE_TYPE

This parameter is required. Only one device can be specified.

SVC

Specify the SVC option, when the database is stored on either the SAN Volume Controller or the Storwize family storage system.

Default

Not available.

Advanced mode only

No.

COPYSERVICES_USERNAME

This parameter identifies the user name. Use the *SVC user* name that you use to log on to the SAN Volume Controller master console or cluster. For Storwize family, use the *Storwize V7000 user* name that you use to log on to the Storwize family.

Default

superuser

Advanced mode only

No.

RECON_INTERVAL

This parameter specifies the interval, in hours, between two subsequent reconciliation operations. The options are whole numbers between 0 and 24 inclusive.

Default

12

Advanced mode only

Yes.

STORAGE_SYSTEM_ID

Specify the storage system ID of the cluster where the storage system is used in the following mirrored environments:

- AIX Logical Volume Manager mirrored environment.
- Oracle ASM mirrored environment where the failure groups are distributed across multiple storage systems.

This parameter must not be specified in non-mirrored environments.

The **STORAGE_SYSTEM_ID** parameter refers to the storage system Cluster ID.

Note: For information about ASM failure group environments, see “LVM mirroring and ASM failure group environments” on page 72.

Default

None.

Advanced mode only

Yes.

COPYSERVICES_COMMPROTOCOL

This parameter identifies the protocol to be used for communication with the CIM Agent. The options are HTTP, for communication in a non-secure mode, and HTTPS, for communication in a secure mode.

Default

HTTPS

Advanced mode only

Yes

COPYSERVICES_CERTIFICATEFILE

When **COPYSERVICES_COMMPROTOCOL** is set to HTTPS, there are two options:

certificate_filename

Name of a certificate file that is created for secure communication between the CIM Client and the CIM Agent.

NO_CERTIFICATE

Select for null trust provider mode.

By default, the CIM Agent for DS8000, which is preinstalled on the HMC, requires communication in secure mode. For this scenario, clients such as Tivoli Storage FlashCopy Manager must connect by using HTTPS instead of HTTP. This connection requires that the CIM Client obtain the public key that is used for encryption from the *truststore* certificate in the CIM Agent. After the client obtains the public key, the CIM Client is authenticated by using the user name and password.

To enable the HTTPS protocol, the Tivoli Storage FlashCopy Manager profile parameter **COPYSERVICES_COMMPROTOCOL** must specify HTTPS. For this scenario, the **COPYSERVICES_CERTIFICATEFILE** parameter can define a certificate file name, and Tivoli Storage FlashCopy Manager exports the certificate by using this file.

The CIM Agent also provides another communication mode that is known as *null trust provider*. In this scenario, 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 file name. To enable this mode, the value of **COPYSERVICES_CERTIFICATEFILE** must be **NO_CERTIFICATE**. This mode is used only if the production and backup systems,

and the storage system, are protected by a firewall. If `NO_CERTIFICATE` is used, the `cimom.properties` parameter **DigestAuthentication** must be set to false.

Default

`NO_CERTIFICATE`

Advanced mode only

Yes

COPYSERVICES_PRIMARY_SERVERNAME

This parameter identifies the server name or address that defines the TCP/IP address of the host that is running the CIM Agent for DS Open API. This host manages the SAN Volume Controller master console and the embedded CIM Agent in the Storwize family storage system. For SAN Volume Controller, the **COPYSERVICES_PRIMARY_SERVERNAME** parameter, if specified, must point directly to the SAN Volume Controller cluster with the embedded CIM server. For Storwize family, the **COPYSERVICES_PRIMARY_SERVERNAME** parameter must point to the Storwize family cluster.

Default

`localhost`

Advanced mode only

No

COPYSERVICES_SERVERPORT

This parameter identifies the server port number on the CIM Agent for DS Open API. This information is used to manage the primary and secondary Copy Services servers of the SAN Volume Controller master console or the embedded CIM Agent on the Storwize family storage system.

Default

The default port number depends on the settings of **COPYSERVICES_HARDWARE_TYPE** and **COPYSERVICES_COMMPROTOCOL**:

<code>COPYSERVICES_HARDWARE_TYPE</code>	<code>COPYSERVICES_COMMPROTOCOL</code>	Default Port
SVC	HTTPS	5989
	HTTP	5988

Advanced mode only

Yes

COPYSERVICES_TIMEOUT

This parameter identifies the maximum length of time, in minutes, that the CIM Client waits for a response to a call put to the CIMOM (CIM Agent). If the CIM Client does not receive a response within this time, an error message is displayed.

Default

6

Advanced mode only

Yes

FLASHCOPY_TYPE

This parameter specifies whether the storage solution does a bit-level copy of data from one logical volume to another. This parameter applies to any FlashCopy storage system. The following options are available:

- COPY** Directs the storage system to run a bit-level copy of the data from one physical volume to another. Specify this value when the following conditions are true:
- A fast snapshot restore of a backed-up database is required.

- A complete copy of the database data on the target volume is required.

NOCOPY Directs the storage system to run a bit-level copy of a track if the data is modified after the initial FlashCopy request. This technique is typically referred as copy-on-write. This option applies only to FlashCopy devices. Specify this value when the following conditions are true:

- A complete copy of the source volumes that contain the database files is not required on the target volumes.
- Backup time constraints are a concern.

INCR This option is similar to the COPY option but the INCR option copies only those tracks that were modified since the previous incremental FlashCopy was created. This option applies only to FlashCopy devices. Specify this value when the following conditions are true:

- Tivoli Storage Manager backups are taken from disk copies. This type of backup creates less burden on the storage system than for the COPY option.
- A snapshot restore operation of the backed up database is to be completed.
- More frequent backups for the database are scheduled.

The **SVC_COPY_RATE** parameter is forced to 0 when the **FLASHCOPY_TYPE** parameter is specified as NOCOPY or INCR.

Default

COPY

Advanced mode only

No

RESTORE_FORCE

This parameter specifies whether to force a restore. During a rerun of a snapshot restore, the message FMM0200E can be generated. This problem occurs if the background copy process of the previous snapshot restore is still running and the **RESTORE_FORCE** parameter is set to NO. There are two ways to resolve the issue that is identified by the message:

- Wait until the background copy process ends.
- Set the **RESTORE_FORCE** parameter to YES in the profile configuration file and try the snapshot restore again. This option withdraws all existing source and target relationships, and creates new source and target relationships. A full copy is completed. If you want to set **RESTORE_FORCE** to YES for a specific restore, you can create a temporary profile configuration file.

Default

NO

Advanced mode only

Yes.

TARGET_SETS

This parameter specifies the target volumes to be used in the FlashCopy operation. The following list identifies the possible options:

VOLUMES_FILE

The name of the target volumes file (.fct).

list_of target_set_names

A list of target set names. For example: TARGET_SETS 1 2 3

To define the naming convention for the target volumes, specify the **TARGET_NAMING** parameter. For example: TARGET_NAMING *string_with_wildcards_%SOURCE_and_%TARGETSET*

This parameter and option define the naming convention for target volumes. When a backup volume is required, Tivoli Storage FlashCopy Manager determines the name of the target set for the operation and the name of the source volume to be backed up. The name of the target volume that stores the backup is the name that is specified after the following strings are replaced with the respective values in the operation: *%SOURCE_and_%TARGETSET*.

Default

None.

Advanced mode only

No.

VOLUMES_FILE

This parameter specifies the name of the target volumes file (.fct).

Default

None.

Advanced mode only

No.

ALLOW_NOCOPY_FLASHCOPY

Use this parameter with the **CLONE_DATABASE** parameter. The following list identifies the possible options:

YES Create a Tivoli Storage FlashCopy Manager clone on space-efficient targets. For this device class, use space-efficient targets and set **FLASHCOPY_TYPE** to NOCOPY. FlashCopy backups cannot be stored on the same source volumes.

NO Do not create a Tivoli Storage FlashCopy Manager clone on space-efficient targets. If both backup and cloning must be completed on the same source volumes, cloning is completed to full targets and the **ALLOW_NOCOPY_FLASHCOPY** parameter is set to NO.

Default

NO

Advanced mode only

Yes.

SVC_CLEAN_RATE

This parameter specifies the cleaning rate for the FlashCopy mapping. A value from 1 to 100 can be entered.

Default

None.

Advanced mode only

Yes.

SVC_COPY_RATE

This parameter specifies the priority that the SAN Volume Controller or Storwize family gives to the FlashCopy background process for the current backup or restore. A value from 0 to 100 can be entered.

A value of 100 indicates the highest priority, but places the greatest burden on the responsiveness of the storage system. A value of 0 indicates the lowest priority, but suppresses the background copy process and forces the **FLASHCOPY_TYPE** parameter to have the NOCOPY option.

Default

50

Advanced mode only

No.

SVC_GRAIN_SIZE

This parameter specifies the grain size, in KB, for FlashCopy mapping for space-efficient virtual disks on SAN Volume Controller or Storwize family. The grain size of the space-efficient virtual disk must match the grain size of the FlashCopy. The options for this parameter are 32, 64, 128, and 256.

After the parameter is set, the value cannot be changed until the backup is deleted with the option -F to remove the mappings.

Default

256

Advanced mode only

Yes.

DEVICE_CLASS XIV system Storage System parameters

The parameters that are defined in the device class section of the Tivoli Storage FlashCopy Manager profile file, configure Tivoli Storage FlashCopy Manager for use with the IBM XIV Storage System.

BACKUP_HOST_NAME

This parameter specifies the name of the backup host that is used during offloaded tape backups only. The following list identifies the possible options:

backup_server_hostname

Enter the host name or cluster name of the backup server as configured on the XIV system Storage System.

None

This option is used if you do not have a backup server.

Default

None

Advanced mode only

No.

CLONE_DATABASE

This parameter is preset by the setup script. If you use the setup script for configuration, it is not necessary to manually update any parameters. The following list identifies the possible options:

YES

Use the device class for cloning. When the parameter is set to YES, the device class is unavailable for non-cloning backup or restore operations. The device class is ignored during backup expiration and reconciliation processing.

NO Do not use the device class for cloning. When the parameter is set to NO, any cloning request fails with an error message and return code 2.

The following example shows the **CLONE_DATABASE** parameter that is specified in the **DEVICE_CLASS** *device* section of the profile:

```
>>> DEVICE_CLASS STANDARD
CLONE_DATABASE YES
COPYSERVICES_HARDWARE_TYPE XIV
# STORAGE_SYSTEM_ID
PATH_TO_XCLI /home/xivtest/XCLI
COPYSERVICES_SERVERNAME nextra
COPYSERVICES_USERNAME admin
# RECON_INTERVAL 12
# USE_WRITABLE_SNAPSHOTS AUTO
BACKUP_HOST_NAME acsback5
<<<
```

Default

This parameter is not explicitly set. The setup script sets the value, depending on if the device class is specified in the **CLIENT** or **CLONING** section.

Advanced mode only

No.

COPYSERVICES_HARDWARE_TYPE

This parameter is required. Only one device can be specified.

XIV

Specify the XIV option, when the database is stored on the XIV system Storage System.

On the console, any notifications that refer to IBM XIV Storage System operations and **COPYSERVICES_HARDWARE_TYPE** are displayed as **COPYSERVICES_HARDWARE_TYPE=GENERIC**. Similarly, when you view the log or trace files in the **ACS_DIR/logs** directory, any references that are related to the **COPYSERVICES_HARDWARE_TYPE** for the XIV system Storage System are displayed as **COPYSERVICES_HARDWARE_TYPE=GENERIC**.

Default

Not available.

Advanced mode only

No.

COPYSERVICES_SERVERNAME

This parameter identifies the TCP/IP host name of the storage system where the data to protect is located.

Default

None

Advanced mode only

No.

COPYSERVICES_USERNAME

This parameter identifies the user name. Use the *XIV user* name that you use log on to the XIV system Storage System.

Default

superuser

Advanced mode only

No.

RECON_INTERVAL

This parameter specifies the interval, in hours, between two subsequent reconciliation operations. The options are whole numbers between 0 and 24 inclusive.

Default

12

Advanced mode only

Yes.

STORAGE_SYSTEM_ID

This parameter specifies the storage system ID of the cluster where the storage system is used in the following mirrored environments:

- AIX Logical Volume Manager mirrored environment.
- Oracle ASM mirrored environment where the failure groups are distributed across multiple storage systems.

This parameter must not be specified in non-mirrored environments.

The **STORAGE_SYSTEM_ID** parameter refers to the four-digit hexadecimal XIV system ID.

Note: For information about ASM failure group environments, see “LVM mirroring and ASM failure group environments” on page 72.

Default

None.

Advanced mode only

Yes.

PATH_TO_XCLI

This parameter specifies the path where the XIV command-line interface, XCLI, is installed. There is no default value. This parameter is only valid when **COPYSERVICES_HARDWARE_TYPE** specifies XIV.

Default

None.

Advanced mode only

No.

USE_WRITABLE_SNAPSHOTS

This parameter determines whether writable snapshots are used. Writable snapshots are required in LVM mirrored environments. The following list identifies the options:

YES Writable snapshots are used.

NO Writable snapshots are not used.

AUTO Based on the environment, the value is automatically selected.

Default

AUTO

Advanced mode only

Yes

DEVICE_CLASS System Storage N series and NetApp parameters

The parameters that are defined in the device class section of the Tivoli Storage FlashCopy Manager profile file, configure Tivoli Storage FlashCopy Manager for use with the IBM System Storage N series and NetApp storage systems.

BACKUP_HOST_NAME

This parameter is dependent on if the N series or NetApp storage systems are in a storage area network (SAN) or network-attached storage (NAS) based infrastructure. The following list identifies the possible options:

backup_server_hostname

For SAN-attached storage, enter the name of the initiator group for the SAN adapter of the backup host as configured on the N series or NetApp storage system. This parameter is used to map the LUNs to the backup host.

For NAS-attached storage, specify the IP address of the backup server.

None

This option is used if you do not have a backup server.

Default

None

Advanced mode only

No

CLONE_DATABASE

This parameter is preset by the setup script. If you use the setup script for configuration, it is not necessary to manually update any parameters. The following list identifies the possible options:

YES Use the device class for cloning. When the parameter is set to YES, the device class is unavailable for non-cloning backup or restore operations. The device class is ignored during backup expiration and reconciliation processing.

NO Do not use the device class for cloning. When the parameter is set to NO, any cloning request fails with an error message and return code 2.

Default

This parameter is not explicitly set. The setup script sets the value, depending on if the device class is specified in the CLIENT or CLONING section.

Advanced mode only

No

COPYSERVICES_HARDWARE_TYPE

This parameter is required. Only one device can be specified. The following list identifies the possible options:

NAS_NSERIES

Specify the NAS_NSERIES option, when the database is stored on NAS-attached storage systems.

SAN_NSERIES

Specify the SAN_NSERIES option, when the database is stored on SAN-attached storage systems.

Default

Not available.

Advanced mode only

No

COPYSERVICES_SERVERNAME

This parameter identifies the TCP/IP host name of the storage system where the data to protect is located.

Default

None

Advanced mode only

No

COPYSERVICES_USERNAME

This parameter identifies the user name to log on to the N series or NetApp storage system.

Default

superuser

Advanced mode only

No

RECON_INTERVAL

This parameter specifies the interval, in hours, between two subsequent reconciliation operations. The options are whole numbers between 0 and 24 inclusive.

Default

12

Advanced mode only

Yes

STORAGE_SYSTEM_ID

This parameter specifies the storage system ID of the cluster where the storage system is used in the following mirrored environments:

- AIX Logical Volume Manager mirrored environment.
- Oracle ASM mirrored environment where the failure groups are distributed across multiple storage systems.

This parameter must not be specified in non-mirrored environments.

The storage system ID as displayed for example in the system status pane of the storage interface.

Note: For information about ASM failure group environments, see “LVM mirroring and ASM failure group environments” on page 72.

Default

None.

Advanced mode only

Yes.

|

DEVICE_CLASS GPFS parameters

The parameters that are defined in the device class section of the Tivoli Storage FlashCopy Manager profile file, configure Tivoli Storage FlashCopy Manager for use with a General Parallel File System (GPFS). In addition to device classes for storage systems, a device can also be a General Parallel File System.

COPYSERVICES_HARDWARE_TYPE

This parameter is required.

GPFS

Specify the GPFS option, when the database is in a DB2 pureScale environment and on a GPFS file system.

Default

Not available.

Advanced mode only

No

NUMBER_GPFS_CONCURRENT_TASKS

This parameter specifies the number of concurrent threads to use during a GPFS operation, for example during a tape backup operation. Use this parameter only when the **COPYSERVICES_HARDWARE_TYPE** has GPFS as the assigned device value.

The following example shows a typical GPFS device class section from a profile file where the number of GPFS concurrent tasks is set to 10.

```
>>> DEVICE_CLASS STANDARD
COPY_SERVICES_HARDWARE_TYPE GPFS
NUMBER_OF_GPFS_CONCURRENT_TASKS 10
```

```
<<<
```

Default

3

Advanced mode only

No

Updating DEVICE_CLASS device for mirroring

To use the mirroring technologies, a **DEVICE_CLASS** section specific to the storage solution used for mirroring needs to be added to the profile configuration file. There is one exception to this statement: If remote backups are run, the existing **DEVICE_CLASS** section for the device is sufficient. No additional **DEVICE_CLASS** section is needed.

About this task

When creating a **DEVICE_CLASS** section for the storage solution used for mirroring, the section includes the same parameters as the device class for the local site, specific vales for the remote site, and the parameters that are required to connect and send requests to the remote cluster. The parameters required to connect and send requests to the remote cluster are identified in the following list:

COPYSERVICES_REMOTE

The option set for this parameter determines if the backup is taken at the remote site. The options are YES and NO. The default option is set to NO.

COPYSERVICES_REMOTE_SERVERNAME

This parameter specifies the IP address or hostname for the secondary cluster. If the **COPYSERVICES_REMOTE** parameter is set to YES, the parameter is required.

If the **COPYSERVICES_REMOTE** parameter is set to NO, the **COPYSERVICES_REMOTE_SERVERNAME** parameter cannot be used. If the parameter is used, an error occurs.

COPYSERVICES_REMOTE_USERNAME

This parameter specifies the user name used to connect to the secondary cluster. The default option is superuser. If the **COPYSERVICES_REMOTE** parameter is set to NO, the **COPYSERVICES_REMOTE_SERVERNAME** parameter cannot be used. If the parameter is used, an error occurs.

TAKEOVER_HOST_NAME

This parameter is required when restoring a remote mirroring backup after a takeover procedure on the remote side. The value for this parameter is the host name of the takeover host and is only used in combination with the secondary cluster defined by the **COPYSERVICES_REMOTE_SERVERNAME** parameter. The value specified for this parameter needs to match the value defined in the storage system. If the values do not match, an error occurs.

The following **DEVICE_CLASS** parameters need to be common to both clusters:

- **COPYSERVICES_COMMPROTOCOL**
- **COPYSERVICES_CERTIFICATEFILE**
- **COPYSERVICES_SERVERPORT**

OFFLOAD

The OFFLOAD section of the configuration contains information that is related to Tivoli Storage Manager backups from a snapshot.

File names that are specified in this section typically point to files that are on a backup server. The offload section is optional and can exist for DB2, DB2 in an SAP environment, Oracle, Oracle in an SAP environment, and custom applications. The parameters do not depend on the storage device.

The following list provides the parameters, a description of each parameter, and default values applicable in all of the following environments:

- DB2
- DB2 in an SAP environment
- Oracle
- Oracle in an SAP environment
- Custom applications

BACKUP_METHOD

This parameter is preset by the setup script (the profile configuration wizard). The setup script value depends on the environment where the setup script is running.

- DB2 and DB2 in an SAP environment - DB2
- DB2 standby server - TSM_CLIENT
- Oracle - ORACLE
- Oracle in an SAP environment - BACKINT
- Custom application - TSM_CLIENT. When this option is set for custom applications, in the CLIENT section, the **APPLICATION_TYPE** is set to GENERIC. If the parameter settings are not correct, an error might occur.

Default

Preset by the setup script, according to the environment.

Advanced mode only

Yes.

Offload DB2 and DB2 in an SAP environment parameters

The following list provides the parameters, a description of each parameter, and default values applicable in only DB2 and DB2 in an SAP environment:

OPTIONS

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.

To be able to set up individual partitions in a DB2 environment in a different manner, the placeholder string `%DB2NODE` can be embedded in the options string. At run time, the string is 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
```

The following two files are referred to:

```
/db2/T01/tdpr3/vendor_0.env  
/db2/T01/tdpr3/vendor_1.env
```

The first file is used for partition `0`, the second for partition `1`. Specifying this parameter overrides the value that is specified by the **VENDOROPT** database configuration parameter.

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 that is located on the backup server. The string is passed directly to the backup utility.

Default

The default value is an empty string.

Advanced mode only

No.

DB2_OPTIONS

This parameter allows certain extra DB2 backup command options to be set during an offload backup to Tivoli Storage Manager. The options string that is specified by the **DB2_OPTIONS** parameter is passed directly to the DB2 backup command.

If multiple options must be specified in `DB2_OPTIONS` parameter string, you must enclose the complete options string in single or double quotation marks. The string (without the quotation marks) is passed to the DB2 backup command. The following example shows you how to define more than one option:

```
DB2_OPTIONS "DEDUP_DEVICE UTIL_IMPACT_PRIORITY 50"
```

<options string>

Specifies options to be used for this Tivoli Storage Manager backup operation. The string is passed directly to the DB2 backup command.

Default

The default value is an empty string.

Advanced mode only

Yes.

DBPARTITIONNUM

This parameter can be overridden by the tsm4acs command option -N.

ALL

All partitions

partition list

Comma-separated list of partition numbers

Default

ALL

Advanced mode only

Yes.

PARALLELISM

The following list identifies the options for this parameter:

n Number of table spaces that can be read in parallel by the backup utility.

AUTO

DB2 calculates an optimum value.

Default

AUTO

Advanced mode only

Yes.

NUM_SESSIONS

The following list identifies the options for this parameter:

n Number of I/O sessions to be created between DB2 and Tivoli Storage Manager.

Default

1

Advanced mode only

No.

NUM_BUFFERS

The following list identifies the options for this parameter:

n The number of buffers to be used by DB2

AUTO

The DB2 software calculates the optimum value for this parameter.

Default

AUTO

Advanced mode only

Yes.

BUFFER_SIZE

The following list identifies the options for this parameter:

- n** The value of this parameter specifies the size, in 4 KB pages, of the buffer that is used by the DB2 software when the backup image is built. The minimum value is 8 pages.

AUTO

If the backup is automatically started, the DB2 software calculates the optimum value.

Default

AUTO

Advanced mode only

Yes.

PARALLEL_BACKUP

The following list identifies the options for this parameter:

YES

The Tivoli Storage Manager backup of all participating partitions is run in parallel.

- NO** The Tivoli Storage Manager backups of all participating partitions are sequentially run.

Default

No

Advanced mode only

Yes.

DATABASE_MEMORY

For Tivoli Storage FlashCopy Manager software to correctly protect DB2 database data, the DB2 database must be started on the backup system during the offload of this database to Tivoli Storage Manager. To start this database on the backup system, the DB2 software needs the database memory size that is specified on the DB2 database on the production system.

This parameter specifies the size of DB2 database shared memory on the backup system. By specifying an empty string or 0, the DB2 memory size that is specified in the DB2 database configuration on the production system is used.

Default

0

Advanced mode only

Yes.

NUMBER_BACKUPS_IN_PARALLEL

In DB2 DPF environments with more than one DB2 partition start the offloaded Tivoli Storage Manager backup in parallel for multiple DB2 partitions. When running in large DB2 DPF environments with more than one backup system, the performance of the overall offloaded Tivoli Storage Manager backup can be increased if the Tivoli Storage Manager backups of each DB2 partition can be started in parallel on each of the backup systems.

This profile parameter specifies the degree of parallelism to use during the offloaded backup. If you specify a positive integer value for this parameter, the specified number of Tivoli Storage Manager backups start in parallel on each of the backup systems. For example, if a value of 1 is specified, one backup is started in parallel on each backup system. If the parameter value is 0, no parallelism is used. If you want to use a value greater than 0 for

NUMBER_BACKUPS_IN_PARALLEL, set the **PARALLEL_BACKUP** value to NO.

Default

0

Advanced mode only

Yes.

VENDOR_LIB**DEFAULT**

Use library or agent corresponding to database environment

DB2_TSM_AGENT

Use the DB2 Tivoli Storage Manager agent.

TSM4ERP

Use IBM Tivoli Storage Manager for Enterprise Resource Planning.

library

Use the fully qualified name for the custom library.

Default

DEFAULT

Advanced mode only

Yes.

Offload Oracle parameters

The following list provides the parameters, a description of each parameter, and default values applicable in only Oracle environments:

OVERWRITE_DATABASE_PARAMETER_FILE

The following list identifies the options for this parameter:

YES

To ensure that the database configuration files are identical, replace the database configuration file on the backup system with the version defined on the production system.

NO Do not copy the production system database configuration file to the backup system.

Default

YES

Advanced mode only

Yes.

DATABASE_BACKUP_INCREMENTAL_LEVEL

This parameter specifies the level of backup. Any numerical value can be entered. The following conditions apply:

- To complete a full backup, use option 0. A full backup must be completed before an incremental backup can be performed.
- To complete an incremental backup, enter a numerical value greater than 0. 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.

Default

0

Advanced mode only

No.

ASM_INSTANCE_USER

This parameter is used for the backup server. If this parameter is not specified for the OFFLOAD section, the value of this parameter, as specified in the ORACLE section, is used for the backup server.

user name

Specify the user name of the ASM instance owner. Use this parameter when the target database and the ASM instance are running under different user IDs. The ASM instance has one of the following permissions: sysdba, sysasm, or sysadm.

AUTO

When this parameter is set to AUTO, the database user who is running the process is used.

Default

There is no default value.

Advanced mode only

Yes.

ASM_INSTANCE_ID

This parameter specifies the SID of the ASM instance. This parameter is used for the backup server. If this parameter is not specified for the OFFLOAD section, the value of this parameter, as specified in the ORACLE section, is used for the backup server.

You can have a SID for the ASM instance other than +ASM. In this scenario, this profile parameter specifies the ASM instance SID.

Default

0

Advanced mode only

Yes.

ASM_ROLE

Specify the role that is used when connecting to the ASM instance. When you use Oracle 11g, specify the sysasm role.

Default

0

Advanced mode only

Yes.

Offload Oracle in an SAP environment parameters

The following list provides the parameters, a description of each parameter, and default values applicable in only Oracle in an SAP environment environments:

PROFILE

This required parameter is used to specify the name of the external SAP Backint profile (init<SID>.utl).

Default

There is no default value.

Advanced mode only

Yes.

Offload custom application parameters

The following list provides the parameters, a description of each parameter, and default values applicable in custom application environments and DB2 standby servers:

MODE

This parameter determines which of the following Tivoli Storage Manager Backup Archive client backup functions to use when a Tivoli Storage Manager offloaded backup is created:

ARCHIVE

Creates an archive backup of all files and directories that are specified in the backup request. Directories are processed recursively.

The ARCHIVE mode is similar to the FULL mode, except that the archive management class is used instead of a backup management class. One of the advantages of the archive management class is that Tivoli Storage FlashCopy Manager does not need to resend all data after a failure during an archive operation. The remainder of the data is sent after the failure occurs.

FULL

Creates a full backup of all files and directories that are specified in the backup request. Directories are processed recursively.

DIFF

Creates a differential backup of all files and directories that are specified in the backup request. Directories are processed recursively. This operation backs up changes since the most recent full backup.

USE_FOR *device class*

Allows the backup mode to be changed based on the device class that is used to create the snapshot. Use this option to define rules that create a weekly full backup and daily incremental backups.

Tip: You can use the USE_FOR option to define multiple **MODE** statements within the OFFLOAD section.

Default

FULL

Advanced mode only

No.

ASNODENAME *nodename*

This required parameter identifies the name of the node where data is stored during a Tivoli Storage Manager offloaded backup.

ASNODENAME is the same option that can be set in the dsm.sys file.

Default

None. This parameter is required.

Advanced mode only

No.

VIRTUALFSNAME *name*

This parameter identifies the virtual file space name of a backup group. The parameter is available when the **MODE** parameter specifies a value of FULL or DIFF. VIRTUALFSNAME is optional.

Default

fcm

Advanced mode only

Yes.

DSM_DIR

This optional parameter identifies the path used for the *DSM_DIR* environment variable. For UNIX and Linux operating systems, specify the path where the executable file *dsmc*, the resource files, and the *dsm.sys* file reside.

Default

The default value is an empty string.

Advanced mode only

Yes.

DSM_OPT

This optional parameter identifies the path and file name of the Tivoli Storage Manager client options file: *dsm.opt*

Default

The default value is the path of the Tivoli Storage Manager client installation directory.

Advanced mode only

Yes.

DSM_LOG

This optional parameter identifies the path used for the Tivoli Storage Manager client error log file: *dsmerror.log*

Default

The default value is an empty string.

Advanced mode only

Yes.

DB2STANDBY

The DB2STANDBY section is the same as the CLIENT section, except when it is configured for a DB2 database that acts as a DB2 HADR secondary. After takeover, when the database is active, the CLIENT section is used. The parameters do not depend on the storage device.

The following list provides the applicable parameters, a description of each parameter, and default values:

PRE_FLASH_CMD

This parameter identifies the command script, or executable file, used to quiesce the DB2 standby server or DB2 High-Availability Disaster Recovery (HADR) secondary server. This quiescing occurs immediately before the snapshot operation begins.

When the value of this parameter includes command arguments, place the values for the command arguments between quotation marks. For example: "

This parameter is required for the profile, or it needs to be specified from the command-line interface. If specified from the command-line interface, the parameter overrides the corresponding parameter in the profile.

Default

There is no default value.

Advanced mode only

No.

POST_FLASH_CMD

This parameter identifies the command script, or executable file, used to resume the DB2 standby server or DB2 High-Availability Disaster Recovery (HADR) secondary server immediately after the snapshot is created.

When the value of this parameter includes command arguments, place the values for the command arguments between quotation marks. For example: "

This parameter is required for the profile, or it needs to be specified from the command-line interface. If specified from the command-line interface, the parameter overrides the corresponding parameter in the profile.

Default

There is no default value.

Advanced mode only

No.

DB2_PRODUCTION_SERVER

This parameter contains the following two values:

host name or TCP/IP name

Specify either the host name or TCP/IP name of the DB2 server where the HADR primary server, the production system, is running.

TCP/IP port

The TCP/IP port where the DB2 production database instance is listening for remote connections (DB2 database manager configuration parameter SVCENAME).

Both value are separated by a space and both values are required to be specified.

Default

There is no default value for this required parameter.

Advanced mode only

No.

DB2_ALIAS

Specify the alias name of the DB2 database running on the HADR primary server.

Default

There is no default value for this required parameter.

Advanced mode only

No.

DB2_USERNAME

This parameter specifies the DB2 user that is used to connect from the HADR standby server to the DB2 database running on the HADR primary server.

Default

The user name of the user who starts the tsm4acs operation.

Advanced mode only

Yes.

DB2_AUTH_TYPE

This optional parameter is used to specify the value of the DB2 instance AUTHENTICATION parameters on the DB2 HADR primary server. The following list identifies valid values:

SERVER

Authentication of the user name and password takes place at the server.

CLIENT

Authentication of the user name and password takes place at the client.

SERVER_ENCRYPT

Specifies that authentication takes place on the node containing the target database, and that the authentication password is to be encrypted.

DATA_ENCRYPT

Specifies that authentication takes place on the node containing the target database, and that connections must use data encryption.

GSSPLUGIN

Specifies that authentication takes place using an external GSS API-based plug-in security mechanism.

Default

SERVER_ENCRYPT

Advanced mode only

No.

TSM_BACKUP

To create a Tivoli Storage Manager backup from a snapshot, install Tivoli Storage FlashCopy Manager on a backup server. The offload agent runs to trigger a Tivoli Storage Manager backup from any snapshot created with **TSM_BACKUP** set to YES, MANDATE, or LATEST.

If Tivoli Storage FlashCopy Manager is used with IBM Tivoli Storage Manager for Enterprise Resource Planning, this parameter is moved to the .utl file under the new name TSM_BACKUP_FROM_SNAPSHOTS for Oracle in an SAP environment environments.

YES

Create a Tivoli Storage Manager backup from this snapshot. If the Tivoli Storage Manager backup operation does not successfully complete, reuse the target set.

MANDATE

In contrast to YES, do not reuse the target set until the Tivoli Storage Manager backup completes.

LATEST

When a snapshot backup was performed with **TSM_BACKUP LATEST** and the offloaded backup to Tivoli Storage Manager has either not started or has failed, any new snapshot backup with option **TSM_BACKUP** set to LATEST, YES, or MANDATE, removes the backup request to Tivoli Storage Manager from the previous backup. This removal prevents backup requests to Tivoli Storage Manager from queuing if the requests are not completed in time.

NO Keep the snapshot backup and do not use the backup as a source for a subsequent tape backup operation.

TSM_ONLY

The backup is automatically marked for deletion during the unmount

operation after the Tivoli Storage Manager backup has completed. This deletion occurs whether or not the backup was successful.

USE_FOR *list of device classes*

This attribute can be combined with any of these options to limit its application to snapshots performed with particular device classes as specified in the profile. Any number of device classes that are listed must be separated by spaces.

Note: (DB2) The ability to create a Tivoli Storage Manager backup from a snapshot requires a Tivoli Storage FlashCopy Manager license.

Default

There is no default value.

Advanced mode only

Yes.

MAX_VERSIONS

When the DB2 system acts as the DB2 standby server or as a high-availability disaster recovery secondary server, this parameter is evaluated, instead of the parameter specified in the CLIENT section.

This parameter accepts the following options:

ADAPTIVE

The maximum number varies depending on the available space. Tivoli Storage FlashCopy Manager reuses the oldest target set as the target for the current backup.

n The value specified as *n* represents the maximum number of snapshot versions to maintain. When this limit is reached, the oldest version is deleted.

Default

ADAPTIVE

Advanced mode only

Yes.

DEVICE_CLASS

When the DB2 system acts as the DB2 standby server or as a high-availability disaster recovery secondary server, this parameter is evaluated, instead of the parameter specified in the CLIENT section.

When specifying the options for this parameter, use the following syntax:

<list of device classes> [*<conditions>*]

During backup, Tivoli Storage FlashCopy Manager uses one of the device classes listed in the *<list of device classes>* of the **DEVICE_CLASS** statement for which the *<conditions>* evaluates to *true*. If multiple *<conditions>* statements evaluate to true the operation fails. For the device classes listed in the *<list of device classes>*, separated by spaces, Tivoli Storage FlashCopy Manager use the device class that follows the device class which was used most recently for the next backup operation. If the last device class in the list was used during the most recent backup, or if no device class in the list was used for a backup, Tivoli Storage FlashCopy Manager uses the first device class in the list. The value of the **DEVICE_CLASS** parameter uses the following syntax:

[USE_AT *<days of week>*] [FROM *<time>* TO *<time>*]
(partitioned DB2 databases) [ON_DBPARTITIONNUMS] *<list of partitions>*

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, Tivoli Storage FlashCopy Manager uses the same **DEVICE_CLASS** value that was used during the backup.

Additional **DEVICE_CLASS** sections are added to the Tivoli Storage FlashCopy Manager profile automatically by the setup script when you add additional instances of the **DEVICE_CLASS** parameter to the **CLIENT** section.

Default

STANDARD

Advanced mode only

Yes.

OFFLOAD_DB2STANDBY

The OFFLOAD_DB2STANDBY section has the same semantics as the OFFLOAD section, except that it is evaluated whenever an offloaded backup from a DB2 HADR secondary occurs instead of the DB2 HADR primary.

The parameters in the OFFLOAD_DB2STANDBY section are the same as the OFFLOAD section, except for the addition of the parameters that are marked for custom applications. The parameters do not depend on the storage device. The parameter **BACKUP_METHOD** is set to TSM_CLIENT for this standby variant of the offload section.

Changing profile parameters

Except for the GLOBAL and ACSD sections, changes to the profile take effect immediately and do not require restarting Tivoli Storage FlashCopy Manager. Updates to the GLOBAL and ACSD sections require a restart of Tivoli Storage FlashCopy Manager.

About this task

To change the GLOBAL and ACSD sections, complete the following steps:

Procedure

1. For each system where Tivoli Storage FlashCopy Manager is installed, enter the following command to stop Tivoli Storage FlashCopy Manager:

```
setup_type.sh -a stop
```

2. Start the setup script by entering the appropriate command for your database environment:

DB2 ./setup_db2.sh

Oracle

 ./setup_ora.sh

Custom applications

 ./setup_gen.sh

To use the advanced mode, use the **-advanced** option with the appropriate setup script command. In the advanced mode, you can specify more parameters.

3. Follow the setup script instructions that are displayed.
4. For each system where Tivoli Storage FlashCopy Manager is installed, enter the following command to start Tivoli Storage FlashCopy Manager:

```
setup_type.sh -a start -d Instance_owner_$HOME directory
```

For DB2 databases, change *INSTANCE_owner_\$HOME_directory* to *INSTANCE_owner_\$HOME_directory/sql1ib*.

Interdependency of LVM_FREEZE_THAW and TARGET_DATABASE_SUSPEND

The **LVM_FREEZE_THAW** and **TARGET_DATABASE_SUSPEND** parameters are interdependent.

These two Tivoli Storage FlashCopy Manager 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 YES 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.
- If **LVM_FREEZE_THAW** is set to AUTO, and the file systems support the freeze function, the effect of AUTO is described in the following table. If the file systems do not support the freeze function, the AUTO value resolves to NO.

For Oracle ASM environments, **TARGET_DATABASE_SUSPEND** is independent of **LVM_FREEZE_THAW**, and **LVM_FREEZE_THAW** is not allowed for ASM.

The following table summarizes the actions taken depending on the values of the two parameters:

Table 20. 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	OFFLINE
YES	Suspend and freeze	Terminate with an appropriate error message. Conflicting parameters.	Offline with freeze
NO	Suspend, no freeze	No suspend, no freeze	Offline without freeze
AUTO	Treat as LVM_FREEZE_THAW YES	Treat as LVM_FREEZE_THAW NO	Offline with freeze

Target volumes

The target volumes file (.fct) identifies the target volumes to be used for a Tivoli Storage FlashCopy Manager backup operation.

During a FlashCopy backup on IBM System Storage DS8000, SAN Volume Controller, or Storwize family a set of target volumes (the target set) are required for each set of source volumes that are to be copied. More than one target set can be defined for use in different FlashCopy backups. The volumes in each target set that are used in a backup must be specified in a similar way in a separate target set topic. These target sets are specified in a target volumes file, the .fct file. The target set section name begins with the prefix **TARGET_SET** and is appended with a target set name. The target set name differentiates different target set sections. The target set name can be any alphanumeric value. Note, target set definitions are not required on XIV system, IBM System Storage N series, and NetApp.

In each topic section in the target volumes file, use one **TARGET_VOLUME** parameter for each target volume to be used in the target set, as shown in the following example:

```
>>> TARGET_SET 1
TARGET_VOLUME ...
.
.
.
TARGET_VOLUME ...
<<<
```

To specify multiple target sets in the target volumes file, add the next target set section with a unique target set ID as shown in this example:

```
>>> TARGET_SET 2
TARGET_VOLUME ...
.
.
.
TARGET_VOLUME ...
<<<
```

Comments can be entered before the first target set section only and are indicated by a “#” character in the first column of each line. Tab characters can be entered.

When **VOLUMES_FILE** is specified in the profile, the target volumes file can have any file name and does not conform to any naming convention.

Managing target volumes by storage system

The storage system affects the mapping of target volumes.

About this task

Table 21. Managing target volume LUNs by storage system

IBM System Storage DS8000	SAN Volume Controller and Storwize family	XIV system, IBM System Storage N series, and NetApp
Manual target LUN creation with the target volumes file (.fct) using the VOLUMES_FILE parameter	<p>Either one of the following options:</p> <ul style="list-style-type: none"> Manual target LUN creation with the target volumes file (.fct) using the VOLUMES_FILE parameter Naming convention with the TARGET_NAMING parameter 	Automatic target LUN creation without using target volumes file (.fct)

On DS8000 and SAN Volume Controller or Storwize family storage systems, use the **TARGET_SETS** parameter to specify the target volumes file (**VOLUMES_FILE**). The **VOLUMES_FILE** can be used to share a target volume file between multiple device classes by restricting a target set to a specific **DEVICE_CLASS**. On a partitioned DB2 environment, use the **VOLUMES_FILE** parameter to create target set definitions for specific **PARTITION** sections. This setting is required when two partitions are accessing the same **TARGET_SET** during a single backup operation.

To further simplify target mapping on SAN Volume Controller, the **TARGET_NAMING** parameter allows a naming convention to be specified for the target volumes. This enables Tivoli Storage FlashCopy Manager to map source volumes to suitable target volumes without requiring the storage administrator to manually list all targets in the target volumes file.

Tivoli Storage FlashCopy Manager uses the following criteria to associate a target volume to a source volume:

- The source volume and target volume in the same storage system.
- The source volume and target volume have the same size.

Tivoli Storage FlashCopy Manager selects a target volume to be validated as a suitable target volume for the source volume depending on the value of the parameter **TARGET_SETS**:

- SAN Volume Controller or Storwize family only: The **TARGET_NAMING** parameter naming convention that is specified:

The following sample explains the usage of the naming convention that is specified by the **TARGET_SETS** and **TARGET_NAMING** parameters:

- Assuming the source volumes are named A01pro_1 and A01pro_2
- Assuming the **TARGET_SETS** profile parameter has a value of 1
- Assuming the **TARGET_NAMING** parameter value as %SOURCE_t%TARGETSET

Using this target naming definition, the source volume A01pro_1, with target set named 1, results in target volume A01pro_1_t1, and source volume A01pro_2 results in the target volume A01pro_2_t1.

- **VOLUMES_FILE**:

A target volumes file (.fct) must be specified.

As a minimum, a list of target volumes must be specified in the target volumes file. The source volumes and the size are both optional. If no source is specified and a FlashCopy relation exists between these target volumes and one of the source volumes, the Tivoli Storage FlashCopy Manager software checks for each of the specified target volumes. If a FlashCopy relation exists, it is reused for the next FlashCopy backup. If no FlashCopy relation exists to one of the source volumes, a new relation between one source volume and this target is created with the next FlashCopy backup. In the latter case, the created source-target pairs are unpredictable because they depend on the order of the target volumes that are listed in the target volumes file. There is also a dependency on the order of the source volumes as they occur in the operating system.

If you want predefined source-target pairs, you must specify the dedicated source volume for each of the target volumes in the target volumes file.

Alternatively you can ensure that all FlashCopy relations exist in the storage system before the start of the FlashCopy backup.

This example shows the syntax of target volumes files that are specified by the **VOLUMES_FILE** parameter:

```
>>> TARGET_SET <target set name>
```

```
DEVICE_CLASS <device class name> # this parameter is optional and allows to
                                   # restrict the use of this target set to a
                                   # specific device class
```

```
>>> PARTITION <name of partition> # e.g. NODE0000 for partition 0 or NODE0001 for
                                   #partition 1, ...
```

```
TARGET_VOLUME <target> [<source>] [<size>]
[...]
```

```
<<<
[...]
```

```
<<<
```

```
[...]
```

In DB2 in an SAP environment multi-partition environments (especially when migrating from Tivoli Storage Manager for Advanced Copy Services 5.4), database files of the DB2 partitions of one production server can be allocated in the same volume groups and on the same source volumes on the storage system. This concept is referred to as volume sharing. Tivoli Storage FlashCopy Manager supports volume when the **TARGET_SETS** profile parameter is set to **VOLUMES_FILE** and the **PARTITION_GROUP** parameter is specified in the **DEVICE_CLASS**. This is an example of such a configuration:

```
<ACS_DIR>/profile:
...
>>> DEVICE_CLASS STANDARD
...
PARTITION_GROUP GROUP_A 0 1
PARTITION_GROUP GROUP_B 2 3
...
TARGET_SETS VOLUMES_FILE
VOLUMES_FILE <ACS_DIR>/acsvolumes/volumes_file.fct
<<<

<ACS_DIR>/acsvolumes/volumes_file.fct:
>>> TARGET_SET 1
>>> PARTITION GROUP_A
TARGET_VOLUME J01acs_td_0
TARGET_VOLUME J01acs_t1_0
TARGET_VOLUME J01acs_td_1
TARGET_VOLUME J01acs_t1_1
...
<<< PARTITION GROUP_A

>>> PARTITION GROUP_B
TARGET_VOLUME J01acs_td_2
TARGET_VOLUME J01acs_t1_2
TARGET_VOLUME J01acs_td_3
TARGET_VOLUME J01acs_t1_3
...
<<< PARTITION GROUP_B
<<< TARGET_SET 1

>>> TARGET_SET 2

...
<<< TARGET_SET 2
```

If you migrated data from Tivoli Storage Manager for Advanced Copy Services 5.5 or later to Tivoli Storage FlashCopy Manager, the **VOLUMES_DIR** parameter is deprecated. Specifying **TARGET_SETS VOLUMES_FILE** and setting the **VOLUMES_FILE** parameter is the required method for specifying the target volumes file.

To further simplify target mapping on SAN Volume Controller, the **TARGET_SETS** parameter allows a naming convention to be specified for your target volumes. This enables Tivoli Storage FlashCopy Manager to map source volumes to suitable target volumes without requiring the storage administrator to manually list all targets in the target volumes file.

Target volume parameter settings (DS8000 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 22. Parameters of the 'VOLUMES_SET_x' Topic (DS8000)

Parameter Name	Value
TARGET_VOLUME <target volume serial number> <source volume serial number> <source volume size>	<p>A target set definition file contains a list of target volumes that are organized into target sets. Tivoli Storage FlashCopy Manager attempts to match source volumes to suitable targets within a target set during backup. To determine source target relations in advance, specify a source serial number with a target serial number in the target set definition file. In this situation, the relation between the source and target is required and backup processing fails if one of the targets is unavailable for the specified source.</p> <p>This example shows a configuration where the DS8000 source volume with serial 75924811011 must be used in a FlashCopy with the target volume with serial number 75924811001.</p> <pre>TARGET_VOLUME 75924811001 75924811011 Size=2.0_GB</pre> <p>The source serial number and the size can be omitted completely or dashes can be entered in both fields as placeholders, as shown in the following example:</p> <pre>TARGET_VOLUME 75924811001 - -</pre> <p>The dashes will be ignored. Note the target volume requirements for a FlashCopy:</p> <ul style="list-style-type: none">• The size must be the same as that of the source volume• The source and target volumes that are listed in one TARGET_SET must be in the same storage subsystem <p>Note: Do not change the order of the parameters (target volume serial number, source volume serial number, size of source volume).</p> <p>See “Target volumes” on page 199 for detailed information about the criteria that are used to associate a target volume to a source volume.</p>

The FLASHCOPY_TYPE parameter is only valid for DS8000 and SAN Volume Controller or Storwize family. If it becomes necessary to make any of these changes:

- change the FLASHCOPY_TYPE value of an existing target set
- remove a target volume from an existing target set
- remove a complete target set

You must use the sequence of commands that are described in “Deleting Tivoli Storage FlashCopy Manager snapshot backups” on page 289 with the force option.

Related reference:

“Example target volumes file DS8000 configuration” on page 234

Target volume parameter settings for SAN Volume Controller configuration and Storwize family

Each target volume that is used must be specified by the corresponding virtual disk name.

A snapshot backup operation looks for either a source volume and target volume correlation, or a target-volume-only specification.

Table 23. Parameters of the 'VOLUMES_SET_x' topic (SAN Volume Controller and Storwize family)

Parameter Name	Value
TARGET_VOLUME <target volume virtual disk name> <source volume virtual disk name> <source volume size>	<p>A target set definition file contains a list of target volumes that are organized into target sets. During the backup process, the Tivoli Storage FlashCopy Manager software attempts to match source volumes to suitable targets within a target set. To determine source target relations in advance, specify a source virtual disk name with a target virtual disk name in the target set definition file. In this scenario, the relation between the source and target is required and backup processing fails if one of the targets is unavailable for the specified source.</p> <p>This example shows a configuration where the SAN Volume Controller source volume with virtual disk name <i>svdfsrc4</i> must be used in a FlashCopy with the target volume with virtual disk name <i>svdftgt4</i>. TARGET_VOLUME svdftgt4 svdfsrc4 Size=2.0_GB</p> <p>The source virtual disk name and the size can be omitted completely or dashes can be entered in both fields as placeholders, as shown in the following example: TARGET_VOLUME svdftgt4 - -</p> <p>The following list identifies the target volume requirements for a FlashCopy:</p> <ul style="list-style-type: none"> • The size of the target volume must be the same or greater than the size of the source volume. • The source and target volumes that are listed in one TARGET_SET must be in the same SAN Volume Controller cluster. <p>Note: Do not change the order of the parameters.</p> <p>For more information about the criteria that are used to associate a target volume to a source volume, see “Target volumes” on page 199.</p>

The **FLASHCOPY_TYPE** parameter is only valid for DS8000, SAN Volume Controller, and Storwize family. If you need to change target volumes, the following changes are supported:

- change the **FLASHCOPY_TYPE** value of an existing target set
- remove a target volume from an existing target set
- remove a complete target set

To complete these types of changes, use the sequence of commands that are described in “Deleting Tivoli Storage FlashCopy Manager snapshot backups” on page 289 with the force option.

For SAN Volume Controller 6.1 or later and Storwize family, with Tivoli Storage FlashCopy Manager software you can delete FlashCopy mappings that are not dependent on other FlashCopy mappings. Only the source and target FlashCopy mappings of the oldest backup can be deleted. If multiple backup generations are

used and you want to delete a backup that is not the oldest backed up version, the background operation that deletes the mappings is delayed until all older backups are deleted or are reused by a new backup request.

The following example presents a typical Multiple Target FlashCopy (MTFC) cascade:

S->T4->T3->T2->T1

S = Source volume

T1-T4 = Snapshots taken at t1, t2, t3, t4 where T1 is the oldest,
T4 the most recent snapshot

T1 depends on T2,T3,T4,S

T2 depends on T3,T4,S

and so on...

Following the path from S to T4 is called *downstream*. The opposite direction is called *upstream*.

Example 1: T2 is restored

All upstream snapshot mappings are stopped: T3,T4

Example 2: T2 is overwritten by a new backup

All downstream snapshot mappings are stopped: T1

Related reference:

“Example target volumes file (SAN Volume Controller configuration or Storwize family)” on page 235

Target set handling for cloning

Cloning operations require specific settings for target sets.

The TARGET_SETS profile parameter identifies the target volumes to be used in the FlashCopy operation. This parameter must be specified in the device class section of the profile. You can specify one of these values with cloning operations:

VOLUMES_FILE *name of the target volumes file (.fct)*

Specify the name of the target volumes file (.fct). The USE_FOR_CLONING *list of clone database names* statement identifies the correct target set to use for a specific clone database name. When more than one clone database name is specified in the list, the referenced target set is used for all specified clone database names. Each name that is specified in the list must be separated by a space. In this situation, the target set must be used by those clone databases only that are identified in the list. The USE_FOR_CLONING *list of clone database names* must be specified in the target volumes file.

TARGET_NAMING *string with wildcards %SOURCE USE_FOR_CLONING list of clone database names*

Available for SAN Volume Controller only. Specify the naming convention for target volumes. When a backup volume is required at backup time, Tivoli Storage FlashCopy Manager determines the name of the target set for the current operation and the name of the source volume to be backed up. The name of the volume that stores the backup is the name that is specified when the string %SOURCE is replaced with the respective value in the current operation. The required USE_FOR_CLONING *list of clone database names* statement identifies the correct target set to use for a specific clone database name. When more than one clone database name is specified in the list, the referenced target set is used for all specified clone database names. Each name that is specified in the list must be separated by a space. In this situation, only

the target set must be used by those clone databases that are identified in the list. The USE_FOR_CLONING list of clone database names must be specified with the TARGET_NAMING parameter itself. It is possible to have multiple TARGET_NAMING entries in the device class where each represents a different clone database name.

Restriction: For SAN Volume Controller and Storwize family, when a new backup is started on a target volume that is not the oldest in the chain, SAN Volume Controller stops all mappings to older target volumes. When a restore is requested from a target volume that is not the youngest in the chain, SAN Volume Controller stops all mappings to newer target volumes. When a mapping to a target volume stops in either of these situations, this target volume immediately goes offline if any of these conditions exist:

- The target volume is a space-efficient volume.
- The mapping was for an incremental copy that was ongoing.
- The mapping was for a full copy that was ongoing.

As a result, the target volumes for the production database to be cloned, and the target volumes for the FlashCopy backup of the same database, must not be on the same SAN Volume Controller or Storwize family cluster. If you are cloning databases in an AIX Logical Volume Mirroring (LVM) environment, use FlashCopy cloning on one of the SAN Volume Controller or Storwize family clusters and FlashCopy backup on the other SAN Volume Controller or Storwize family cluster. Avoid space-efficient target volumes for cloning. If space-efficient target volumes are used, the profile parameter ALLOW_NOCOPY_FLASHCOPY YES must be specified in the cloning device class section of the profile.

Target volumes file (.fct) cloning examples

The target volumes file (specified by the VOLUMES_FILE parameter) must have the following syntax (for multi-partition DB2):

```
>>> TARGET_SET target set name
DEVICE_CLASS <device classes> USE_FOR_CLONING <list of clone database names>
# this parameter is mandatory for FlashCopy Cloning and allows to
# restrict the use of this target set to a specific device class
# and to a specific clone database name or a list of clone database names
>>> PARTITION name of partition
# e.g. NODE0000 for partition 0 or NODE0001 for partition 1, ...
# or the name of a PARTITION_GROUP
TARGET_VOLUME target [source] [size]
[...]
```

The target volumes file (specified by the VOLUMES_FILE parameter) must have the following syntax (single partition DB2 and Oracle):

```
>>> TARGET_SET target set name
DEVICE_CLASS <device classes> USE_FOR_CLONING <list of clone database names>
# this parameter is mandatory for FlashCopy Cloning and allows to
# restrict the use of this target set to a specific device class
# and to a specific clone database name
TARGET_VOLUME target [source] [size]
[...]
```

Tivoli Storage FlashCopy Manager password file

To access the storage system where the database volumes are stored, Tivoli Storage FlashCopy Manager requires a password file.

About this task

The password file contains a *master password* that is required by the agents such as application agents or offload agents, when they are authenticating or connecting to the Management Agent. When Tivoli Storage FlashCopy Manager agents are running in a distributed environment across multiple servers or in DB2 DPF partitions, separate password file instances can be used for different nodes. In a distributed environment, you must ensure that each local password file instance contains all the passwords that are needed by the agents that are running on the node. The master password must be included in all instances. Use the SSH for the setup to ensure that the password files are replicated to all nodes automatically.

The master password is only prompted for in advanced mode, and is only needed when you are installing Tivoli Storage FlashCopy Manager separately on the backup servers or cloning servers without using SSH. In this case, you must know the password. The password is defined when you configure the production server; for backup and cloning servers this password must be used so that the servers can connect to the management agent on the production server. When you use SSH for remote deployment to the backup and cloning servers, the password file is copied to the servers automatically.

In basic mode, the password is not prompted as it is generated automatically if it is not set earlier. A generated password is available as the default password in advanced mode.

A password file is created during the Tivoli Storage FlashCopy Manager configuration process. The setup script that is used for the configuration also updates information that is stored in the `/etc/inittab` directory. An example of the path to the password file follows:

```
<ACS_DIR>/shared/pwd.acsd
```

where `<ACS_DIR>` is the value of the **ACS_DIR** parameter in the profile.

The minimum length of the master password is 8 characters. The password must contain at least one number and one letter. The use of special symbols increases the strength of the password.

BACKINT configuration file

The BACKINT configuration file includes parameters for the SAP with Oracle BACKINT interface and the backup server. The file extension for the BACKINT configuration file is `.utl`.

SAP Oracle FlashCopy Manager with Tivoli Storage Manager

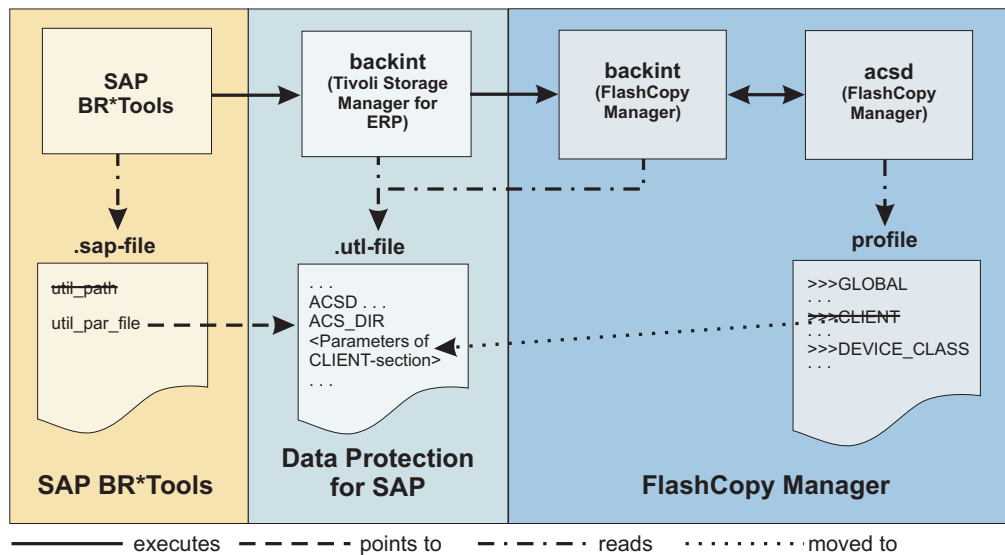


Figure 17. SAP with Oracle, Tivoli Storage FlashCopy Manager with Tivoli Storage Manager

If Tivoli Storage FlashCopy Manager is used with IBM Tivoli Storage Manager for Enterprise Resource Planning to protect an SAP system that runs with an Oracle database, the parameters that are typically specified in the CLIENT section can be added to the Tivoli Storage Manager for ERP configuration file (.utl file). If the parameters are specified in the Tivoli Storage Manager for ERP configuration file, Tivoli Storage FlashCopy Manager does not require a separate .utl file.

When you use the Tivoli Storage FlashCopy Manager setup script, new instances of the DEVICE_CLASS parameter are added to the CLIENT section of the profile configuration file. If you use Tivoli Storage FlashCopy Manager with IBM Tivoli Storage Manager for Enterprise Resource Planning, the Tivoli Storage FlashCopy Manager profile does not contain a CLIENT section.

The following list describes each parameter, associated values, and default values for the .utl file. The **TSM_BACKUP_FROM_SNAPSHOT**, **TARGET_DATABASE_SUSPEND**, and **ACS_DIR** parameters must be defined in the .utl file. All other parameters are optional and are not required to be specified in the .utl file.

TSM_BACKUP_FROM_SNAPSHOT

To create a Tivoli Storage Manager backup from a snapshot, install Tivoli Storage FlashCopy Manager on a backup server. The offload agent can be run to trigger a Tivoli Storage Manager backup from any snapshot that is created with **TSM_BACKUP** set to YES, MANDATE, or LATEST.

If Tivoli Storage FlashCopy Manager is used with IBM Tivoli Storage Manager for Enterprise Resource Planning, this parameter is moved to the .utl file under the new name **TSM_BACKUP_FROM_SNAPSHOTS** for SAP with Oracle environments.

YES

Create a Tivoli Storage Manager backup from this snapshot. If the Tivoli Storage Manager backup operation does not complete successfully, the target set can be reused.

MANDATE

In contrast to YES, do not reuse the target set until the Tivoli Storage Manager backup completes.

LATEST

When a snapshot backup was run with **TSM_BACKUP LATEST**, and the offloaded backup to Tivoli Storage Manager failed or did not start, any new snapshot backup with option **TSM_BACKUP** set to LATEST, YES, or MANDATE, removes the backup request to Tivoli Storage Manager from the previous backup. This removal prevents backup requests to Tivoli Storage Manager from queuing if the requests cannot be completed in time.

NO Keep the snapshot backup and do not use it as a source for a subsequent tape backup operation.

TSM_ONLY

The backup is automatically marked for deletion during the unmount operation after the Tivoli Storage Manager backup is completed. The backup is marked for deletion when the backup is successful and when the backup is unsuccessful.

USE_FOR *list of device classes*

This attribute can be combined with any of the options to limit application to snapshots run with particular device classes as specified in the profile. Use a space to separate device classes.

Note: (DB2 only) A Tivoli Storage FlashCopy Manager license is required to create a Tivoli Storage Manager backup from a snapshot.

Default

There is no default value, you must specify a value from one of the possible options.

Advanced mode only

No

MAX_SNAPSHOT_VERSIONS

There are two options: ADAPTIVE and *n*. For ADAPTIVE, the maximum number varies depending on the available space. Tivoli Storage FlashCopy Manager reuses the oldest target set as the target for the current backup. For *n*, *n* equals the maximum number of snapshot versions to be maintained. When this limit is reached, the oldest version is deleted.

Default

ADAPTIVE

Advanced mode only

Yes

LVM_FREEZE_THAW

The **LVM_FREEZE_THAW** and **TARGET_DATABASE_SUSPEND** profile parameters are interdependent:

- 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 YES 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.

- If **LVM_FREEZE_THAW** is set to **AUTO**, and the file systems support the freeze function, the effect of **AUTO** is described in the following table. If the file systems do not support the freeze function, the **AUTO** value resolves to **NO**.

For Oracle ASM environments, **TARGET_DATABASE_SUSPEND** is independent of **LVM_FREEZE_THAW**, and **LVM_FREEZE_THAW** is not allowed for ASM.

The following table summarizes the actions that can be completed, depending on the values of the **LVM_FREEZE_THAW** and **TARGET_DATABASE_SUSPEND** parameters:

Table 24. 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	OFFLINE
YES	Suspend and freeze	Stops with an appropriate error message. Conflicting parameters.	Offline with freeze
NO	Suspend, no freeze	No suspend, no freeze	Offline without freeze
AUTO	Treat as LVM_FREEZE_THAW YES	Treat as LVM_FREEZE_THAW NO	Offline with freeze

YES

Enable freeze before the snapshot, and enable thaw afterward. For AIX, the value **YES** is valid only if all file systems involved in the backup are JFS2 file systems.

- NO** Do not enable a freeze. To set this parameter to **NO**, a licensed version of Tivoli Storage FlashCopy Manager is needed and a backup server is required for mounting the snapshot to ensure file system consistency.

The value **NO** is required if at least one JFS file system is involved.

AUTO

If **TARGET_DATABASE_SUSPEND** is **YES**, **LVM_FREEZE_THAW** is also set to **YES**.

Default

AUTO

Advanced mode only

Yes

TARGET_DATABASE_SUSPEND

The **LVM_FREEZE_THAW** and **TARGET_DATABASE_SUSPEND** profile parameters are interdependent:

- 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 **YES** 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.
- If **LVM_FREEZE_THAW** is set to **AUTO**, and the file systems support the freeze function, the effect of **AUTO** is described in the following table. If the file systems do not support the freeze function, the **AUTO** value resolves to **NO**.

For Oracle ASM environments, **TARGET_DATABASE_SUSPEND** is independent of **LVM_FREEZE_THAW**, and **LVM_FREEZE_THAW** is not allowed for ASM.

The following table summarizes the actions that are taken depending on the values of the **LVM_FREEZE_THAW** and **TARGET_DATABASE_SUSPEND** parameters:

Table 25. 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	OFFLINE
YES	Suspend and freeze	Stops with an appropriate error message. Conflicting parameters.	Offline with freeze
NO	Suspend, no freeze	No suspend, no freeze	Offline without freeze
AUTO	Treat as LVM_FREEZE_THAW YES	Treat as LVM_FREEZE_THAW NO	Offline with freeze

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. Use this value 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 you run a backup with OFFLINE specified, the target database on the production system must be in a *startup mount* state at the time that either *acsora* or *acsutil* is issued. Otherwise, recovery must be run to restore the database.

Default

There is no default. A value for this parameter must be specified by the user.

Advanced mode only

No

DEVICE_CLASS

When you back up data, the Tivoli Storage FlashCopy Manager software uses a device class. The following sample identifies the syntax that can be used with the **DEVICE_CLASS** parameter:

```
DEVICE_CLASS <list_of_device_classes> [conditions]
```

When a list of device classes is specified, the software determines which device class matches the device class in the environment. When multiple device classes are specified, separate the device classes with the space character. The condition statement is optional. When you use the condition statement, use the following syntax:

```
[USE AT days of week] [FROM time TO time]
(partioned DB2 databases) [ON_DBPARTITIONNUMS list of partitions]
```

When there are different devices, multiple sections can be used. Each section provides information about a particular device. To select a particular section, use the **DEVICE_CLASS** parameter. When the software restores data, the software uses the **DEVICE_CLASS** value that is specified when the data was backed up.

The configuration wizard (the setup script) automatically adds **DEVICE_CLASS** sections to the Tivoli Storage FlashCopy Manager profile when you add more instances of the **DEVICE_CLASS** parameter to the CLIENT section of the profile.

Default

STANDARD

Advanced mode only

No.

ALLOW_FULL_FILE_BACKUP

This parameter cannot be changed when you use the setup script. The options are YES and NO. This value specifies whether a full file backup is stored to the repository. Storing a full file backup or a full database backup to the repository affects performance.

Default

NO

Advanced mode only

Yes

TIMEOUT_FLASH

Specify the maximum time in seconds that the database agent waits for a response to the management agent call during the flash phase. If the database agent does not receive a response within the specified time, an error message is posted.

This parameter also specifies the maximum time in seconds that database can be suspended. This time setting also sets the maximum time for which JFS2 file systems can be frozen. If the timeout is reached, the file systems thaw, the database is resumed, and the backup operation ends with an error. If the parameter **LVM_FREEZE_THAW** is set to AUTO or YES, the minimal time value for **TIMEOUT_FLASH** is 5 seconds. The minimal value is 1 second.

Default

120 seconds

Advanced mode only

Yes

TIMEOUT_<PHASE>

Specify the maximum time in seconds that the database agent waits for a response to the management agent call during the <phase> phase. If the database agent does not receive a response within the specified time, an error message is posted.

You can specify one of these phase values for a FlashCopy backup. For example, **TIMEOUT_PREPARE**.

- PARTITION
- PREPARE
- FLASH
- VERIFY
- CLOSE

You can specify one of these phase values for a FlashCopy restore. For example, **TIMEOUT_FLASHRESTORE**.

- PREPARERESTORE
- FLASHRESTORE
- COMPLETERESTORE
- CLOSE

Default

3600 seconds

Advanced mode only

Yes

GLOBAL_SYSTEM_IDENTIFIER

Specify a string that is used in the IBM Tivoli Storage Manager for Enterprise Resource Planning Administration Assistant that uniquely identifies an Oracle database in the system landscape. This parameter is only valid when the **ADMIN_ASSISTANT** parameter is specified in the ACSD section of the profile.

Default

ORA_<DBname>

Advanced mode only

Yes

ACS_DIR

Path to the Tivoli Storage FlashCopy Manager configuration directory. This parameter is required. The following subdirectories are included in this directory:

logs The subdirectory contains all log and trace information for Tivoli Storage FlashCopy Manager.

shared The subdirectory contains information that is shared among all Tivoli Storage FlashCopy Manager components.

When the subdirectory is initially created, the only file that is stored in the directory is the password file: `pwd.acsd`. This file contains the passwords for all devices that are specified within the profile. The file also contains a master password that is used from all components for authentication when they are connecting to the management agent. When you are running remote configuration tasks from the production system with SSH, the information in these directories is promoted to all systems that belong to the instance where Tivoli Storage FlashCopy Manager is configured.

Default

`user_home/acs`

Advanced mode only

Yes

ACSD

The host name and port of the system where the management agent is running. The following format is used for **ACSD**: `hostname port`

This parameter must be identical on all systems where Tivoli Storage FlashCopy Manager is installed for a database instance. While the parameter must be identical, each database instance can be managed by an individual management agent.

Default

localhost 57328

Advanced mode only

No

BACKUPIDPREFIX

This parameter specifies a string that is added in front of the backup ID that is generated by FlashCopy Manager. This parameter can be used to separate the backups within the same repository so that other clients are not able to query, restore, or delete these backups.

The string can contain letters, integers, or the underscore character. The string must be 6 characters.

This parameter has the same meaning as the corresponding parameter in the IBM Tivoli Storage Manager for Enterprise Resource Planning *.utl file. Use the same value.

Default

None

Advanced mode only

Yes

TRACE, TRACEFILE

This parameter activates tracing. These parameters are set when you receive instructions from IBM Support.

Default

None

Advanced mode only

Yes

INCREMENTAL

This parameter is only for use with Oracle Recovery Manager (RMAN).

NO No is the default value. If it is set to NO all the other **INCREMENTAL*** parameters have no effect.

CUMULATIVE

The backup type is cumulative RMAN. Cumulative backups are run by using RMAN.

DIFFERENTIAL

The backup type is incremental RMAN. Incremental backups are run by using RMAN.

Default

NO

Advanced mode only

No

INCREMENTAL_CATALOG_CONNECT_STRING

This parameter is only for use with Oracle Recovery Manager (RMAN).

This parameter specifies the name of the catalog that is passed to RMAN to connect to the catalog database. This is the name of the listener for the catalog database. If the **INCREMENTAL** parameter is enabled and this value is missing, an error message is displayed.

Default

There is no default value. You must specify a value if the **INCREMENTAL** parameter has any value other than NO.

Advanced mode only

No

INCREMENTAL_CATALOG_USER

This parameter is only for use with Oracle Recovery Manager (RMAN).

This parameter specifies the name of the catalog that is passed to RMAN to connect to the catalog database. If the **INCREMENTAL** parameter is enabled and this value is missing an error message is displayed.

Default

There is no default value. You must specify a value if the **INCREMENTAL** parameter has any value other than NO.

Advanced mode only

No

INCREMENTAL_CHANNELS

This parameter is only for use with Oracle Recovery Manager (RMAN).

Specifies the number of parallel RMAN channels, 1 or more, that transfer the data.

Default

1

Advanced mode only

No

.

INCREMENTAL_LEVEL

This parameter is only for use with Oracle Recovery Manager (RMAN).

The RMAN incremental level is an integer of value 0 or 1. An **INCREMENTAL_LEVEL** of 0 generates a full backup and an **INCREMENTAL_LEVEL** value of 1 generates an incremental backup. The specification of day and time is optional. If day and time are used, multiple occurrences of this parameter are valid if the time specifications do not overlap. Time must be specified in the 24-hour format. Days can be specified by weekday abbreviations such as *Mon* or *Tue*, or by numerical values 0 or 6 where 0 is Sunday and 6 is Saturday. The syntax for day and time specification is [USE_AT <days of week> FROM <time> TO <time>]

Default

0

Advanced mode only

No

IBM Global Security Kit configuration

IBM Tivoli Storage FlashCopy Manager uses the security suite IBM Global Security Kit (GSKit), for Secure Socket Layer (SSL) and Transport Layer Security (TLS) TCP/IP connections. GSKit supports Federal Information Processing Standards (FIPS140-2) and also incorporates the new security standards as defined in the Special Publications 800131 (SP 800-131). GSKit is automatically installed by Tivoli Storage FlashCopy Manager.

This security standard requires longer key lengths, stronger cryptographic algorithms, and incorporates TLS Protocol version 1.2.

Enforcing SP800-131 compliant encryption

During the installation, Tivoli Storage FlashCopy Manager automatically creates a new key pair and a self-signed certificate if no default certificate exists. The key pair is stored in the local key database file. The self-signed certificate is created from the key pair and automatically distributed to all backup and cloning servers through the existing SSH remote deployment mechanisms.

If you do not use the SSH remote deployment capabilities of Tivoli Storage FlashCopy Manager, you must complete the following steps:

1. Manually copy the self-signed certificate `fcmselcert.arm` file to the Tivoli Storage FlashCopy Manager `INSTANCE_DIR` directory on the backup and cloning servers. The manually copied self-signed certificate is imported automatically when the setup routine is rerun on the backup or cloning servers.
2. Globally install GSKit on each server by running the setup script as root user on the backup or cloning server. The required installation files are available in the `gskit_install` subdirectory of the Tivoli Storage FlashCopy Manager `INSTANCE_DIR` directory. The files are visible to the backup and cloning servers. To install GSKit, enter one of the following commands
 - For DB2: `./setup_db2.sh -a install_gskit -d instance_directory`
 - For Oracle in an SAP environment or Oracle: `./setup_ora.sh -a install_gskit -d instance_directory`
 - For custom applications: `./setup_gen.sh -a install_gskit -d instance_directory`

If manually copying the self-signed certificate file to the backup and cloning servers is not feasible, as an alternative, use a signed certificate. The signed certificate can be from an internal or external certificate authority (CA). When SP800-131 encryption is enforced, the signed certificate must comply with the standard as defined by the National Institute of Standards and Technology (NIST) SP800-131 standard encryption. This standard requires a minimum key size = 2048 bits and a signature algorithm = RSA with SHA-224 or higher. Import the CA signed certificate to the key database on the production server.

If you use a standard CA-signed certificate, you do not need to handle `fcmselcert.arm` files. You must import the CA-signed certificate manually into the production server key ring. Use the GSKit command-line utilities to import the certificate to the production server. If the CA-signed certificate is not a standard certificate that GSKit has a root certificate for, you must import the certificate to all sites. No further action is necessary on the auxiliary server.

The following GSKit files are installed by Tivoli Storage FlashCopy Manager:

- A key database file, `fcmcert.kdb`, is in the **INSTANCE_DIR** directory.
The KDB file on the production server contains a new key pair and a self-signed certificate. On the backup and cloning servers, the KDB file contains the public part of the self-signed certificate.
- A request database file, `fcmcert.rdb`, is in the **INSTANCE_DIR** directory.
The request database file is used to store certificate requests that are associated with the key database. This file is automatically created when Tivoli Storage FlashCopy Manager creates a key database file. This file is created with the same name as the key database file, but with a `.rdb` extension.
- An encrypted stash file, `fcmcert.sth`.
The password that is protecting the key database file is generated automatically and is stored in the encrypted stash file.
- An ASCII encoded binary file, `fcmselfcert.arm`.
This file is used to export the public part of the self-signed certificate. It is also used to import the public part of the self-sign certificate to the backup and cloning servers.
When you install backup and clone servers separately without the use of SSH, the installation process installs and sets up IBM GSKit. In this scenario, after IBM GSKit installation, manually copy the self-signed certificate to the backup and cloning servers.
- A certificate revocation list file, `fcmcert.crl`.
This file contains a list of revoked certificates.

The `.kdb`, `.rdb`, `.crl`, and the `.sth` files contain critical security parameters and these parameters must be protected against unauthorized access by the operating system. It is advisable to back up the key database files regularly, especially if you are using a CA signed certificate.

If you are working with the self-signed certificates that are created by the setup script, you need to ensure that the `.arm` file is integrated on the auxiliary server. To do this, run the setup script on the production server through OpenSSL, or manually copy it to the auxiliary server and run the setup script there.

If you are using a CA signed certificate, you must use the GSKit command-line utilities to import the certificate to the production server. If the CA signed certificate is not a standard certificate that GSKit has a root certificate for, you must import the certificate to all sites.

The files that are needed for IBM GSKit are automatically installed during the installation. To enforce SP800-131 compliant encryption, during the configuration of Tivoli Storage FlashCopy Manager, you must set the **ENFORCE_TLS12** parameter to YES in the Tivoli Storage FlashCopy Manager profile file. You must use the advanced mode during the configuration to specify this parameter. Otherwise, TLS Protocol version 1.0 and 1.1 is enabled as the default value for the **ENFORCE_TLS12** parameter is NO.

Any existing self-signed certificates that were created by a previous version of Tivoli Storage FlashCopy Manager must be deleted to allow Tivoli Storage FlashCopy Manager to create new self-signed certificates. To remove any existing self-signed certificates, go to the Tivoli Storage FlashCopy Manager installation (**INSTANCE_DIR**) directory and enter the following command:

```
rm fmcert.*
```

Note: It is not required to delete an existing external certificate authority (CA) signed certificates. However, if the CA signed certificate does not meet the minimum SP800-131 criteria, you must manually replace it with a new one.

Uninstalling GSKit

GSKit must not be uninstalled unless you are sure that no product on the system is using it. By uninstalling GSKit you are removing the global GSKit installation from the system entirely.

You can globally uninstall GSKit on each server by running the setup script on the backup or cloning server with one of the following options:

- For DB2: `./setup_db2.sh -a uninstall_gskit -d instance_directory`
- For Oracle in an SAP environment or Oracle: `./setup_ora.sh -a uninstall_gskit -d instance_directory`
- For custom applications: `./setup_gen.sh -a uninstall_gskit -d instance_directory`

Related reference:

“GSKit commands” on page 248

Oracle in an SAP environment BR*Tools configuration profile (.sap)

This configuration profile is stored in the `$ORACLE_HOME/dbs` directory.

The `.sap` profile is described in detail in the *SAP® database guide for Oracle* that is provided by SAP®. It is possible that there is an existing `.sap` file in your environment. The following information identifies the profile parameters that are valid in the `.sap` profile.

The following list contains parameters that you most likely need to add or change in the existing `.sap` file.

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_mode

Identifies the scope of the backup. This parameter is only used by `brbackup`. The default is `all`; however, if the parameter is set to `all` and Oracle RMAN is used, an incremental backup cannot be created. When the **backup_mode** parameter is set to `all`, a backup of all data files is completed using the `backint` interface.

For an incremental backup of an Oracle in an SAP environment database using Oracle RMAN, set the BR*Tools option for the **backup_mode** parameter to `full`.

backup_dev_type

Determines the backup medium that is used (the default is `tape`). To create a snapshot backup using Tivoli Storage FlashCopy Manager, this parameter must be set to `util_vol` or to `util_vol_online`. Minimize the time during which the database is degraded.

util_par_file

If you are running Tivoli Storage FlashCopy Manager with IBM Tivoli

Storage Manager for Enterprise Resource Planning, set this parameter to the fully qualified path of the IBM Tivoli Storage Manager for Enterprise Resource Planning profile (.utl file). This way Tivoli Storage FlashCopy Manager uses the configuration that was added to the IBM Tivoli Storage Manager for Enterprise Resource Planning configuration file (.utl file).

If you are running Tivoli Storage FlashCopy Manager in an environment where IBM Tivoli Storage Manager for Enterprise Resource Planning is not configured, set this parameter to the fully qualified path of the Tivoli Storage FlashCopy Manager profile. This way Tivoli Storage FlashCopy Manager uses the configuration that was added to the CLIENT section of the Tivoli Storage FlashCopy Manager profile.

util_path

Specifies the path to the backint executable.

If you are running Tivoli Storage FlashCopy Manager with IBM Tivoli Storage Manager for Enterprise Resource Planning, you do not need to set this parameter.

If you are running Tivoli Storage FlashCopy Manager in an environment where IBM Tivoli Storage Manager for Enterprise Resource Planning is not available, set this parameter to the INSTANCE_DIR (<Instance owner \$HOME directory>/acs/).

util_vol_unit

Specifies the smallest unit that can be backed up with a snapshot or clone, and also determines restore granularity. The possible values are sap_data (finest restore granularity), all_data, and all_dbf (not typically used).

Note: SAP requires that the setting of this parameter correctly describes the disk layout of your database.

If your disk layout consists of the following volume groups, use sap_data:

- At least one volume group for each sapdata directory
- At least one volume group for each origlog directory
- At least one volume group for each mirrlog directory

For sap_data, there must be exactly one volume group for each sapdata directory, exactly one volume group for each origlog directory, and exactly one volume group for each mirrlog directory. If one of the sap_data, origlog, or mirrlog directories contains more than one volume group, a fourth parameter value disk_vol must be used. The parameters disk_vol and all_dbf contradict the SAP recommendation about the separation of data files and redo log files. The default value set by SAP is sap_data.

If your disk layout consists of the following volume groups, use all_data:

- At least one volume group for sapdata
- At least one volume group for origlog
- At least one volume group for mirrlog

util_vol_access

Specifies the accessibility of snapshot backup volumes:

- none (required on the production system)
- copy (not supported)
- mount (required on the backup system if SAP BR*Tools that are installed on the backup system)
- both (not supported)

util_vol_nlist = (<nfile_name1>, <nfile_name2>, ...) | no_check

This parameter defines a list of non-database files or directories that are 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.

util_options = <additional_backint_options>

This parameter defines extra BACKINT options that BR*Tools places after the standard command-line options when calling the BACKINT program. With this parameter, the Tivoli Storage FlashCopy Manager backint options -O <TSM_BACKUP_FROM_SNAPSHOT value> and -S <device class> can be specified. For more information about backint options, see "BR*TOOLS - User interface for Oracle in an SAP environment" on page 275.

Example:

```
util_options = "-O yes -S STANDARD"
```

Tivoli Storage Manager option files used by Data Protection for Oracle

When using Data Protection for Oracle, the following Tivoli Storage Manager option files are used:

- Client system options (dsm.sys)
- Client user options (dsm.opt)
- Data Protection for Oracle options (tdpo.opt)
- RMAN backup script

Example 1 shows you how to configure the system options file (dsm.sys) to point to the same Tivoli Storage Manager.

In the following examples, the client user options file dsm.opt, stored in the /usr/tivoli/tsm/client/ba/bin and /usr/tivoli/tsm/client/api/bin directories, includes a server with the following TCP/IP address: *arrow.la.xyzcompany.com*. The servername option in the dsm.opt and dsm.sys files define the server stanza names only. The tcpserveraddress option indicates which server is contacted.

For the dsm.opt file that is stored in the /usr/tivoli/tsm/client/ba/bin directory, use the following example:

```
servername tdphdw
```

For the dsm.sys file that is stored in the /usr/tivoli/tsm/client/ba/bin directory, use the following example:

```
servername      tdphdw
commmethod      tcpip
tcpport         1500
```

```
tcpserveraddress arrow.la.xyzcompany.com
passwordaccess generate
schedmode prompted
nodename hdworc1
```

For the `dsm.opt` file that is stored in the `/usr/tivoli/tsm/client/api/bin` directory, use the following example:

```
servername tdporc
```

For the `dsm.sys` file that is stored in the `/usr/tivoli/tsm/client/api/bin` directory, use the following example:

```
servername tdporc
commmethod tcpip
tcpport 1500
tcpserveraddress arrow.la.xyzcompany.com
passwordaccess prompt
nodename hdworc1
```

Example 2 shows you how to configure multiple server stanzas in the system options file (`dsm.sys`).

To configure multiple server stanzas in the system options file (`dsm.sys`), copy the option settings from the Tivoli Storage Manager for Databases: Data Protection for Oracle `dsm.sys` file to the Tivoli Storage FlashCopy Manager `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
```

Appendix B. Examples

Refer to these Tivoli Storage FlashCopy Manager examples when you are configuring, updating, or following product tasks.

Examples (DB2)

Example overall disk layout for a DB2 environment

Refer to this example when you are configuring the disk layout for a DB2 environment.

The following figure shows file systems that are involved in an example disk layout.

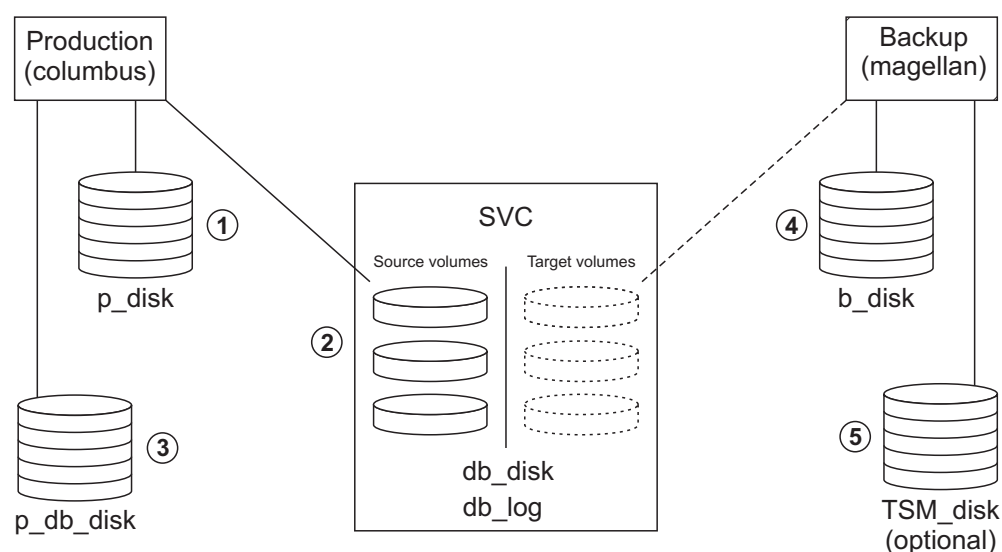


Figure 18. Example overall disk layout for a DB2 environment

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/sql1ib
 - /sapmnt/D01
 - /usr/sap/D01
 - /usr/sap/trans
 - /opt/IBM/db2/V10.5
 - /db2/D01/acs (ACS_DIR)
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. Local disks on the production system (p_db_disk category) for the file systems

```

/db2/D01/log_archive
/db2/D01/log_retrieve

```

4. Local disks on the backup system (b_disk category) for the file systems

```

/db2/D01
/opt/IBM/db2/V9.5
/db2/D01/acs (ACS_DIR)

```

5. Disks for the Tivoli Storage Manager server (TSM_disk category) for the file systems

```

/tsmdb

```

Example profile for Tivoli Storage FlashCopy Manager for DB2

The profile file provides parameters that customize how Tivoli Storage FlashCopy Manager works within a particular environment. Use this example to verify that the configuration of the profile is correct for your DB2 data partitioning environment.

The following sample profile is used for a DB2 DPF environment. The profile specifies that snapshots are completed from *06am* to *8pm* and snapshots with offloaded backups for the remaining time. These offloaded backups use two different SAN Volume Controller clusters, one from *00am* to *6am* and the other cluster from *8pm* to *12pm*. Each cluster is backed up by a separate backup system, even though that fact is not obvious in the example.

```

>>> GLOBAL
ACS_DIR /db2/D01/acs
ACSD acsprod5 57328
TRACE NO
<<<
>>> ACSD
ACS_REPOSITORY /db2/D01/acs/acsrepository
# ADMIN_ASSISTANT NO
# REPOSITORY_LABEL TSM
<<<
>>> OFFLOAD
BACKUP_METHOD DB2
OPTIONS @/db2/D01/tdp_r3/vendor.env
# PARALLELISM AUTO
# NUM_SESSIONS 1
# NUM_BUFFERS AUTO
# BUFFER_SIZE AUTO
<<<
>>> CLIENT
# BACKUPIDPREFIX DB2____
APPLICATION_TYPE DB2____
TSM_BACKUP YES
TSM_BACKUP NO USE_FOR SVC_NO_TSM
MAX_VERSIONS ADAPTIVE
# LVM_FREEZE_THAW AUTO
# NEGATIVE_LIST NO_CHECK
# TIMEOUT_FLASH 120
# GLOBAL_SYSTEM_IDENTIFIER

```

```

DEVICE_CLASS SVC2 FROM 00:00 TO 05:59
DEVICE_CLASS SVC_NO_TSM FROM 06:00 TO 20:00
DEVICE_CLASS SVC1 FROM 20:01
<<<

>>> DEVICE_CLASS SVC_NO_TSM
COPYSERVICES_HARDWARE_TYPE SVC
COPYSERVICES_PRIMARY_SERVERNAME 192.168.1.104
# COPYSERVICES_USERNAME superuser
# SVC_COPY_RATE 80
# SVC_CLEAN_RATE 50
# COPYSERVICES_COMMPROTOCOL HTTPS
# COPYSERVICES_CERTIFICATEFILE NO_CERTIFICATE
COPYSERVICES_SERVERPORT 5989
FLASHCOPY_TYPE COPY
# COPYSERVICES_TIMEOUT 6
# RESTORE_FORCE NO
STORAGE_SYSTEM_ID TSMDEVSVC2
TARGET_SETS VOLUMES_FILE
VOLUMES_FILE /db2/D01/acs/acsvolumes/fct.file
BACKUP_HOST_NAME PREASSIGNED_VOLUMES
<<<

>>> DEVICE_CLASS SVC1
COPYSERVICES_HARDWARE_TYPE SVC
COPYSERVICES_PRIMARY_SERVERNAME 192.168.1.101
# COPYSERVICES_USERNAME superuser
# SVC_COPY_RATE 80
# SVC_CLEAN_RATE 50
# COPYSERVICES_COMMPROTOCOL HTTPS
# COPYSERVICES_CERTIFICATEFILE NO_CERTIFICATE
# COPYSERVICES_SERVERPORT 5989
FLASHCOPY_TYPE INCR
# COPYSERVICES_TIMEOUT 6
# RESTORE_FORCE NO
STORAGE_SYSTEM_ID TSMDEVSVC1
TARGET_SETS VOLUMES_FILE
VOLUMES_FILE /db2/D01/acs/acsvolumes/fct.file
BACKUP_HOST_NAME PREASSIGNED_VOLUMES
<<<

>>> DEVICE_CLASS SVC2
COPYSERVICES_HARDWARE_TYPE SVC
COPYSERVICES_PRIMARY_SERVERNAME 192.168.1.104
# COPYSERVICES_USERNAME superuser
# SVC_COPY_RATE 80
# SVC_CLEAN_RATE 50
# COPYSERVICES_COMMPROTOCOL HTTPS
# COPYSERVICES_CERTIFICATEFILE NO_CERTIFICATE
COPYSERVICES_SERVERPORT 5989
FLASHCOPY_TYPE INCR
# COPYSERVICES_TIMEOUT 6
# RESTORE_FORCE NO
STORAGE_SYSTEM_ID TSMDEVSVC2
TARGET_SETS VOLUMES_file
VOLUMES_FILE /db2/D01/acs/acsvolumes/fct.file
BACKUP_HOST_NAME PREASSIGNED_VOLUMES
<<<

```

Example profile for Tivoli Storage FlashCopy Manager for DB2 pureScale

The profile file provides parameters that customize how Tivoli Storage FlashCopy Manager works within a particular environment. Use this example to verify that the configuration of the profile is correct for your DB2 pureScale environment.

This example contains a sample profile for backing up and restoring data in a DB2 pureScale environment.

```
>>> GLOBAL
ACS_DIR /db2/db2an1/acs
ACSD akuma 45454
# TRACE NO
<<<

>>> ACSD
ACS_REPOSITORY /db2/db2an1/acs/acsrepository
# REPOSITORY_LABEL TSM
<<<

>>> CLIENT
# BACKUPIDPREFIX DB2____
APPLICATION_TYPE DB2____
TSM_BACKUP YES
MAX_VERSIONS 5
# LVM FREEZE_THAW AUTO
# NEGATIVE_LIST NO_CHECK
# TIMEOUT_FLASH 120
# GLOBAL_SYSTEM_IDENTIFIER
# DEVICE_CLASS STANDARD
<<<

>>> OFFLOAD
BACKUP_METHOD DB2
VENDOR_LIB DB2_TSM_AGENT
# OPTIONS
# DB2_OPTIONS
# PARALLELISM AUTO
# NUM_SESSIONS 1
# NUM_BUFFERS AUTO
# BUFFER_SIZE AUTO
# NUMBER_BACKUPS_IN_PARALLEL 0
# DATABASE_MEMORY 0
<<<

>>> DEVICE_CLASS STANDARD
COPYSERVICES_HARDWARE_TYPE GPFS
NUMBER_GPFS_CONCURRENT_TASKS 10
<<<
```

Examples (Oracle)

Example overall disk layout for a Oracle environment

Refer to this example when configuring the disk layout in a Oracle environment.

The following figure shows file systems involved in a sample disk layout.

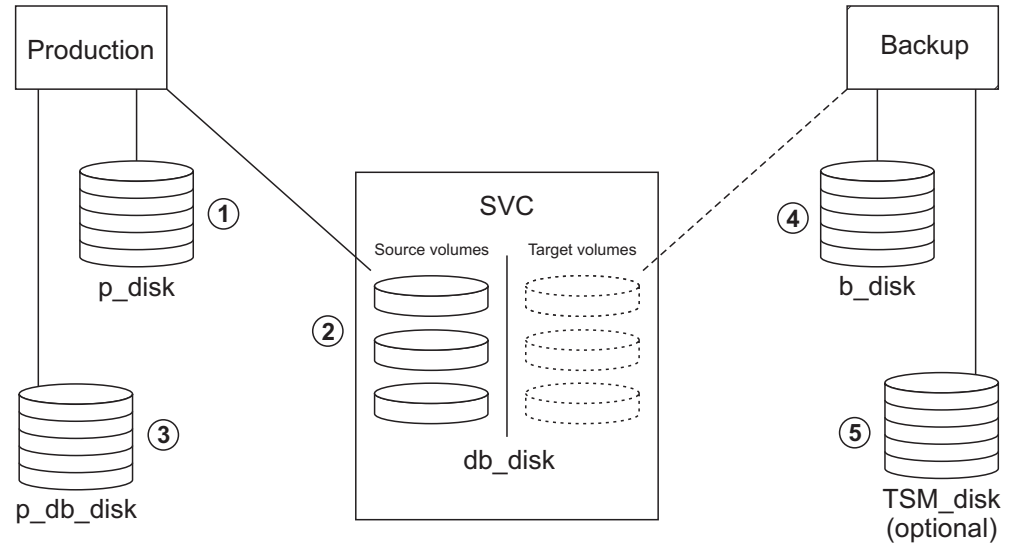


Figure 19. Example overall disk layout for a Oracle environment

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
/oracle/A01/acs  (ACS_DIR)
```

The Oracle database binary files are located in the directory that is defined by the ORACLE_HOME environment variable.

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_11
/oracle/A01/origlogB        part of VG ora_11
```

```
/oracle/A01/mirrlogA        part of VG ora_12
/oracle/A01/mirrlogB        part of VG ora_12
```

The file systems for the control files must not reside on volume groups that are part of the FlashCopy backup. For FlashCopy cloning at least one of the three Oracle control files must reside on a volume group that is part of the FlashCopy cloning operation.

```
/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. The p_db_disk category is not used for this setup.
4. Local disks on the backup system (b_disk category) for the file system

```
/oracle/A01
/oracle/A01/acs  (ACS_DIR)
```

There is no need to create separate volume groups for logs and control files.

Example profile for Tivoli Storage FlashCopy Manager for Oracle

The profile file provides parameters that customize how Tivoli Storage FlashCopy Manager works within a particular environment. Use this example to verify that the configuration of the profile is correct for your Oracle environment.

The following sample profile is provided for when Tivoli Storage FlashCopy Manager software backs up Oracle databases:

```
>>> 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
DATABASE_CONTROL_FILE_RESTORE NO        # YES | NO
<<<
>>> ACSD
ACS_REPOSITORY /oracle/A10/acs/acsrepository # *mandatory parameter*
# ADMIN_ASSISTANT NO                     # NO | <server> <port>
<<<
>>> DEVICE_CLASS STANDARD
COPYSERVICES_HARDWARE_TYPE SVC          # *mandatory parameter* SVC | DS8000 | XIV
COPYSERVICES_PRIMARY_SERVERNAME cim_srv #
TARGET_SETS VOLUMES_FILE # *mandatory parameter*
VOLUMES_FILE /oracle/A01/acs/volumes/volumes_file.fct
# 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
BACKUP_HOST_NAME NONE
<<<
```

Example profile for Tivoli Storage FlashCopy Manager for Oracle with ASM

The profile file provides parameters that customize how Tivoli Storage FlashCopy Manager works within a particular environment. Use this example to verify that the configuration of the profile is correct for your Oracle with ASM environment.

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        #
VOLUME_MGR ASM                  # ASM | LVM
<<<
>>> OFFLOAD
BACKUP_METHOD ORACLE            #
# OVERWRITE_DATABASE_PARAMETER_FILE YES # YES | NO
# DATABASE_BACKUP_INCREMENTAL_LEVEL 0    #
#ASM_INSTANCE_USER AUTO          # User name | AUTO
#ASM_INSTANCE_ID +ASM            # ASM instance SID | +ASM
#ASM_ROLE SYSDBA                # SYSDBA or SYSASM | SYSDBA
<<<
>>> 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
#ASM_INSTANCE_USER AUTO                # User name | AUTO
#ASM_INSTANCE_ID +ASM                  # ASM instance SID | +ASM
#ASM_ROLE SYSDBA                      # SYSDBA or SYSASM | SYSDBA
<<<
>>> ACSD
ACS_REPOSITORY /oracle/A10/acs/acsrepository # *mandatory parameter*
# ADMIN_ASSISTANT NO                     # NO | <server> <port>
<<<
>>> DEVICE_CLASS STANDARD
COPYSERVICES_HARDWARE_TYPE SVC          # *mandatory parameter* SVC | DS8000 | XIV
COPYSERVICES_PRIMARY_SERVERNAME cim_srv #
TARGET_SETS VOLUMES_FILE # *mandatory parameter*
VOLUMES_FILE /oracle/A01/acs/volumes/volumes_file.fct
# 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
BACKUP_HOST_NAME NONE
<<<
```

The **ASM_INSTANCE_USER**, **ASM_INSTANCE_ID**, and **ASM_ROLE SYSDBA** parameters in the OFFLOAD section contain values for the backup server. They can be commented out if the same parameters in the ORACLE section are also valid for the backup server.

Example of the RMAN backup script

Refer to this example when you are configuring Data Protection for Oracle on the backup server.

The RMAN backup script must be specified in the profile with the **DATABASE_BACKUP_SCRIPT_FILE** parameter. The example shows the required syntax of the RMAN backup script. The keyword backup must be entered on a single line of text without any other text as shown in this example. There must be a line break after the backup keyword.

```
run
{
    allocate channel 'c1' type 'sbt_tape' parms 'ENV=(TDPO_OPTFILE=/home/oracle/tdpo.opt)';
    backup
    (database);
    release channel c1;
}
```

Examples (SAP with Oracle)

Example overall disk layout for an Oracle in an SAP environment

Refer to this example when configuring the disk layout in an Oracle in an SAP environment.

The following figure shows file systems involved in a sample disk layout.

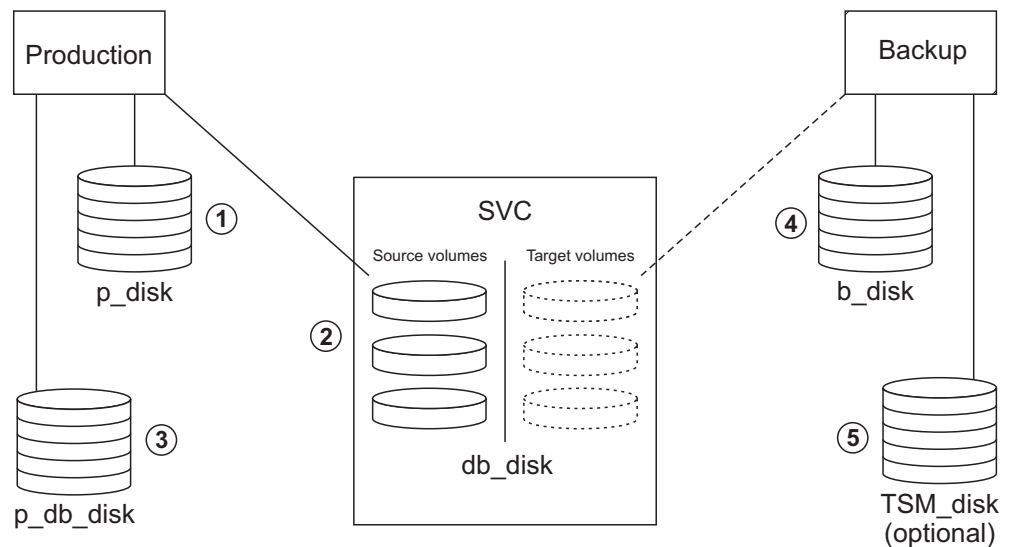


Figure 20. Example overall disk layout for an SAP with Oracle environment

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
/oracle/A01/920_64
```

```

/oracle/A01/sapbackup
/oracle/A01/sapreorg
/sapmnt/A01
/oracle/A01/acs (ACS_DIR)

```

2. Source volume disks on the production system (*db_disk* category) for the file systems

```

/oracle/A01/sapdata1      part of VG sapfc11
/oracle/A01/sapdata2      part of VG sapfc12
/oracle/A01/sapdata3      part of VG sapfc12
/oracle/A01/sapdata4      part of VG sapfc13
/oracle/A01/sapdata5      part of VG sapfc13
/oracle/A01/sapdata6      part of VG sapfc13

/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 and development purposes; they could also have been in a common one.

The Oracle control files are placed in \$ORACLE_HOME/dbs/init<SID>.ora.:

```

/oracle/A01/sapdata1/cntrl/cntrlA01.dbf
/oracle/A01/origlogA/cntrl/cntrlA01.dbf
/oracle/A01/origlogB/cntrl/cntrlA01.dbf

```

3. Local disks on the production system (*p_db_disk* category) for the file systems

```

/oracle/A01/saparch

```

4. Local disks on the backup system (*b_disk* category) for the file systems

```

/oracle/A01
/usr/sap/A01
/usr/sap/trans
/oracle/A01/acs (ACS_DIR)

```

5. (Tivoli Storage Manager 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 Tivoli Storage FlashCopy Manager for Oracle in an SAP environment (disk only)

The profile file provides parameters that customize how Tivoli Storage FlashCopy Manager works within a particular environment. Use this example to verify that the configuration of the profile is correct for your Oracle in an SAP environment.

The following depicts a sample profile:

```

>>> GLOBAL
# ACS_DIR /oracle/A01/acs
ACSD acsprod5 57328
# TRACE NO
<<<
>>> ACSD
ACS_REPOSITORY /oracle/A01/acs/pmtest
ADMIN_ASSISTANT no
# REPOSITORY_LABEL TSM
<<<
>>> CLIENT
# BACKUPIDPREFIX SAP__
APPLICATION_TYPE SAP_ORACLE
TARGET_DATABASE_SUSPEND YES
TSM_BACKUP YES
# MAX_VERSIONS ADAPTIVE
LVM_FREEZE_THAW 120

```

```

# TIMEOUT_FLASH 120
GLOBAL_SYSTEM_IDENTIFIER A01
# DEVICE_CLASS STANDARD
<<<
>>> DEVICE_CLASS STANDARD
COPYSERVICES_HARDWARE_TYPE XIV
# STORAGE_SYSTEM_ID
PATH_TO_XCLI /home/xivtest/XCLI
COPYSERVICES_SERVERNAME nextra
COPYSERVICES_USERNAME admin
# RECON_INTERVAL 12
# USE_WRITABLE_SNAPSHOTS AUTO
BACKUP_HOST_NAME acsback5
<<<

```

Example profile for Tivoli Storage FlashCopy Manager for Oracle in an SAP environment (offload)

The profile file provides parameters that customize how Tivoli Storage FlashCopy Manager works within a particular environment. Use this example to verify that the configuration of the profile is correct for an offloaded backup with IBM Tivoli Storage Manager for Enterprise Resource Planning.

Some parameters that are typically defined within the Tivoli Storage FlashCopy Manager profile are defined in the IBM Tivoli Storage Manager for Enterprise Resource Planning .utl file, with some parameters under different names.

The following profile is an example of a Oracle in an SAP environment profile that does not contain a CLIENT section:

```

>>> GLOBAL
# ACS_DIR /oracle/CET/acs
ACSD dooku 62000
TRACE YES
<<<

>>> ACSD
ACS_REPOSITORY /oracle/CET/acs/repository
# ADMIN_ASSISTANT NO
REPOSITORY_LABEL CET
<<<

>>> OFFLOAD
BACKUP_METHOD BACKINT
PROFILE /oracle/oracle11R2/dbs/initCET.utl
<<<

>>> DEVICE_CLASS STANDARD
COPYSERVICES_HARDWARE_TYPE SVC
COPYSERVICES_PRIMARY_SERVERNAME 192.168.1.104
# COPYSERVICES_USERNAME superuser
SVC_COPY_RATE 95
# SVC_CLEAN_RATE 50
# COPYSERVICES_COMMPROTOCOL HTTPS
# COPYSERVICES_CERTIFICATEFILE NO_CERTIFICATE
# COPYSERVICES_SERVERPORT 5989
FLASHCOPY_TYPE COPY
# COPYSERVICES_TIMEOUT 6
# RESTORE_FORCE NO
# STORAGE_SYSTEM_ID
# RECON_INTERVAL 12
BACKUP_HOST_NAME bano
TARGET_SETS T1
TARGET_NAMING %SOURCE_%TARGETSET
<<<

```

The following excerpt is an example of the GLOBAL and CLIENT sections in a .utl file:

```
...
### TSM4ERP parameters
MAX_SESSIONS ...
CONFIG_FILE ...
BACKUPIDPREFIX CET___
...
### FlashCopy Manager parameters
ACS_DIR /oracle/CET/acs/
ACSD dooku 62000
TRACE ON
...
TARGET_DATABASE_SUSPEND YES
LVM_FREEZE_THAW AUTO
TSM_BACKUP_FROM_SNAPSHOT YES
MAX_SNAPSHOT_VERSIONS ADAPTIVE
DEVICE_CLASS STANDARD
...
### TSM4ERP server section parameters
SERVER ...
SESSIONS ...
```

The following example depicts the situation when the two profiles are created for the same database instance:

```
>>> GLOBAL
# ACS_DIR /oracle/CET/acs
ACSD dooku 62000
TRACE NO
<<<

>>> ACSD
ACS_REPOSITORY /oracle/CET/acs/repository
# ADMIN_ASSISTANT NO
REPOSITORY_LABEL CET
<<<

>>> CLIENT
BACKUPIDPREFIX CET___
APPLICATION_TYPE SAP_ORACLE
TARGET_DATABASE_SUSPEND NO
# MAX_VERSIONS ADAPTIVE
# LVM_FREEZE_THAW AUTO
# TIMEOUT_FLASH 120
# GLOBAL_SYSTEM_IDENTIFIER
# DEVICE_CLASS STANDARD
<<<

>>> DEVICE_CLASS STANDARD
COPYSERVICES_HARDWARE_TYPE SVC
COPYSERVICES_PRIMARY_SERVERNAME 192.168.1.104
# COPYSERVICES_USERNAME superuser
# CLONE_DATABASE NO
# SVC_COPY_RATE 80
# SVC_CLEAN_RATE 50
# COPYSERVICES_COMMPROTOCOL HTTPS
# COPYSERVICES_CERTIFICATEFILE NO_CERTIFICATE
# COPYSERVICES_SERVERPORT 5989
FLASHCOPY_TYPE INCR
# COPYSERVICES_TIMEOUT 6
# RESTORE_FORCE NO
# STORAGE_SYSTEM_ID
# RECON_INTERVAL 12
```

```

BACKUP_HOST_NAME BANO
TARGET_SETS T1 T2 T3 T4
TARGET_NAMING %SOURCE_%TARGETSET
<<<

```

Example profile for Tivoli Storage FlashCopy Manager for Oracle in an SAP environment incremental (offload)

Refer to this example when editing the IBM Tivoli Storage Manager for Enterprise Resource Planning profile (.utl file) for an off-loaded backup using Tivoli Storage Manager for ERP with Oracle RMAN.

The following excerpt is an example of a Tivoli Storage Manager for ERP profile (.utl file) that can be used on the production and backup server:

```

...
BACKUPIDPREFIX          TPR__

INCREMENTAL              DIFFERENTIAL
INCREMENTAL_CHANNELS     2
INCREMENTAL_LEVEL        1 USE_AT MON TUE WED Thu Fri Sat
INCREMENTAL_LEVEL        0 USE_AT SUN
INCREMENTAL_CATALOG_CONNECT_STRING catdb
INCREMENTAL_CATALOG_USER rman

TARGET_DATABASE_SUSPEND NO

MAX_SESSIONS             2
MAX_ARCH_SESSIONS        1
RL_COMPRESSION            0
REDOLOG_COPIES           2
MAX_VERSIONS             2

BUFFCOPY                 PREVENT
BUFFSIZE                 131072          # block size in bytes
REPORT                   5              # all additional messages + summary
CONFIG_FILE              /oracle/TPR/102_32/dbs/initTPR.bki

SERVER                   PYXIS_1          # Servername
SESSIONS                 2              # Max sessions
PASSWORDREQUIRED         YES            # Use a password
ADSMNODE                 TPR_ORA102_LNX  # Tivoli Storage Manager Nodename
BRBACKUPMGTCCLASS        MBDISK1        # Mgmt-Classes
BRARCHIVEMGTCCLASS       MLOG1 MLOG2    # Mgmt-Classes

```

Example target volumes files

Example target volumes file DS8000 configuration

Refer to this example when you are editing the target volumes file for a DS8000 storage subsystem configuration.

The following file is an example of a VOLUMES_FILE .fct file that includes the target set configuration that is used for cloning:

```

#
#***** First sample *****#
#
#=====#

>>> TARGET_SET 1
>>> PARTITION NODE0000
TARGET_VOLUME 13ABCTA0111 - -

```

```

TARGET_VOLUME 13ABCTA0112 - -
TARGET_VOLUME 13ABCTA0113 - -
<<<
<<<

>>> TARGET_SET 3

DEVICE_CLASS CLONE USE_FOR_CLONING D98
>>> PARTITION NODE0000
TARGET_VOLUME 13ABCTA011D - -
TARGET_VOLUME 13ABCTA011E - -
TARGET_VOLUME 13ABCTA011F - -
<<<
<<<

#=====#

```

The following file shows a VOLUMES_FILE .fct file for DB2 EEE configurations:

```

#
#***** Second sample *****#
#
#=====#

>>> TARGET_SET 1

DEVICE_CLASS CLONE USE_FOR_CLONING S98
>>> PARTITION NODE0000
    TARGET_VOLUME S97p5d1_t1 - -
    TARGET_VOLUME S97p5d2_t1 - -
<<<
>>> PARTITION NODE0001
    TARGET_VOLUME S97p5d3_t1 - -
    TARGET_VOLUME S97p5d4_t1 - -
<<<
>>> PARTITION NODE0002
    TARGET_VOLUME S97p511_t1 - -
    TARGET_VOLUME S97p512_t1 - -
<<<
>>> PARTITION NODE0003
    TARGET_VOLUME S97p513_t1 - -
    TARGET_VOLUME S97p514_t1 - -
<<<
<<<

#=====#

```

Example target volumes file (SAN Volume Controller configuration or Storwize family)

Refer to this example when you are editing the target volumes file for an SAN Volume Controller or Storwize family storage system configuration.

```

#***** First sample *****#
#
#=====#

>>> TARGET_SET VOLUMES_SET_1
TARGET_VOLUME svdftgt1 svdrsrc2 -
TARGET_VOLUME svdftgt2 svdfsrc3 -
TARGET_VOLUME svdftgt3 svdfsrc4 -
TARGET_VOLUME svdftgt4 svdfsrc5 -
TARGET_VOLUME svdftgt5 svdfsrc6 -
<<<

#=====#

```

The following sample profile is an example of a profile in a non-mirrored environment. Create three space-efficient disk-only backups and one dual backup, at midnight, per day.

```
>>> CLIENT
...
TSM BACKUP LATEST USE FOR DISK TSM
DEVICE_CLASS DISK_ONLY FROM 5:30 TO 23:59
DEVICE_CLASS DISK_TSM FROM 0:00 TO 05:29
<<<
>>> DEVICE_CLASS DISK_ONLY
COPYSERVICES_HARDWARE_TYPE SVC
FLASHCOPY_TYPE NOCOPY # space efficient targets
TARGET_SETS 1 2 3
TARGET_NAMING %SOURCE_%TARGETSET
...
<<<
>>> DEVICE_CLASS DISK_TSM
COPYSERVICES_HARDWARE_TYPE SVC
FLASHCOPY_TYPE NOCOPY # space efficient targets
TARGET_SETS DUAL
TARGET_NAMING %SOURCE_%TARGETSET
...
<<<
```

This scenario illustrates a profile in a mirrored environment. On MIRROR_1, two space-efficient FlashCopy backups are created on Monday, Wednesday, and Friday. The backup that is created at midnight is copied to Tivoli Storage Manager. The backup that is created at noon is retained only on disk. The backup that is created on Monday is retained until the target sets are reused on Wednesday. On MIRROR_2, only one incremental FlashCopy backup was created on Sunday, Tuesday, Thursday, and Saturday. This backup is also copied to Tivoli Storage Manager. The backup is retained until the next incremental backup is started.

```
>>> CLIENT
...
TSM BACKUP LATEST USE FOR MIRROR_1 DISK_TSM MIRROR_2
DEVICE_CLASS MIRROR_1_DISK_ONLY USE_AT Mon Wed Fri FROM 5:30 TO 23:59
DEVICE_CLASS MIRROR_1_DISK_TSM USE_AT Mon Wed Fri FROM 0:00 TO 05:29
DEVICE_CLASS MIRROR_2_USE_AT SUN Tue Thu Sat
<<<
>>> DEVICE_CLASS MIRROR_1_DISK_ONLY
COPYSERVICES_HARDWARE_TYPE SVC
FLASHCOPY_TYPE NOCOPY # space efficient targets
TARGET_SETS DO
TARGET_NAMING %SOURCE_%TARGETSET
...
<<<
>>> DEVICE_CLASS MIRROR_1_DISK_TSM
COPYSERVICES_HARDWARE_TYPE SVC
FLASHCOPY_TYPE NOCOPY # space efficient targets
TARGET_SETS DT
TARGET_NAMING %SOURCE_%TARGETSET
...
<<<
>>> DEVICE_CLASS MIRROR_2
COPYSERVICES_HARDWARE_TYPE SVC
FLASHCOPY_TYPE INCR
TARGET_SETS 1
TARGET_NAMING %SOURCE_%TARGETSET
...
<<<
```

This example is like the previous example, but the example does not create Tivoli Storage Manager backups from MIRROR_1. Rather, the example retains the space-efficient FlashCopy images for one week (same schedule).

```
>>> CLIENT
...
TSM BACKUP LATEST USE_FOR MIRROR_1 DISK_TSM MIRROR_2
DEVICE_CLASS MIRROR_1_DISK_ONLY USE_AT Mon Wed Fri
DEVICE_CLASS MIRROR_2 USE_AT Sun Tue Thu Sat
<<<
>>> DEVICE_CLASS MIRROR_1_DISK_ONLY
COPYSERVICES_HARDWARE_TYPE SVC
FLASHCOPY_TYPE NOCOPY # space efficient targets
TARGET_SETS 1A 1B 3A 3B 5A 5B
TARGET_NAMING %SOURCE_%TARGETSET
...
<<<
>>> DEVICE_CLASS MIRROR_2
COPYSERVICES_HARDWARE_TYPE SVC
FLASHCOPY_TYPE INCR
TARGET_SETS 1
TARGET_NAMING %SOURCE_%TARGETSET
...
<<<
```

Example target volume file

The following sample shows a configuration of SAP in a multi-partition DB2 environment.

ACS_DIR/profile:

```
>>> DEVICE_CLASS STANDARD
...
TARGET_SETS VOLUMES_FILE
VOLUMES_FILE <ACS_DIR>/acsvolumes/volumes_file.fct
<<<
```

ACS_DIR/acsvolumes/volumes_file.fct:

```
>>> TARGET_SET 1
>>> PARTITION NODE0000
TARGET_VOLUME J01acs_td_0
TARGET_VOLUME J01acs_tl_0
<<<

>>> PARTITION NODE0001
TARGET_VOLUME J01acs_td_1
TARGET_VOLUME J01acs_tl_1
<<<

>>> PARTITION NODE0002
TARGET_VOLUME J01acs_td_2
TARGET_VOLUME J01acs_tl_2
<<<

>>> PARTITION NODE0003
TARGET_VOLUME J01acs_td_3
TARGET_VOLUME J01acs_tl_3
<<<
<<<

>>> TARGET_SET 2
>>> PARTITION NODE0000
TARGET_VOLUME J01acs_td_2_0
TARGET_VOLUME J01acs_tl_2_0
```

```

<<<

>>> PARTITION NODE0001
TARGET_VOLUME J01acs_td_2_1
TARGET_VOLUME J01acs_t1_2_1
<<<

>>> PARTITION NODE0002
TARGET_VOLUME J01acs_td_2_2
TARGET_VOLUME J01acs_t1_2_2
<<<

>>> PARTITION NODE0003
TARGET_VOLUME J01acs_td_2_3
TARGET_VOLUME J01acs_t1_2_3
<<<
<<<

```

Example profile for custom applications

This example contains a sample profile for backing up and restoring data in a custom application environment.

```

>>> GLOBAL
# ACS_DIR /home/gbauer/acs
ACSD ehonda 61000
TRACE YES
<<<

>>> ACSD
ACS_REPOSITORY /home/gbauer/acs/repository
REPOSITORY_LABEL GBA
<<<

>>> OFFLOAD
BACKUP_METHOD TSM_CLIENT
# MODE FULL
ASNODENAME GBA_aha_target
# DSM_DIR
# DSM_CONFIG
# VIRTUALFSNAME fcm
<<<

>>> CLIENT
BACKUPIDPREFIX GBA_
APPLICATION_TYPE GENERIC
INFILE /home/gbauer/acs/infile
PRE_FLASH_CMD /home/gbauer/acs/scripts/preflash.cmd
POST_FLASH_CMD /home/gbauer/acs/scripts/postflash.cmd
TSM_BACKUP YES
# MAX_VERSIONS ADAPTIVE
# LVM_FREEZE_THAW AUTO
NEGATIVE_LIST NO_CHECK
# TIMEOUT_FLASH 120
# GLOBAL_SYSTEM_IDENTIFIER
DEVICE_CLASS STANDARD
<<<

>>> DEVICE_CLASS STANDARD
COPYSERVICES_HARDWARE TYPE SVC
COPYSERVICES_PRIMARY_SERVERNAME 192.168.1.101
# COPYSERVICES_USERNAME superuser
# CLONE_DATABASE NO
SVC_COPY_RATE 90
# SVC_CLEAN_RATE 50
# COPYSERVICES_COMMPROTOCOL HTTPS
# COPYSERVICES_CERTIFICATEFILE NO_CERTIFICATE

```

```
# COPYSERVICES_SERVERPORT 5989
FLASHCOPY_TYPE INCR
# COPYSERVICES_TIMEOUT 6
# RESTORE_FORCE NO
# STORAGE_SYSTEM_ID
# RECON_INTERVAL 12
BACKUP_HOST_NAME sagat
TARGET_SETS TS1 TS2 TS3
TARGET_NAMING %SOURCE_%TARGETSET
<<<
```

Example profile for a DB2 HADR standby server environment

This example contains a sample profile that shows configuration parameters for a DB2 HADR standby server.

```
>>> GLOBAL
ACS_DIR /db2/CET/acs
ACSD ehonda 63000
TRACE YES
<<<

>>> ACSD
ACS_REPOSITORY /db2/CET/acs/acsrepository
REPOSITORY_LABEL CET
<<<

>>> CLIENT
BACKUPIDPREFIX CET___
APPLICATION_TYPE DB2
# MAX_VERSIONS ADAPTIVE
# LVM_FREEZE_THAW AUTO
# NEGATIVE_LIST NO_CHECK
# TIMEOUT_FLASH 120
# GLOBAL_SYSTEM_IDENTIFIER
# DEVICE_CLASS STANDARD
<<<

>>> DB2STANDBY
DB2_PRODUCTIVE_SERVER akuma 60050
DB2_ALIAS CET
PRE_FLASH_CMD /db2/CET/acs/scripts/pre_flash_cmd
POST_FLASH_CMD /db2/CET/acs/scripts/post_flash_cmd
# DB2_USERNAME db2cet
DB2_AUTH_TYPE SERVER
<<<

>>> DEVICE_CLASS STANDARD
COPYSERVICES_HARDWARE_TYPE SVC
COPYSERVICES_PRIMARY_SERVERNAME 192.168.1.104
# COPYSERVICES_USERNAME superuser
# CLONE_DATABASE NO
SVC_COPY_RATE 95
# SVC_CLEAN_RATE 50
# COPYSERVICES_COMMPROTOCOL HTTPS
# COPYSERVICES_CERTIFICATEFILE NO_CERTIFICATE
# COPYSERVICES_SERVERPORT 5989
FLASHCOPY_TYPE INCR
# COPYSERVICES_TIMEOUT 6
# RESTORE_FORCE NO
# STORAGE_SYSTEM_ID
# RECON_INTERVAL 12
BACKUP_HOST_NAME sagat
TARGET_SETS TS1 TS2
TARGET_NAMING %SOURCE_%TARGETSET
<<<
```

Appendix C. Administrative commands

You can use commands to administer Tivoli Storage FlashCopy Manager.

Administrative commands are available for you to do the following tasks:

- Start, stop, or configure Tivoli Storage FlashCopy Manager.
- Mount or unmount a snapshot backup on a secondary system.
- Create a backup to Tivoli Storage Manager from a snapshot if you have Tivoli Storage Manager configured in your environment

To use the commands to automate operations for Tivoli Storage FlashCopy Manager, add entries to the cron table (crontab) file. Because there are so many ways to implement Tivoli Storage FlashCopy Manager software, there are no templates. To automate operations, either specify the commands in the crontab file, or create scripts and add the scripts to the crontab file.

Configuration commands

Use configuration commands to run the setup script, maintain Tivoli Storage FlashCopy Manager passwords, and query the amount of storage space that is used for backups.

Installation setup script

The setup script provides instructions for configuration. The setup script is used by the Tivoli Storage FlashCopy Manager installation program. The setup script can also be used to manually set up Tivoli Storage FlashCopy Manager and to complete a basic configuration.

The setup script uses the following command syntax:

```
setup_type.sh -a action -d Instance_owner_$HOME directory
```

For the *type* parameter, in the setup script name, the following values can be specified:

- setup_db2.sh
- In an IBM DB2 pureScale environment: setup_db2.sh [-hosts [all | host1, host2, host3]]
- setup_ora.sh
- setup_gen.sh

In a DB2 pureScale environment, Tivoli Storage FlashCopy Manager by default updates the instance shared file system that stores the instance shared data for all host members. Using the -hosts option, you can omit host members from the configuration process.

You can use the setup script for the following purposes:

- Activation or upgrade of Tivoli Storage FlashCopy Manager for one instance-specific installation, as root user:

```
setup_type.sh -a install -d Instance_owner_$HOME_directory
```

The setup script is run from the *FCM_INSTALL_DIR* directory.

- Initial configuration and reconfiguration:

```
setup_type.sh
```

The setup script must be run as the database instance owner. For custom applications, run the script as the application backup user. Run the script from the *INSTANCE_DIR* directory.

- Initial configuration and reconfiguration in advanced mode:

```
setup_type.sh -advanced
```

- Stopping an activated instance:

```
setup_type.sh -a stop -d Instance_owner_$HOME directory
```

The command must run as the database instance owner. For custom applications, run the command as the application backup user. The command must be run from the *INSTANCE_DIR* directory.

- Starting an activated instance:

```
setup_type.sh -a start -d Instance_owner_$HOME directory
```

The command must be run as the database instance owner. For custom applications, run the command as application backup user. The command must be run from the *INSTANCE_DIR* directory.

- Disabling a stopped instance:

```
setup_type.sh -a disable -d Instance_owner_$HOME_directory
```

The command must be run as the database instance owner. For custom applications, run the command as the application backup user. The command must be run from the *INSTANCE_DIR* directory. This command completely removes the entries from the */etc/inittab*.

For a typical configuration, these commands are run on a production system. There are some scenarios where these commands need to be run on a backup system. If you are running the commands on both systems, when you stop or disable Tivoli Storage FlashCopy Manager, run the command on the production system before the backup system.

The setup script can be used to install Tivoli Storage FlashCopy Manager on multiple backup nodes from the production server. As a prerequisite, Open Secure Shell (OpenSSH) must be installed on all of the nodes in the backup server. NFS shares between the production server and backup server nodes are not required for this type of remote installation. OpenSSH is the preferred method for Tivoli Storage FlashCopy Manager.

The script must be run from the database instance-specific installation directory:

- (DB2) *Instance owner \$HOME directory/sqllib/acs/*
- (Oracle) *Instance owner \$HOME directory/acs/*

The default action, *setup*, is performed and the instance is configured.

For FlashCopy Manager for Custom Applications, there is no database instance-specific directory. The script must be run from the *\$HOME* directory of the backup user. The backup user needs to be able to access all file systems that are going to be protected.

If the script is called without parameters, it can be issued as the instance owner. The script creates a profile or changes an existing profile, and updates

/etc/inittab according to the current profile (production system) or user preference (backup system). Updates to inittab require starting and stopping Tivoli Storage FlashCopy Manager as intermediate steps. This call cannot stop the Tivoli Storage FlashCopy Manager on the backup system if the following conditions are present:

- Tivoli Storage FlashCopy Manager is running on the production system
- The binary files in the instance-specific installation directory are NFS-shared between the production and backup systems.

If Tivoli Storage FlashCopy Manager cannot be stopped, stop Tivoli Storage FlashCopy Manager on the production system before you run the script with the `-a install -d Instance_owner_$HOME_directory` options.

Installation setup script for DB2 pureScale

The **setup_db2.sh** command is used to configure Tivoli Storage FlashCopy Manager in an IBM DB2 pureScale environment. Use the **setup_db2.sh** to run common commands in a DB2 pureScale cluster environment.

The setup script uses the following command syntax:

```
setup_db2.sh [-hosts [ all | host1, host2, host3 ]]
```

After you install Tivoli Storage FlashCopy Manager, the binary files are deployed to `/usr/tivoli/tsfcm/acs_VERSION`.

After the deployment, the setup script automatically starts with the root user ID and copies the necessary files to the instance-specific directory. Configure Tivoli Storage FlashCopy Manager by running the command **setup_db2.sh [-hosts [all | host1, host2, host3]]** from the command line with or without the `-hosts` option. The `-hosts` option is used to specify either all hosts or to specify individual host names. The local host must be included in the **[-hosts]** list when you run the script for the first time. The hosts are configured for Tivoli Storage FlashCopy Manager high availability in a DB2 pureScale clustered environment. In a DB2 pureScale environment, if the `-hosts` option is not specified, all hosts in the cluster are configured for Tivoli Storage FlashCopy Manager high availability.

The setup script is used to run the following actions:

- Use the **start** action to start Tivoli Storage FlashCopy Manager in a DB2 pureScale cluster. Enter the command on one line:

```
setup_db2.sh -a start [-hosts [ all | host1, host2, host3 ]] -d
Instance_owner_$HOME_directory
```

The command must be run as the database instance owner and must be run from the `INSTANCE_DIR` directory. This command starts `acsd`, `acsgen`, and `tsm4acs` daemons in high availability mode, and activates Tivoli Storage FlashCopy Manager high availability mode on all DB2 pureScale hosts or on a subset of hosts if specified. This command adds entries to the systems inittab file.

- Use the **stop** action to stop the Tivoli Storage FlashCopy Manager in a DB2 pureScale cluster. Enter the command on one line:

```
setup_db2.sh -a stop [-hosts [ all | host1, host2, host3 ]] -d
Instance_owner_$HOME_directory
```

The command must be run as the database instance owner and must be run from the `INSTANCE_DIR` directory. This command stops `acsd`, `acsgen`, and `tsm4acs` daemons for all DB2 pureScale hosts or on the subset of hosts if specified. Any

host where the daemons are stopped is no longer available in the event of a failover. This option can be used to temporarily disable Tivoli Storage FlashCopy Manager on specified hosts. However, the host names are not deleted from the host list and can be restarted with the `setup_db2.sh -a start` command. The host list contains a list of Tivoli Storage FlashCopy Manager enabled hosts in a DB2 pureScale environment. The same list is maintained on the backup server.

- Use the **install** action to add a Tivoli Storage FlashCopy Manager member to a DB2 pureScale cluster. Enter the command on one line:

```
setup_db2.sh -a install [-hosts [ all | host1, host2, host3 ]] -d
Instance_owner_$HOME_directory
```

The command must be run by the database instance owner and must be run from the `INSTANCE_DIR` directory. This command activates all hosts or a subset of hosts if specified. Tivoli Storage FlashCopy Manager must already be installed on the DB2 pureScale production cluster. The host names are also added to the host list on the backup system.

- Use the **disable** action to remove a Tivoli Storage FlashCopy Manager member from a DB2 pureScale cluster. Enter the command on one line:

```
setup_db2.sh -a disable [-hosts [ all | host1, host2, host3 ]] -d
Instance_owner_$HOME_directory
```

The command must be run as the database instance owner and must be run from the `INSTANCE_DIR` directory. This command completely removes the entries from the systems `/etc/inittab` file and you cannot run the `setup_db2.sh -a start` command to restart the host. The command also removes the host names from the host list on the backup system. Before you remove a host from a DB2 pureScale cluster, use this command to remove the specific Tivoli Storage FlashCopy Manager host member from the cluster.

- Use the **status** action to query the status of Tivoli Storage FlashCopy Manager daemons in a DB2 pureScale cluster:

```
setup_db2.sh -a status -d Instance_owner_$HOME_directory
```

The command shows the following information:

- The member hosts where the Tivoli Storage FlashCopy Manager daemons are running.
- All DB2 pureScale member hosts where Tivoli Storage FlashCopy Manager can run.
- The member hosts where Tivoli Storage FlashCopy Manager is temporarily stopped.

For example:

```
dbuser@machine:] ./setup_db2.sh -a status
acsd production3 57328
acsgen production1
tsm4acs production3
```

```
DB2 pureScale member hosts: production1, production2, production3, production4
FCM enabled hosts: production1, production2, production3
dbuser@machine:]
```

Setup script values

The following values are available for `setup_type.sh`.

setup_db2.sh

Configures Tivoli Storage FlashCopy Manager.

setup_ora.sh

Configures Tivoli Storage FlashCopy Manager for Oracle or Tivoli Storage FlashCopy Manager for Oracle in an SAP environment.

setup_gen.sh

Configures FlashCopy Manager for Custom Applications.

The following values are available for action:

disable

This call can be issued as the root or instance owner. It stops Tivoli Storage FlashCopy Manager and removes all entries from `/etc/inittab`. To reactivate Tivoli Storage FlashCopy Manager, call the script without parameters.

This call cannot stop Tivoli Storage FlashCopy Manager on the backup system if the following conditions are present:

- Tivoli Storage FlashCopy Manager is running on the production system
- The binary files in the instance-specific installation directory are NFS-shared between the production and backup systems.

If Tivoli Storage FlashCopy Manager cannot be stopped, stop Tivoli Storage FlashCopy Manager on the production system before running `setup_type.sh -a install -d <Instance owner $HOME directory>`. For DB2 databases, change `<INSTANCE owner $HOME directory>` to `<INSTANCE owner $HOME directory>/sqlib`.

install

This call needs to be issued with the root user ID. When issued, the following actions are completed:

1. Stops Tivoli Storage FlashCopy Manager (`setup_type.sh -a stop -d <Instance owner $HOME directory>`) For DB2 databases, change `<INSTANCE owner $HOME directory>` to `<INSTANCE owner $HOME directory>/sqlib`.
2. Copies all binary files from the Tivoli Storage FlashCopy Manager installation directory to the instance-specific installation directory (`INSTANCE_DIR`)
3. Sets the appropriate access rights for the binary files
4. Restarts Tivoli Storage FlashCopy Manager (`setup_type.sh -a start -d <Instance owner $HOME directory>`). For DB2 databases, change `<INSTANCE owner $HOME directory>` to `<INSTANCE owner $HOME directory>/sqlib`.

The steps to start and stop Tivoli Storage FlashCopy Manager are skipped if Tivoli Storage FlashCopy Manager is not configured.

This call cannot stop Tivoli Storage FlashCopy Manager on the backup system if the following conditions are present:

- Tivoli Storage FlashCopy Manager is running on the production system
- The binary files in the instance-specific installation directory are NFS-shared between the production and backup systems.

If Tivoli Storage FlashCopy Manager cannot be stopped, stop Tivoli Storage FlashCopy Manager on the production system before running `setup_type.sh`

`-a install -d <Instance owner $HOME directory>`. For DB2 databases, change `<INSTANCE owner $HOME directory>` to `<INSTANCE owner $HOME directory>/sqlib`.

start

This call can be issued as the root or instance owner. The call starts a previously installed and configured version of Tivoli Storage FlashCopy Manager. This call starts different entries in `/etc/inittab`, by changing the action for the existing entries to *respawn*, depending on whether the call is issued on the backup or production system.

stop

This call can be issued as the root or instance owner. It stops the version of Tivoli Storage FlashCopy Manager that is currently running. This call updates `/etc/inittab` and checks that Tivoli Storage FlashCopy Manager is stopped successfully (a write lock can be acquired for the `.lock` file that is located in the instance-specific installation directory).

This call fails on the backup system in environments where the instance-specific installation directory is shared between the production and backup systems, if Tivoli Storage FlashCopy Manager is running on the production system. To successfully stop Tivoli Storage FlashCopy Manager in those environments, stop Tivoli Storage FlashCopy Manager on the production system.

The instance directory name (`-d` option) is required for all explicit actions. This option is not required for the default setup function.

Setting or changing passwords with the setup script

You can set or change passwords by issuing the setup script without the `-a` action option.

Use the command in this example:

```
setup_type.sh
```

Running the setup script without the `-a` action option proceeds through several tasks that are similar to the tasks described in Chapter 3, “Installing and upgrading,” on page 39.

When this command is issued, the profile wizard starts. You can use the profile wizard to edit the profile, and to set or change passwords. Using this wizard to administer passwords is preferred because the wizard updates changed passwords on the backup systems. To update passwords on the backup system, specify *YES* at the following prompt:

Select the backup system to update or delete:

- 1) acsback5
- n) configure a new backup system
- b) return to previous menu
- q) quit configuration

Select one of the options.

1

The selected backup system is acsback5

The backup system on acsback5 is configured with the device class(es) `DISK_ONLY`.

Select the action you want to take on the backup system acsback5:

- 1) update IBM Tivoli Storage FlashCopy Manager installation
- 2) start IBM Tivoli Storage FlashCopy Manager services
- 3) stop IBM Tivoli Storage FlashCopy Manager
- 4) uninstall IBM Tivoli Storage FlashCopy Manager

```

5) setup the SSH key authentication
b) return to backup system selection
q) quit the configuration
Select one of the options.
1
Do you want to update the Backup System installation on acsback5? [y|n] [y]

```

Password administration

You can use the `setup.sh` script or the `fccli -f password` command to change the Tivoli Storage FlashCopy Manager passwords.

The `fccli -f password` command supports an interactive and a non-interactive mode. To use the interactive mode, do not enter a password when you issue the command and you are prompted to enter the following passwords:

- The master password, which is the password of the acsd management agent. By default, a 32 character password is automatically generated. However, you can enter an alternative password.
- The password for the ORACLE section if defined in the specified profile.
- The password for the DB2STANDBY section if defined in the specified profile.
- The passwords for the disk storage subsystems that are referenced by the `DEVICE_CLASS` sections in the specified profile.

If the specified profile contains multiple `DEVICE_CLASS` sections that reference the same physical disk storage subsystem, the password is queried one time by combining these `DEVICE_CLASS` sections.

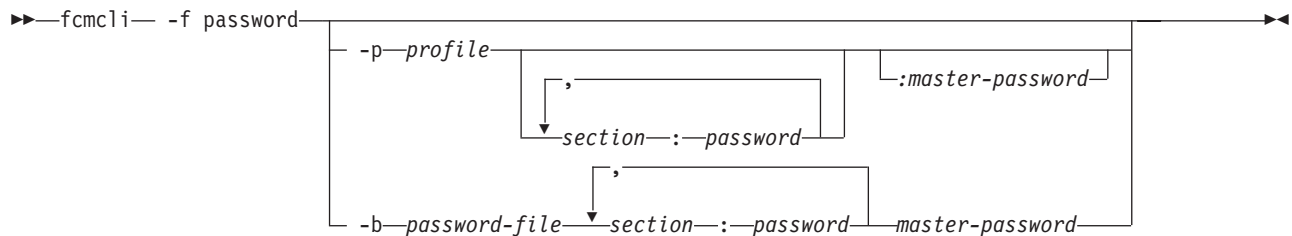
The interactive mode is the preferred method for setting passwords. Using this method, the passwords are verified by testing the connections to the corresponding storage devices, management agent, or database. For the non-interactive mode, the command syntax is verified but no additional validations are performed.

Note: The minimum length of the master password is 8 characters. The password must contain at least one number and one letter. The use of special symbols increases the strength of the password.

Tip: To ensure that backup servers are also updated by SSH if applicable, use the setup scripts to modify any passwords.

Use the following syntax to change the passwords for intercommunication between Tivoli Storage FlashCopy Manager components, and communication to Oracle and DB2 databases and to storage devices.

fccli command: -f password



Parameters

-p *profile*

Specify the full path and name of the profile that is used. If the path is not specified, the profile file in the current working path is used.

In interactive mode, the command searches the profile for the ORACLE, DB2STANDBY, and DEVICE_CLASS sections and then requests you to enter the relevant passwords.

-b *password-file*

Specify the password file to be created or updated. By default, the shared/acsd.pwd password file is in the directory that is specified by the **ACS_DIR** parameter. This parameter is included in the GLOBAL section of the profile file. This information is read from one of the following profiles:

- When the -p option is not specified, the profile file in the current working directory is used.
- When the -p option is specified, the profile file that is specified by this option is used.

sectionname:password

Specify the password for the user account that is referenced by the ORACLE, DB2STANDBY, and DEVICE_CLASS sections of the profile. To specify the password for the DEVICE_CLASS section, replace the *sectionname* variable with the *DEVICE_CLASS:device class name* variable for example, *DEVICE_CLASS:STANDARD*. Use this syntax when you specify the password: *DEVICE_CLASS:device class name:password*.

No spaces are allowed between the *sectionname:password* syntax.

:masterpassword

Specify the master password that is used to authenticate a library or agent to the acsd management agent. Alternatively, enter the value *auto* to enable Tivoli Storage FlashCopy Manager to auto-generate a password. For example, issue the following command to auto-generate the master password:

```
./fcmcli -f password :auto
```

GSKit commands

If you are not using SSH for remote installation and configuration of Tivoli Storage FlashCopy Manager on backup and cloning systems, use GSKit commands to manually import a self-signed certificate. If you decide to use a CA signed certificate, use GSKit commands to complete a manual setup.

Manually importing the self-signed certificate

The self-signed certificate is automatically created by Tivoli Storage FlashCopy Manager. When the Tivoli Storage FlashCopy Manager setup script is run on the production server, it automatically creates the *fcmselcert.arm* file. It is stored on the production server in the default installation path. The *fcmselcert.arm* file is automatically imported on the backup and cloning servers from the production server with the SSH remote deployment mechanisms of the setup script. When remote deployment is not used and you separately run the setup script on the backup or cloning server, the *fcmselcert.arm* file if present is automatically imported to the local key database and then deleted. To use this automation, copy the *fcmselcert.arm* file from the production server to either the backup or cloning server before you start the setup routines on the backup or cloning server.

Alternatively, you can import the self-signed certificate by using the following GSKit command. However, in most scenarios this step is not necessary as the file is automatically imported as part of the Tivoli Storage FlashCopy Manager setup process.

```
gsk8capicmd_64 -cert -add -db fmcert.kdb -stashed -label "FCM server  
certificate" -file <path to fcmselfcert.arm> -format ascii
```

This command fails if the key database already contains a certificate with the label FCM server certificate. To remove the certificate with the label FCM server certificate, you can use the following command:

```
gsk8capicmd_64 -cert -delete -db fmcert.kdb -stashed -label "FCM server  
certificate"
```

CA Certificate

You can use a CA signed certificate for Tivoli Storage FlashCopy Manager. If the certificate that is assigned by a CA has no built-in GSKit support, import the CA root certificate into the key database file (fmcert.kdb). Use the GSKit command-line utilities to update the file on the production system, the backup system, and the cloning system. The root certificate of a trusted CA certificate is in the key database. GSKit has the following trusted root certificates:

- Entrust.net Global Secure Server Certification Authority
- Entrust.net Global Client Certification Authority
- Entrust.net Client Certification Authority
- Entrust.net Certification Authority (2048)
- Entrust.net Secure Server Certification Authority
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 2 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 1 Public Primary Certification Authority - G3
- Thawte Personal Premium CA
- Thawte Personal Freemail CA
- Thawte Personal Basic CA
- Thawte Premium Server CA
- Thawte Server CA
- RSA Secure Server Certification Authority
- Secure Server Certification Authority

The following example shows the command to request that a CA signed certificate is included:

```
gsk8capicmd_64 -certreq -create -db fmcert.kdb -stashed -label "FCM server  
certificate request" -dn dist_name -target fcmservercertreq.arm
```

For SP800-131 compliance, when the **ENFORCE_TLS12** parameter is set to YES in the Tivoli Storage FlashCopy Manager profile, ensure that the certificate meets the minimum requirement by adding the following two options:

- `-size 2048` (or higher)
- `-sigalg sha224` (or higher)

Note: Tivoli Storage FlashCopy Manager creates a self-signed certificate that is signed with SHA512, and the size is 4086 bits.

The **label** parameter can have any value except FCM server certificate. This value is already used by the self-signed certificate in the key database.

When you use a certificate that is signed by a CA that has no built-in GSKit support, you must import the CA root certificate. This task must be completed before the certificate is received or imported. The CA root certificate must be imported into the key database (KDB) files on the production system. The CA root certificate must also be imported into the KDB files on the backup and cloning servers. Issue the following command to import the root certificate:

```
gsk8capicmd_64 -cert -add -db fmcert.kdb -stashed -label "FCM server certificate request" -file path to CARootCertificate.arm
```

Issue the following command to import a signed certificate when it is received from a CA:

```
gsk8capicmd_64 -cert -receive -file fcmservercertsigned.arm -db fmcert.kdb -stashed
```

Rename the CA signed certificate label to FCM server certificate. Usually, the key database still contains the self-signed certificate, it must be deleted before the CA signed certificate can be renamed. To remove the self-signed certificate from the key database, issue the following command:

```
gsk8capicmd_64 -cert -delete -db fmcert.kdb -stashed -label "FCM server certificate"
```

To rename the CA signed certificate issue the following command:

```
gsk8capicmd_64 -cert -rename -db fmcert.kdb -stashed -label "FCM server certificate request" -new_label "FCM server certificate"
```

The file `fcmselfcert.arm` is used to export the self-signed certificate. When you use a CA certificate, the `.arm` file is obsolete and must be deleted on the production system. The self-signed certificate is automatically removed from the key database on the backup or cloning system during the next remote update with the setup script. If remote deployment is not used, you can manually remove the self-signed certificate from the key database on the backup and cloning servers. To remove the self-signed certificate, issue the following command:

```
gsk8capicmd_64 -cert -delete -db fmcert.kdb -stashed -label "FCM server certificate"
```

Monitoring the expiry date of certificates

When a self-signed certificate is created, an expiry date can be specified. The expiration time of the certificate is specified in days. The default is 365 days. The duration is 1-7300 days (20 years). The Tivoli Storage FlashCopy Manager setup script creates the self-signed certificate for the production, backup, and cloning servers. The expiration time of all self-signed certificates that is generated by the setup script is 20 years. If you are using CA signed certificates, the expiration date is set by the certificate authority. You must monitor certificates for expiry and

remove any expired certificates. If the key database does not contain a valid certificate with the label FCM server certificate and the setup script is rerun, a new self-signed certificate is generated. The.kdb, .rdb, .arm and .sth files are rewritten.

Related information:



ftp://ftp.software.ibm.com/software/webserver/appserv/library/v80/GSK_CapiCmd_UserGuide.pdf

Query managed capacity

Use the **fcmlcli -f managed_capacity** command to display information about the Tivoli Storage FlashCopy Manager managed capacity for each source disk, and the total managed capacity amount for all source disks.

When you run the **fcmlcli -f managed_capacity** command, the output lists all the source volumes that are protected by Tivoli Storage FlashCopy Manager for which a backup (FlashCopy or snapshot) was created. If a volume contains multiple backups, that volume is counted only once during the query. Identify the repository from which to list backups by specifying the profile that is associated with the source volume. The output displays the source volume ID, the size (capacity) of each source volume, and the total managed capacity of all source volumes.

The **fcmlcli -f managed_capacity** syntax is as follows:

```
fcmlcli -f managed_capacity -p profile [-c]
```

-p Specify the name of the Tivoli Storage FlashCopy Manager profile that is associated with the backups on the volume.

-c Specify this option to display the output as comma-separated values.

Example output

This command displays all source volumes for the profile that is in db2/S01/acs:

```
fcmlcli -f managed_capacity -p /db2/S01/acs/profile
```

Output:

```
FFM0000I managed capacity for repository /db2/S01/acs/repo
```

```
FFM0000I volume ID: A0FR6HJ83C capacity: 2 GB
```

```
FFM0000I volume ID: A0FR6HENQ1 capacity: 2 GB
```

```
FFM0000I volume ID: A0FR6HAV80 capacity: 2 GB
```

```
FFM0000I total managed capacity 6 GB
```

This command displays all volumes for the profile that is in db2/S01/acs as comma-separated values:

```
fcmlcli -f managed_capacity -p /db2/S01/acs/profile -c
```

Output:

```
A0FR6HJ83C,2147483648
```

```
A0FR6HENQ1,2147483648
```

```
A0FR6HAV80,2147483648
```

```
*TOTAL*,6442450944
```

Background daemons

For Tivoli Storage FlashCopy Manager to work, some background daemon processes are required. Background daemon processes are not started directly. Instead, they are usually added to the `/etc/inittab` through the **setup_*.sh** commands.

To support high availability environments where the `/etc/inittab` cannot be used, you can instruct the `setup_*.sh` scripts to provide you with the exact commands that must be added to your high availability scripts instead of adding entries to `/etc/inittab`.

Management agent: acsd

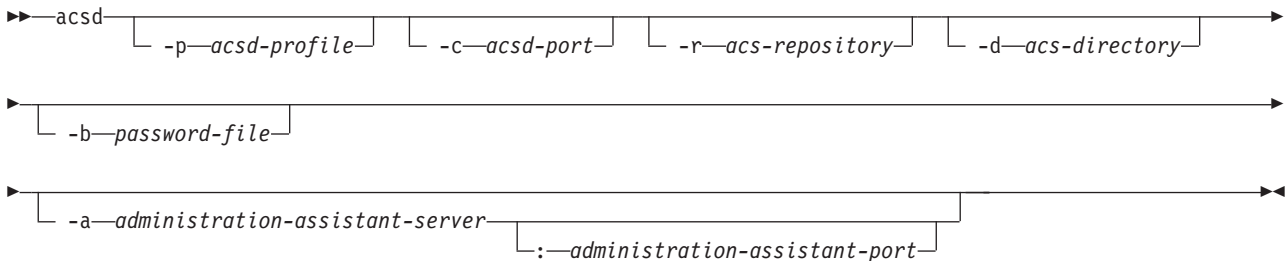
The management agent, `acsd`, coordinates the snapshot backup operation. It is a background daemon process that starts automatically.

The management agent, `acsd`, controls the backup flow and mediates between the other agents. The `acsd` agent 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.

If you must deviate from the standard installation, the management agent offers the following command options for customization:

acsd management agent



Syntax for obtaining version or help information:

acsd management agent help



Table 26. 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 that is used by the management agent. The management agent uses the GLOBAL and acsd sections of the configuration profile.	INSTANCE_DIR/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 Tivoli Storage FlashCopy Manager directory	ACS_DIR	
-b password-file	File in which the Tivoli Storage FlashCopy Manager 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 that are specified in the acsd profile or the corresponding default values. The shared and logs directories are automatically created in ACS_DIR. If no parameters are entered, acsd starts with the default profile and uses the default parameter values where applicable, or an error message is shown if this profile does not exist.

(DB2) When a user installs DB2 and creates a DB2 instance, the acsd management agent, is copied to the *DB2 instance directory/acs* directory. To activate Tivoli Storage FlashCopy Manager, the user must start the setup script as the DB2 instance owner from this same directory. This script creates two entries in the */etc/inittab* directory. The management agent, acsd, starts automatically from the */etc/inittab* directory without any command-line arguments. The default values are used for configuring the management agent, acsd. The default values can be overridden by providing a profile. By default, this profile is in the directory *DB2 instance directory/acs*.

When acsd is started for the first time, or with a new **ACS_DIR** parameter, the following actions occur:

- Create the subdirectories shared and logs
- Create a password file pwd.acsd in the shared subdirectory
- Generate a master password

When 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 they can read the master password from that directory.

Note: The minimum length of the master password is 8 characters. It must contain at least one number and one letter. The use of special symbols increases the strength of the password.

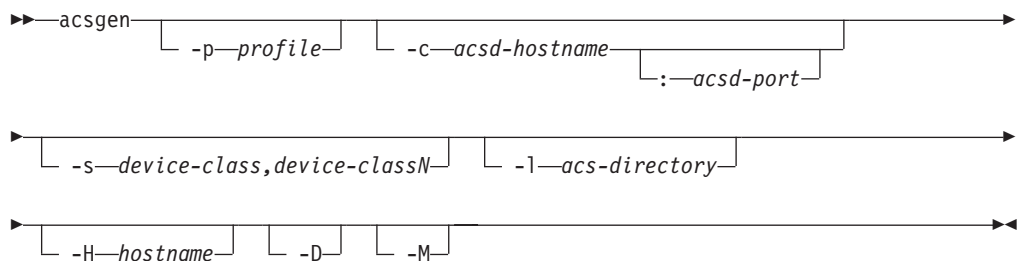
Generic device agent: acsgen

The generic device agent, acsgen, is the component that uses adapters to start snapshot commands on snapshot-compatible devices.

The generic device agent, acsgen, is started as a background daemon so you are not required to manually start it.

If you must deviate from the standard installation, the generic device agent, acsgen, offers the following command options for customization:

acsgen generic device agent



Syntax for obtaining version or help information:

acsgen generic device agent help

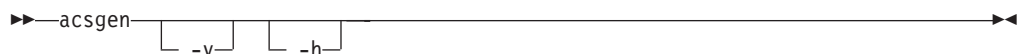


Table 27. Options for starting the generic device agent, acsgen. Description of acsgen options with default values if applicable.

Option	Description	Default
-p profile	Full profile name.	<INSTANCE_DIR>/profile
-c acsd-hostname	Name of the server where the management agent, acsd, is running.	localhost

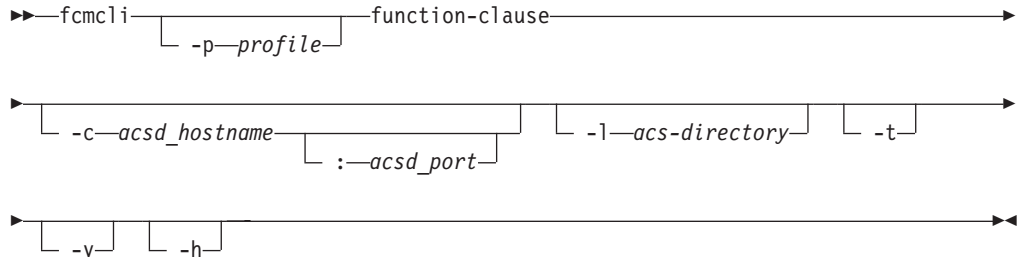
Table 27. Options for starting the generic device agent, *acsngen* (continued). Description of *acsngen* options with default values if applicable.

Option	Description	Default
<code>acsd-port</code>	TCP/IP port number or service name on which the management agent, <code>acsd</code> , is listening.	57328
<code>-s device-class</code>	Section in the profile that pertains to the device class. Specify multiple device classes by separating each device class by a space.	STANDARD
<code>-l acs-directory</code>	Directory where the logs and shared directories can be found.	<ACS_DIR>
<code>-D</code>	Start as daemon. The <code>-a</code> option defines the usability states that the device agent responds to. Valid only when started from the following path: <code>/etc/inittab</code>	Run and end.
<code>-H hostname</code>	The host name where the process is running. The primary use is by the launchpad component to check its partitions in a DB2 multi-partition environment.	The system host name that is displayed by the hostname command.
<code>-M</code>	Start the device agent as a mount agent. This agent is called for mounting or unmounting the target volumes on the backup system when any of the following situations exist: <ul style="list-style-type: none"> • An offloaded backup to Tivoli Storage Manager is requested • Database files on JFS file systems • Database files on AIX LVM mirrored volumes • The database is not suspended A mount verifies the consistency of the associated file systems.	Start as the monitoring agent.
<code>-v</code>	Display version and help information.	None
<code>-h</code>	Display help information only.	None

Mounting and unmounting snapshots on a secondary system

Tivoli Storage FlashCopy Manager commands are available to mount or unmount a snapshot backup on a secondary system.

fcmcli command



Where:

-p *profile*

Full profile name. Default value: *INSTANCE_DIR/profile*

-c *acsd-hostname*

Name of the server where the management agent (acsd) is running. Default value: *localhost*

acsd-port

TCP/IP port number or service name on which the management agent (acsd) is listening. Default value: *57328*

-l *acs-directory*

Directory where the logs and shared directories are located. Default value: *ACS_DIR*

-t Start with trace on. Default value: off.

-v Show version.

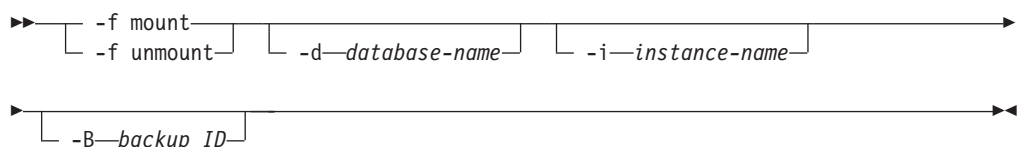
-h Show help text.

The return code of the **fcmcli** command is *0* if it finishes the request without an error or if there were no candidates for the request. Return code *1* indicates one or more minor issues occurred that are not critical but can be checked to prevent major issues later. Return code *2* indicates that an error occurred during the command execution.

FlashCopy administrative operations

The following functions are supported by the **fcmcli** command option **-f** 'function' for mount and unmount:

-f mount and **-f unmount** function-clauses



Where:

-f mount

Mount snapshot target set.

-f unmount

Unmount snapshot target set.

-d database-name

Database name.

-i instance-name

Instance name to apply to the command. There are no limitations.

-B backup ID

The Backup ID as displayed by `fcmlcli -f inquire [_detail]` or `db2acsutil` command.

The following functions are supported by the **fcmlcli** command option **-f 'function'** for forced unmount:

-f unmount function-clause with force option

►► -f unmount — -F — -d—database-name— -i—instance-name— -B—backup ID—►◄

Where:

-f unmount

Unmount snapshot target set.

-F Force a reset of **TAPE_BACKUP_IN_PROGRESS** usability states for the specified snapshot backup during the unmount force function. This parameter also requires the following arguments:

- -d database-name
- -i instance-name
- -B backup-id

-d database-name

Database name.

-i instance-name

Instance name to apply to the command. There are no limitations.

-B backup ID

The Backup ID as displayed by `fcmlcli -f inquire [_detail]` or `db2acsutil` command.

The functions **mount**, **unmount**, or **tape_backup** cannot run in parallel on the same backup server.

-f mount

This command mounts a snapshot backup on a backup system.

Mounting a backup means the following occurs:

1. Configure the target volumes, which might need to be assigned to the offload system (see the profile parameter **BACKUP_HOST_NAME** in “DEVICE_CLASS *device*” on page 171 for details).
2. Import the volume groups from the target volumes.
3. Mount all file systems within the volume groups.

The mount is performed by one mount agent for each backup server. As a result, a mount agent is started by the launchpad daemon that runs on the respective backup server. By specifying additional options (filter arguments) such as

```
-i instance-name  
-d database-name  
-B backup-id
```

a specific snapshot backup can be selected for mounting on the offload system.

Note: If the option **-B** is omitted, the oldest backup still in state *tape_backup_pending* is selected implicitly.

(DB2) In a DPF environment with multiple partitions, IBM Tivoli Storage FlashCopy Manager always mounts all partitions associated with a snapshot backup operation.

To reflect whether a snapshot backup is currently being mounted or is mounted, the usability states **MOUNTING** and **MOUNTED**, respectively, are set for those backups in the snapshot backup repository. These two state values prevent a duplicate mount request for a backup that is currently being mounted, or is already mounted, on the backup system. If multiple snapshot backups of a database are candidates to be mounted, Tivoli Storage FlashCopy Manager picks the one with the most recent snapshot backup ID.

-f unmount

This command releases all resources on the offload server that were used by the mount command.

For *normal mode*, the unmount is completed by one mount agent for each backup server. A mount agent is started by the launchpad daemon that runs on the respective backup server. The following steps are completed by the software:

1. Unmount the filesystem that belong to the target volumes.
2. Export the assigned volume group.
3. Remove the devices, *vpath/hdisk*, from the offload system.

When additional options, known as filter arguments, are specified, a specific snapshot backup can be selected for unmounting from the offload system. The following list identifies filter arguments:

```
-i instance-name  
-d database-name  
-B backup-id
```

(DB2) In a DPF environment with multiple partitions, IBM Tivoli Storage FlashCopy Manager unmounts all partitions associated with a snapshot backup.

If the unmount does not succeed because of problems related to the device agent, the usability state of the backup remains **MOUNTED** in the snapshot backup repository. After resolving the problems on the backup system, the **fcmcli unmount** command has to be issued again. The command is issued again to finalize the unmount of the filesystems and update the usability state of the backup in the snapshot backup repository. If an off-loaded tape backup is running, the usability state **TAPE_BACKUP_IN_PROGRESS** is set and those backups are not be picked by Tivoli Storage FlashCopy Manager for unmounting.

For *force mode*, unexpected system failures with offloaded tape backups can lead to an incorrect state of the backup reflected in the snapshot backup repository. The state **TAPE_BACKUP_IN_PROGRESS** is set. A built-in force option, **-F**, for the **fcmcli unmount** function is provided to return the system to a usable state. Besides the normal unmount function, the unmount force option picks backups in the **TAPE_BACKUP_IN_PROGRESS** state as candidates to be unmounted and to reset the **TAPE_BACKUP_IN_PROGRESS** usability state for those backups. The **-d**, **-i**, and **-B** options are specified to uniquely identify the backup involved.

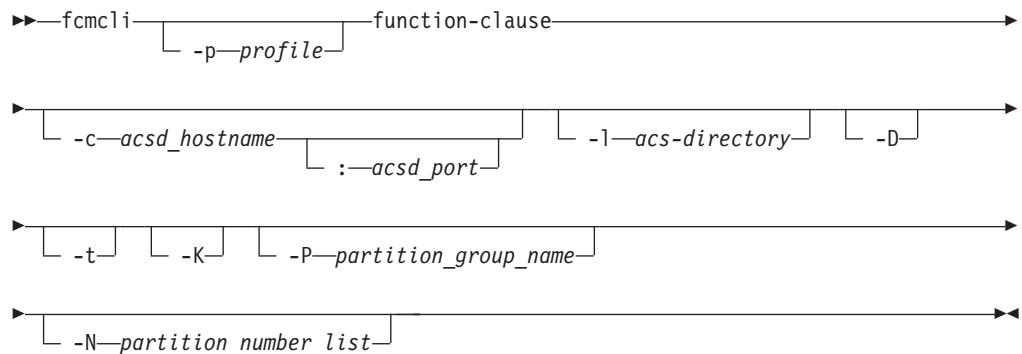
Integration with Tivoli Storage Manager

If Tivoli Storage Manager is set up and configured in your environment, you can create a backup to Tivoli Storage Manager from a snapshot.

The fcmcli offload agent

The offload agent is a daemon process that manages offloaded backups to Tivoli Storage Manager. The agent also provides a command line interface offering functions for managing Tivoli Storage Manager backups.

fcmcli command



Where:

-p profile

Full profile name. Default value: *INSTANCE_DIR/profile*

-c acsd_hostname

Name of the server where the management agent (acsd) is running. Default value: *localhost*.

acsd-port

TCP/IP port number or service name on which the management agent (acsd) is listening. Default value: *57328*.

- l** *acs-directory*
Directory where the logs and shared directories are located. Default value: *ACS_DIR*.
- D** Run as daemon process. Valid only when started from */etc/inittab*. Default value: Run and end.
- t** Start trace on. Default value: Trace off.
- K** In a multi-partition environment, the partitions remain mounted when all participating partitions are successfully offloaded to Tivoli Storage Manager. The offload agent unmounts all partitions after the last partition is successfully offloaded. Default value: Off. The unmount operation is part of every Tivoli Storage Manager backup operation.
- P** *partition_group_name*
The name of a partition group as specified in the profile with the **PARTITION_GROUP** parameter.
- N** *partition_number_list*
A single number or list of numbers that are separated by a comma that specifies the partitions to apply the action against. When not specified, the action is applied to all partitions.

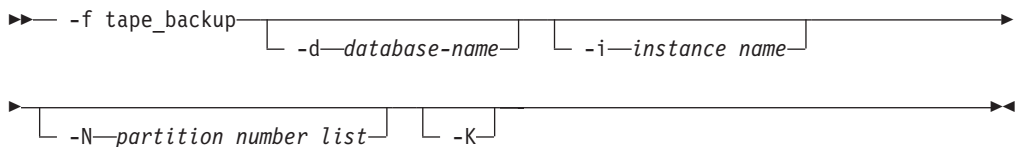
The values for the function-clause parameter are described in the following sections.

FlashCopy offload operations

In a DB2 environment, the installation of Tivoli Storage FlashCopy Manager enables the offload function that otherwise is not available.

The following functions are supported by the *fccli* command option **-f function**:

-f tape_backup function-clause



Where:

- f tape_backup**
Backs up a snapshot target set to Tivoli Storage Manager.
- d database-name**
The name of the database.
- i instance name**
The name of the instance to apply the action against. This parameter is required for the **-F** option. There are no limitations.
- N partition_number_list**
A single number or list of numbers that are separated by a comma that specifies the partitions to apply the action against. When not specified, the action is applied to all partitions.
- K** In a multi-partition environment, the partitions remain mounted when all

participating partitions are successfully offloaded to Tivoli Storage Manager. The offload agent unmounts all partitions after the last partition is successfully offloaded. Default value: Off. The unmount operation is part of every Tivoli Storage Manager backup operation.

The functions mount, unmount, or tape_backup cannot run in parallel on the same backup server.

The function update_status is supported by the **fcmccli** command:

-f update_status function-clause

►► -f update_status — -d—*database-name*— -i—*instance-name*—————►

► -B—*backup ID*— -S—*TSM_BACKUP=yes|no*—————►◄

Where:

-f update_status

Update the usability state after a snapshot backup operation completes to one of the following states:

- Offload a snapshot backup to Tivoli Storage Manager (**TSM_BACKUP=yes**).
- Do not offload a snapshot backup to Tivoli Storage Manager (**TSM_BACKUP=no**) if it was scheduled to offload.

-d database-name

The name of the database.

-i instance-name

The name of the instance to apply the action against. This parameter is required for the -F option. There are no limitations.

-B backup ID

The Backup ID as displayed by **fcmccli -f inquire [_detail]** or **db2acsutil** command.

-S TSM_BACKUP=yes|no

Use this option to inform Tivoli Storage FlashCopy Manager that a Tivoli Storage Manager backup is no longer required or that a Tivoli Storage Manager backup is requested. This option is only valid with the **update_status** function.

The fmccli process connects to the acsd management agent and then runs the function that is specified with the -f option. After the operation is finished, the fmccli agent passes notification to the acsd agent and the snapshot backup repository is backed up. When started as a daemon (-D option), as is the case for the standard /etc/inittab entry, fmccli runs offloaded tape backup operations. This action results in a synchronous tape backup of all snapshot backups. When a new snapshot is started with **TSM_BACKUP YES**, the offload agent starts the backup to tape when it becomes available for mounting on a backup system (**REMOTELY_MOUNTABLE**).

If the offload agent completes the request without an error and there are no candidates for the request, the return code is 0. If there is a warning, the return code is 1. If there is an error, the return code is 2.

-f tape_backup

This offload agent command backs up data to tape storage.

Note: IBM Tivoli Storage Manager for Enterprise Resource Planning must be installed on the production and backup server if you use IBM Tivoli Storage FlashCopy Manager in an SAP environment with Oracle or DB2. Tivoli Storage Manager for Databases: Data Protection for Oracle as well as Oracle must be installed on the production and backup server if you use Tivoli Storage FlashCopy Manager to protect an Oracle non-SAP environment. If FlashCopy Manager for Custom Applications is used, the Tivoli Storage Manager backup-archive client must be 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 updates the usability state with **TAPE_BACKUP_PENDING**. The Tivoli Storage FlashCopy Manager offload agent then picks up all snapshot backups in the state **TAPE_BACKUP_PENDING** and backs them up to tape.

To start the offload backup to tape, enter the command:

```
fccli -f tape_backup
```

By specifying additional options or filter arguments such as

```
-i instance-name  
-d database-name
```

the appropriate backup for the given instance and or database can be selected for offloading to tape. The **-B backup-id** option cannot be specified in conjunction with **-f tape_backup**. The backups should be processed in chronological order. The **tsm4acs** backs up the oldest snapshot eligible for transfer to Tivoli Storage Manager.

(DB2) Offloaded tape backups are not be registered in the DB2 history on the production system. They are reflected in the DB2 history on the offload system when the assigned volumes have not been overwritten. For more information, see “DB2 backup history file overview” on page 105.

By specifying the **-D** option for the offload agent, it acts as a daemon process that periodically checks for outstanding tape backup requests. Furthermore, the offload agent, running as a daemon, tries to offload a snapshot backup to tape only one time. If the first attempt fails for some reason, the snapshot backup is marked accordingly and is not be picked a second time by the **tsm4acs** daemon for offloading to tape. This type of backup must be offloaded to tape manually by issuing the following command:

```
fccli -f tape_backup filter_arguments
```

If multiple snapshot backups of a database are candidates for offloading to tape, the Tivoli Storage FlashCopy Manager offload agent (whether as a daemon or with the **-f tape_backup** function) always selects the one with the oldest snapshot backup ID. This selection ensures that the Tivoli Storage Manager backups are created in the appropriate sequential order.

Tip: Whenever a new snapshot backup with **TSM_BACKUP** set to YES, MANDATE, or LATEST is created, Tivoli Storage FlashCopy Manager sets the **TAPE_BACKUP_PENDING** status to NO for all snapshot backups that were previously created with **TSM_BACKUP**

set to LATEST. This prevents backup requests to Tivoli Storage Manager from queuing if they cannot be completed in time.

The tsm4acs **tape_backup** function internally does the following steps:

1. Mount the file systems on the offload system if they were not previously mounted using fcmcli with the 'mount' function or by a forced mount request. If all necessary file systems were mounted, this step is skipped (see “**-f mount**” on page 258).
2. Update the usability state to **TAPE_BACKUP_IN_PROGRESS** for all partitions that have 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** and set **TAPE_BACKUP_COMPLETE**. For those partitions where the backup failed, set the usability state **TAPE_BACKUP_FAILED**. For all participating partitions, reset the usability state **TAPE_BACKUP_IN_PROGRESS**.
5. Unmount the file systems from the offload system (see “**-f unmount**” on page 258).

When the usability state for a partition is **TAPE_BACKUP_IN_PROGRESS**, any request to restart the offload of that partition to tape is refused.

If a backup to Tivoli Storage Manager fails, the Tivoli Storage FlashCopy Manager software can try the backup operation again.

(DB2) In DPF environments, offloaded backups can be performed only when the snapshot was created on all partitions. If the Offload Agent retries a backup operation, it only backs up those partitions that have not been backed up successfully.

(DB2) In DPF environments with more than one partition it can be useful to perform the offloaded Tivoli Storage Manager backup in parallel on multiple partitions. This is useful when the DB2 DPF database is spread across more than one backup system. The profile parameter **NUMBER_BACKUPS_IN_PARALLEL** in the OFFLOAD section can be used to specify the degree of parallelism. For more information, see Appendix A, “Configuration files,” on page 135.

-f update_status

This offload agent command updates the usability state of a specified snapshot backup.

The usability state of a specified snapshot backup can be updated to either offload a snapshot backup to Tivoli Storage Manager (TSM_BACKUP=yes) or to not offload a snapshot backup to Tivoli Storage Manager (TSM_BACKUP=no). This provides opportunity to offload a snapshot backup to Tivoli Storage Manager although the TSM_BACKUP or TSM_BACKUP_FROM_SNAPSHOT profile parameter was deactivated during the snapshot backup operation. In this situation, if there is no longer a need to offload the snapshot backup to Tivoli Storage Manager (which was performed with the parameter TSM_BACKUP or TSM_BACKUP_FROM_SNAPSHOT activated), the usability state can be reset accordingly.

To identify the backup whose state is to be modified, these parameters must also be specified when using -f update_status:

```
-d database-name  
-i instance-name  
-B backup-id
```

Appendix D. Backup, restore, cloning commands, and utilities

You can issue commands to trigger a snapshot backup or snapshot restore, and to inquire and delete snapshot backups within the Tivoli Storage FlashCopy Manager repository. In addition, you can create and manage database clones from the command-line interface.

Commands for DB2 that use DB2 utilities

Tivoli Storage FlashCopy Manager fully integrates with DB2 backup utilities like `db2 backup` and `db2 restore` commands. In addition, Tivoli Storage FlashCopy Manager provides the **fcml** command-line interface, which you can use for extra tasks for example, to restore backups from a DB2 partition groups.

For detailed information about how to use DB2 to create snapshot backups, see the *DB2 Command Reference*.

You can use the options in the following table as parameters in the `<option string>` option to be specified with the following commands:

- `db2 backup db <dbname> [...] use snapshot options <option string>`
- `db2 restore db <dbname> [...] use snapshot options <option string>`
- `db2acsutil [...] options <option string>`

Where `<option string>` has the form `<parameter>[=<value>]`
`[<parameter>[=<value>] ...]`.

PROFILE

Absolute path and file name of profile. The default value is `<ACS_DIR>/profile`.

TSM_BACKUP

Options include YES, MANDATE, LATEST, and NO. Applies to only **db2 backup**.

DELETE_FORCE

This option applies to only **db2acsutil**. With **db2acsutil delete**, withdraws any FlashCopy relations for the target set represented by the backup (applicable to CIM devices only). A manual withdraw of FlashCopy relations is needed for a restore when multiple target sets are in use. At least one target set other than the one to be restored is in a **NOCOPY** or **INCR** FlashCopy relation.

With **db2acsutil query**, also lists backups that are deleted without the `DELETE_FORCE` option.

For DS8000 and SAN Volume Controller, incremental FlashCopy relations are not withdrawn.

DEVICE_CLASS

In the profile, see *device_section_name*. Applies only to **db2 backup** command.

Commands for DB2 that use the fcmcli command-line interface

The fcmcli command-line interface provides extra commands in situations where the DB2 utilities commands cannot be used. For example, to restore backups of DB2 partition groups or operations on DB2 standby servers. You can also use the fcmcli commands to query the Tivoli Storage FlashCopy Manager repository for valid snapshot backups.

You can run the **fcmcli -f** command with one of the following functions: **[inquire, inquire_detail, delete, restore]**.

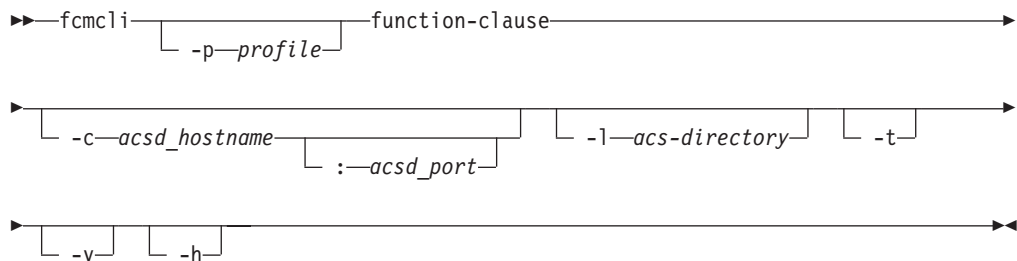
The fcmcli -f inquire queries the backup repository and lists all available backups. This command is of special interest in environments where multiple partitions are located on the same volume group, for volume sharing.

The -f inquire_detail command is similar to **-f inquire** but prints additional information like usability states and background copy progress for each backup.

The -f delete is used as part of the version control mechanism of Tivoli Storage FlashCopy Manager and can be used to delete full backups.

The fcmcli -f restore command is used in partitioned DB2 environments with SAP workload, where multiple DB2 partitions are on a single volume group and backups cannot be restored directly from DB2.

fcmcli command



Where:

-p *profile*

Full profile name. Default value: *INSTANCE_DIR/profile*

-c *acsd-hostname*

Name of the server where the management agent (acsd) is running. Default value: *localhost*

acsd-port

TCP/IP port number or service name on which the management agent (acsd) is listening. Default value: *57328*

-l *acs-directory*

Directory where the logs and shared directories are located. Default value: *ACS_DIR*

-t Start with trace on. Default value: off.

-v Show version.

-h Show help text.

The return code of the **fcmccli** command is 0 if it finishes the request without an error or if there were no candidates for the request. Return code 1 indicates one or more minor issues occurred that are not critical but can be checked to prevent major issues later. Return code 2 indicates that an error occurred during the command execution.

FlashCopy operations of DB2 with partition group function-clauses

The following functions are supported by the **fcmlcli** command option **-f** function for a FlashCopy restore of DB2 with a partition group:

-f restore function-clause

```

▶▶ -f restore — -B—backup ID — -P—partition_group_name — -d—database-name————▶
▶ [ -i—instance-name ]————▶

```

Where:

-B *backup ID*

The Backup ID as displayed by `fcmlcli -f inquire [_detail]` or `db2acsutil` command.

-P *partition group name*

The name of a partition group as specified in the profile with the **PARTITION_GROUP** parameter.

-d *database-name*

The name of the database.

-i *instance-name*

The name of the instance to apply the action against. This parameter is required for the -F option. There are no limitations.

The **fcmccli -f restore** command can be used to restore a backup of a DB2 partition group. During the restore operation, the DB2 database is stopped and a FlashCopy restore is initiated. After the restore operation finishes, the database starts and initializes. The restore operation is performed for all partitions that correspond to the specified partition group.

For more information about how to use this command with the **PARTITION_GROUP** parameter, see “CLIENT” on page 143 profile parameters.

FlashCopy operations of DB2 with and without partition group function-clauses

The following functions are supported by the **fcmccli** command option -f 'function' for FlashCopy inquire and delete of DB2 snapshots:

-f inquire and -f inquire detail function-clauses

➤ `-f inquire` `-f inquire detail` `-B backup ID` `-F` `-i instance-name`

Where:

-B *backup ID*

The Backup ID as displayed by `fccli -f inquire [_detail]` or `db2acsutil` command.

-F DELETE_FORCE flag. Applies to **inquire** and **inquire_detail** command:

With the `inquire[_detail]` function, it also lists backups that are deleted without the **DELETE_FORCE** flag.

-i *instance-name*

The name of the instance to apply the action against. This parameter is required for the **-F** option. There are no limitations.

-f delete function-clause

►► -f delete— -B—*backup ID*— -i—*instance-name*— -F—►

Where:

-i *instance-name*

The name of the instance to apply the action against.

-B *backup ID*

The Backup ID as displayed by `fccli -f inquire [_detail]` or `db2acsutil` command.

-F DELETE_FORCE

With the delete function, withdraws any FlashCopy relations currently in effect for the target set represented by the backup (applicable to DS8000 and SAN Volume Controller only).

You can use the delete function to delete a snapshot. This task can take some time to process as it is carried out as a background asynchronous task. However, during this process the snapshot is no longer available for inquiry or restore operations. The snapshot backup remains visible in the storage device or GPFS file system until the snapshot is deleted by the background monitor.

The **-f delete** function operates exclusively on snapshot backups. Backups to Tivoli Storage Manager are not affected by this command.

The processing of the delete command is also dependent on the type of storage system and the file system where applicable:

- IBM XIV Storage System, IBM System Storage N series, or NetApp, the snapshot is deleted asynchronously by the background monitor after the command is issued.
- Similarly, in a DB2 pureScale environment, the GPFS file system snapshot is deleted asynchronously by the background monitor.
- IBM System Storage DS8000 and SAN Volume Controller the FlashCopy relationships between the source and target volumes are withdrawn after the command is issued. These relationships can be used for future backups. To delete these relationships, specify the **-F** option when you issue the delete command on these storage systems. The snapshot is deleted asynchronously by the background monitor.

The following example shows the command syntax to use as database instance owner on the production system:

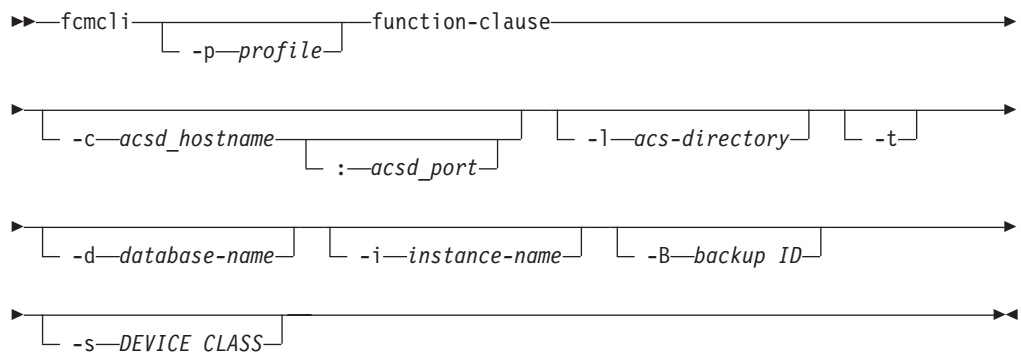
```
./fcmcli -f delete [-F]
```

fcmcli -f *_db2standby

Information for the support of DB2 standby server and DB2 HADR environments is provided.

With FlashCopy Manager for Custom Applications you can create snapshot backups of a DB2 standby server and DB2 HADR environments. You can back up to Tivoli Storage Manager from a snapshot by using the Tivoli Storage Manager backup-archive client.

fcmcli command



Where:

-p profile

Specifies the full profile name. The default value: *<INSTANCE_DIR>/profile*

-c acsd-hostname

Specifies the name of the server where the management agent (acsd) is running. The default value: *localhost*

acsd-port

Specifies the TCP/IP port number or service name on which the management agent (acsd) is listening. The default value: *57328*

-l acs-directory

Specifies the directory where the logs and shared directories are located. The default value: *<ACS_DIR>*

-t Specifies to start with the trace facility turned on. By default, the trace facility is turned off.

-d database-name

Specifies the database name. Required for -F option. There is no default value.

-i instance-name

Specifies the instance name that applies to the command. Required for -F option. There is no default value.

-B backup ID

Specifies the Backup ID as displayed by `fcmcli -f inquire [_detail]` or `db2acsutil`. There is no default value.

-s *DEVICE_CLASS*

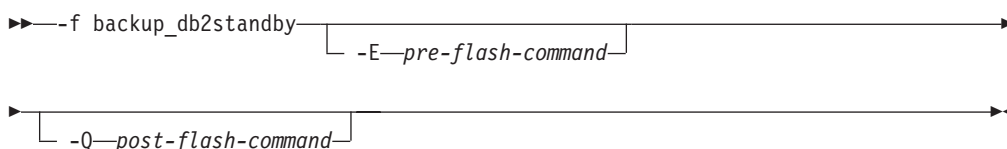
Specifies the name of the *DEVICE_CLASS* section in the profile that is used for the backup operation. The default value is specified in the profile.

The values for the function-clause parameter are described in the following sections.

Function-clause: FlashCopy operations of DB2 HADR databases

The following functions are supported by the **fcmcli** command option **-f** function for FlashCopy backups of DB2 HADR databases:

fcmcli command functions



Where:

-E preflash command

This option overrides the value of the **PRE_FLASH_CMD** parameter that is specified in the **CLIENT** section of the profile. The **preflash** command is run on the production server and can be a script. The return code of the **preflash** command is evaluated. The following return codes are used:

0 Indicates a successful operation. The Tivoli Storage FlashCopy Manager backup operation continues.

Any value other than 0

Indicates an unsuccessful operation. The Tivoli Storage FlashCopy Manager backup operation ends.

There is no default value.

-Q postflash command

This option overrides the value of the **POST_FLASH_CMD** parameter that is specified in the **CLIENT** section of the profile. The **postflash** command is run on the production server and can be a script. The return code of the **postflash** command is evaluated. The following return codes are used:

0 Indicates a successful operation. The Tivoli Storage FlashCopy Manager backup operation continues.

Any value other than 0

Indicates an unsuccessful operation. The Tivoli Storage FlashCopy Manager backup operation ends.

There is no default value.

The **-f backup_db2standby** function operates like the **fcmcli -f backup** function. However, instead of requesting the user to specify a list of files for backup, this command retrieves this information from the active DB2 instance. It is important that the names of the files and file systems from the active DB2 database (HADR primary) match the names of files and file systems of the standby server (HADR

secondary). The editable sample **preflash** and **postflash** command files assist you to shut down and restart the DB2 standby server (HADR secondary). This action creates a consistent backup image.

The following figure illustrates the workflow that is executed from this command.

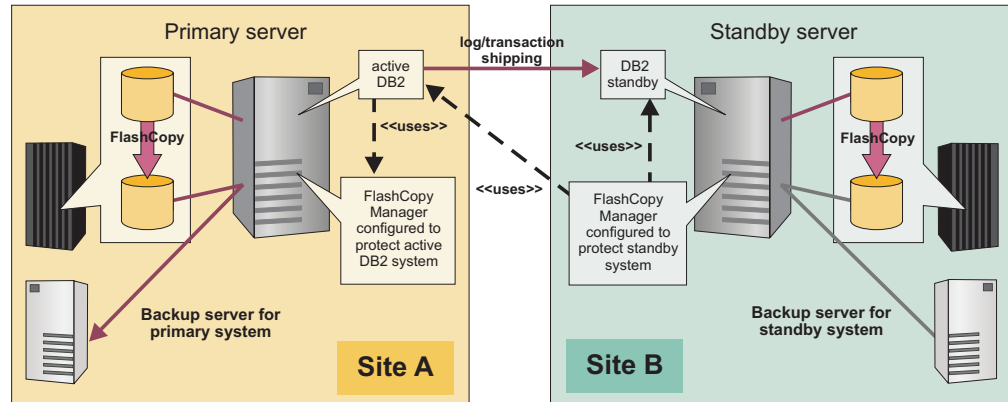
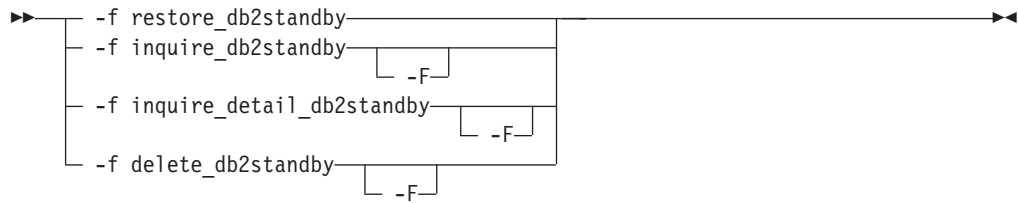


Figure 21. Protection of DB2 HADR standby nodes with FlashCopy Manager for Custom Applications

1. It starts with connecting to the active DB2 database (for example site A) to retrieve a list of files from the active database.
2. This list of files is then translated into a list of volumes and LUNs in site B, using the assumption that the names of DB2 files and file systems in site A are identical to the names of files and file systems in site B.
3. The preflash script is invoked. The preflash script typically stops the DB2 standby system in order to enable FlashCopy Manager to create a consistent snapshot backup. The return code of the **preflash** command is evaluated as follows:
 - 0 Successful. The Tivoli Storage FlashCopy Manager backup operation continues.
 - Any value other than 0** Unsuccessful. The Tivoli Storage FlashCopy Manager backup operation terminates.
4. Once the snapshot has been taken, the **postflash** command is invoked, which typically starts the DB2 standby system again. The return code of the **postflash** command is evaluated as follows:
 - 0 Successful. The Tivoli Storage FlashCopy Manager backup operation continues.
 - Any value other than 0** Unsuccessful. The Tivoli Storage FlashCopy Manager backup operation terminates.

The following functions are supported by the **fcmccli** command option **-f** function for FlashCopy restore, inquire, and delete of DB2 HADR databases:

fcmccli command



The following list identifies the options to use when you use the **fcmccli** command in DB2 standby server and DB2 HADR environments:

-f restore_db2standby

Use to restore a DB2 HADR snapshot backup. There is no default value.

-f inquire_db2standby

Use to query the backup repository and list all available backups. There is no default value.

-f inquire_detail_db2standby

Use to query the backup repository and list all available backups in detail. There is no default value.

-f delete_db2standby

Use to unmount and delete a snapshot of a DB2 standby server. There is no default value.

-i instance-name

The instance name that applies to the command. This option is required for **-F** option. There is no default value.

-F The DELETE_FORCE flag applies to the following commands:

- **inquire_db2standby**
- **inquire_detail_db2standby**
- **delete_db2standby**

When you run the **delete_db2standby** command, for only DS8000 and SAN Volume Controller storage systems, any FlashCopy relations that are set for the target set represented by the backup are withdrawn.

When you run the **inquire_detail_db2standby** command, backups that are deleted with the DELETE_FORCE flag are deleted. There is no default value.

-t Start with the trace facility turned on. By default, the trace facility is turned off.

-v Displays the version. There is no default value.

-h Displays the help information. There is no default value.

-B The backup ID as displayed by the following commands: **fcmccli -f inquire [_detail]** or **db2acsutil**. There is no default value.

-s DEVICE_CLASS

The name of the DEVICE_CLASS section in the profile that is used for the backup operation. The default value is specified in the profile.

If the **fcmccli** command finishes the request without an error or if there were no candidates for the request, the return code is *0*. If one or more non-critical issues are reported, the return code is *1*. Resolve these issues to prevent more issues from occurring. If an error is reported, the return code is *2*.

The following sections describe the details of the various functions that are specified with the **-f** option of the **fcmccli** command.

-f inquire_db2standby

This command queries the backup repository and lists all available backups.

This command applies to DB2 HADR standby server environments. To run the **-f inquire_db2standby** command, specify the following option to get an overview of the files that are contained in the snapshot backup:

-B backup-id

-f inquire_detail_db2standby

This command queries the backup repository and lists all available backups.

This command is similar to the **-f inquire_dbstandby** command. When available, the command prints additional information like usability states and background copy progress for each backup. This command applies to DB2 HADR standby server environments. To run the **-f inquire_detail_db2standby** command, you can specify the following option to get an overview of the files that are contained in the snapshot backup:

-B backup-id

-f restore_db2standby

This command restores a DB2 high-availability disaster recovery (HADR) target database.

During the restore operation, the DB2 database is stopped and a FlashCopy restore is initiated. After the restore operation is completed, the database is started and initialized. When using the **-f restore_db2standby** command, the following option can be used:

-B backup ID

Backup and restore commands for Oracle

Commands to back up and restore native Oracle and SAP with Oracle databases are provided.

The acsora user interface for Oracle

Use the production system user interface, *acsora*, to issue commands in an Oracle database environment.

The *acsora* syntax follows:

```
acsora [-p profile] -f function [-B backupID] [-F] [-s DEVICE_CLASS ]
```

where *<function>* is one of:

```
backup
restore
delete
inquire
inquire_detail
```

Table 28. Parameters for Oracle databases

Option	Description	Default
-p profile	Full path and name of the profile that is used by the Management Agent The Management Agent uses the GLOBAL and ACS sections of the profile.	<ACS_DIR>/profile
-B backupID	The backup ID for restore, delete, inquire functions	
-f backup	Backup database	Function backup if -f is not specified.
-f restore	Restore database	
-f delete	Delete snapshot backup	
-f inquire	List snapshot backups	
-f inquire_detail	List snapshot backups	
-F	When specified with the -f delete or -f inquire options, the -F option withdraws source and target relationships.	
-s DEVICE_CLASS	The name of the DEVICE_CLASS section in the profile that is used for the backup operation.	As specified in the profile.

The return code of acsora is 0 if it finishes the request without an error. The return code 1 indicates one or more issues occurred during the process. Although not considered critical, resolve these minor issues to prevent potential critical issues later. Return code 2 indicates that an error occurred during command processing and that the operation did not complete successfully.

-f backup

This command backs up the Oracle database according to the profile settings.

Example (backup database):

```
acsora -f backup -s STANDARD
```

-f restore

This command restores the Oracle database from the backup that is specified by the backup ID, or the latest backup.

The Oracle database is available for immediate use after a snapshot restore and a rollforward recovery. However, for DS8000 and SAN Volume Controller, background copy processing from the target volumes to the source volumes might require more time to complete, especially if **FLASHCOPY_TYPE COPY** is specified. Although the database is available, you cannot perform another Tivoli Storage FlashCopy Manager backup or restore until background copy processing completes.

Example (restore specified backup):

```
acsora -f restore -B A0FZ36AY8G
```

See “Restoring Oracle databases from Tivoli Storage Manager” on page 106 and “Restoring Oracle databases” on page 105 for detailed instructions on how to restore your Oracle database.

-f inquire

This command lists the details for the snapshot backup that is denoted by the backup ID, if specified by using the **-B** option, or all backups.

Example (list all backups):

```
acsora -f inquire
```

-f inquire_detail

This command queries the backup repository and lists all available backups.

This command is like the **-f inquire** command, but it prints more information like usability states and background copy progress, if available, for each backup.

-f delete

This command deletes the snapshot backup that is denoted by the entered backup ID.

Example (deleted specified backup):

```
acsora -f delete -B A0FZ36AY8G
```

BR*TOOLS - User interface for Oracle in an SAP environment

Because Tivoli Storage FlashCopy Manager fully integrates with SAP® BR*TOOLS, Tivoli Storage FlashCopy Manager does not provide a separate user interface. Information is provided about the query and deletion of snapshot backups, operations that are not directly supported by BR*TOOLS.

For detailed information about how to use BR*TOOLS to create snapshot backups, see *SAP Database Guide for Oracle*. Tivoli Storage FlashCopy Manager provides a console user interface that can be used instead of BR*TOOLS for query and restore operations. See “acsutil Snapshot Object Manager for Oracle” on page 277 for detailed information.

Important: If IBM Tivoli Storage Manager for Enterprise Resource Planning is not installed, Tivoli Storage FlashCopy Manager does not use the default path `/usr/sap/<SID>/SYS/exe/run` to install the backint executable file. By not using the default path, an existing backint file cannot be overwritten. Therefore, you must start the backint executable file from the Tivoli Storage FlashCopy Manager installation directory (`<INSTANCE_DIR>`).

If Tivoli Storage Manager for ERP is installed, you can run the backint executable file from the default installation path. Tivoli Storage FlashCopy Manager inquire and delete commands can use the **backint** interface.

The syntax of the **backint** command is as follows:

backint [-p profile] -f <function> -t <backup_type> [-F]

where <function> is one of the following options:

inquire
inquire_detail
delete

and <backup_type> is one of the following options:

volume
file

Table 29. Parameters for Tivoli Storage FlashCopy Manager **backint** command

Option	Meaning
-p	Tivoli Storage FlashCopy Manager Backint profile (see "BACKINT configuration file" on page 207)
-f inquire or inquire_detail	Inquire function with or without detailed information about the backups.
-f delete	Delete function.
-t volume	This option can be used to manage snapshot backups that are created with Tivoli Storage FlashCopy Manager.
-t file	Use this option to manage files that are backed up directly to the Tivoli Storage FlashCopy Manager repository. Note: When IBM Tivoli Storage Manager for Enterprise Resource Planning is installed, both options are also supported by IBM Tivoli Storage Manager for Enterprise Resource Planning. However, in this case option -t file is used to manage backups that are sent to the Tivoli Storage Manager server instead.
-F	Force option to be used with inquire , inquire_detail , or delete functions. When used with inquire or inquire_detail , all available backups and all backups marked for deletion are displayed. When used with the delete function, the option withdraws the source target FlashCopy relations on DS8000 and SAN Volume Controller.

-f inquire and -f inquire_detail functions

The **inquire** function that is run by SAP BR*Tools and BRRESTORE, is used to query the Tivoli Storage Manager server for backup IDs or files that belong to a particular backup ID. For troubleshooting, run this function from the command line. You must specify the *backup_type* as -t volume when you use the **inquire** function to obtain details about Tivoli Storage FlashCopy Manager backups. The following code is provided as an example:

```
backint -p /oracle/<SID>/dbs/init<SID>.utl -f inquire -t volume
```

Tivoli Storage FlashCopy Manager prompts you to enter the inquiry in one of the following formats:

#NULL

Use to display all saved backup IDs. The following sample is provided:

```
#BACKUP JE0__A0DNE9Z74C
```

In this example, JE0__A0DNE9Z74C is the backup ID. #BACKUP is not part of the backup ID. The first 6 characters are the user-defined prefix. The following 10 characters represent the unique ID for the backup.

BackupID

Use to display all of the files that relate to this backup ID. The following sample result is provided:

```
#BACKUP JE0__A0DNE9Z74C /oracle/C21/dbs/initC21.utl.
```

#NULLfilename

Use to display all of the backup IDs corresponding to this file. The *filename* variable must include both the path to and name of the file.

BackupID filename

Use to verify if a specific file is saved with a particular backup ID. The *filename* variable must include both the path to and name of the file.

-f delete

Tivoli Storage FlashCopy Manager version control mechanism deletes backups. However, you can manually delete a Tivoli Storage FlashCopy Manager backup by using the **delete** function and specifying the backup to delete. You must specify the *backup_type* as **-t volume** when you use the **delete** function to delete Tivoli Storage FlashCopy Manager backups. The delete function can delete full backups only.

This function can be started from the command line as follows:

```
backint -p /oracle/<SID>/dbs/init<SID>.utl -f delete -t volume
```

You are prompted to enter the backup ID.

acsutil Snapshot Object Manager for Oracle

The Snapshot Object Manager for Oracle, *acsutil*, provides a snapshot backup query and restore interface for Oracle and Oracle in an SAP environment environments.

Functions of the acsutil command

The Snapshot Object Manager for Oracle, *acsutil*, provides an interface for *acsora* to show available backups, run restore operations, and delete unwanted backups. It communicates with *acsora* through input and output files.

Syntax of the acsutil command

```
acsutil [-p profile]
```

Where **-p profile** is the path and name of the Tivoli Storage FlashCopy Manager profile. The default value is *ACS_DIR/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 V4.1.1.0, Copyright IBM 2014

Backup ID's	Files stored under

TAB change windows
F6 fileInfo
F2 Restore
F7 -----
F3 -----
F8 Delete
F4 -----
F10 eXit
F5 reFresh

If you mark the backup ID you are interested in and then press the Tab key, all file names that belong to the marked backup ID are displayed.

Tab - Switch window side

Move the cursor between the 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.

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 must confirm the deletion operation. The backup ID and all included files are deleted.

For each restore, a log file is created.

Backup and restore commands for custom applications

The Tivoli Storage FlashCopy Manager command line interface, **fcmcli**, is used to create snapshot backups, snapshot restores, inquire, and delete operations for applications when a native backup adapter does not exist.

When you run the **fcmcli** command, provide a list of files for which a snapshot backup is created. You can specify the list of files either through the configuration file or through the command line interface. Optionally, you can provide **fcmcli** with the following scripts:

- A script to prepare your environment before the snapshot is created. For instance, provide a script to quiesce or shutdown the applications that are backed up.
- A script to resume your environment after the snapshot is complete.

If specified, the scripts are started immediately before and after the snapshot is created to minimize application downtime.

fcmcli command

```
►► -fcmcli [ -p—profile ] function-clause
[ -c—acsd_hostname [ :—acsd_port ] ] [ -l—acs-directory ]
[ -B—backup ID ] [ -s—DEVICE_CLASS ]
```

The values for the **function-clause** parameter are described in the following sections.

FlashCopy operations of custom applications: function-clause:

The following functions are supported by the **fcmcli** command option **-f** 'function' for FlashCopy Manager for Custom Applications backups of custom applications:

fcmcli command functions

```
►► -f backup [ -I—infile-name ] [ -E—pre-flash-command ]
[ -Q—post-flash-command ] [ -s—DEVICE_CLASS ]
```

The following functions are supported by the **fcmcli** command option **-f** function for FlashCopy restores, inquire, and delete of custom applications:

fcmcli command functions

```
►► -f restore [ -I—infile-name ] [ -B—backup ID ]
```

fcmcli command functions

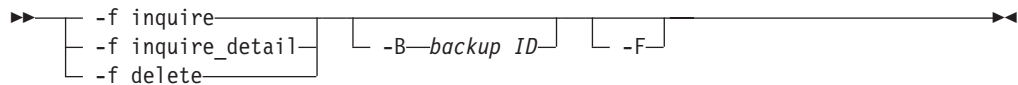


Table 30. Options for the Tivoli Storage FlashCopy Manager **fcmcli** command for custom applications

Option	Description	Default
-p profile	Full profile name.	INSTANCE_DIR/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
-l acs-directory	Directory where the logs and shared directories can be found.	ACS_DIR
-f backup	Back up a custom application.	
-f restore	Restore a regular DB2 snapshot backup (with advanced restore options) or restore a custom application backup.	
-E preflash command	<p>Overrides the value of the PRE_FLASH_CMD parameter as specified in the CLIENT section of the profile. The preflash command is run on the production server and can be a script. The return code of the preflash command is evaluated as follows:</p> <p>0 Successful. The Tivoli Storage FlashCopy Manager backup operation continues.</p> <p>Any value other than 0 Unsuccessful. The Tivoli Storage FlashCopy Manager backup operation stops.</p>	

Table 30. Options for the Tivoli Storage FlashCopy Manager **fcmlcli** command for custom applications (continued)

Option	Description	Default
-Q postflash command	<p>Overrides the value of the POST_FLASH_CMD parameter as specified in the CLIENT section of the profile. The postflash command is run on the production server and can be a script. The return code of the postflash command is evaluated as follows:</p> <p>0 Successful. The Tivoli Storage FlashCopy Manager backup operation continues.</p> <p>Any value other than 0 Unsuccessful. The Tivoli Storage FlashCopy Manager backup operation stops.</p>	
-I infile	<p>Overrides the value of the INFILE parameter as specified in the CLIENT section of the profile. The fcmlcli functions inquire, inquireDetails, and delete do not recognize the infile parameter. The function restore accepts infile as an optional parameter.</p>	
-F	<p>Use the force option with the inquire, inquire_detail, or delete functions. When used with inquire or inquire_detail, all available backups and all backups marked for deletion are displayed. When used with the delete function, the force option withdraws the source target FlashCopy relations on DS8000 or SAN Volume Controller.</p>	None.
-v	Display version.	
-h	Display help text.	
-B	The Backup ID as displayed by fcmlcli -f inquire [_detail] or db2acsutil .	None.
-s DEVICE_CLASS	The name of the DEVICE_CLASS section in the profile that is used for the backup operation.	As specified in the profile.

- The return code of the **fcmccli** command is *0* if it finishes the request without an error or if there were no candidates for the request.
- The return code is *1* if one or more minor issues occur that are not critical but must be checked to prevent major issues later.
- The return code is *2* indicating that an error occurred during the command execution.

The following sections describe the details of the various functions that are specified with the **-f** option of the Tivoli Storage FlashCopy Manager command, **fcmccli**.

-f backup

This command creates a FlashCopy backup of custom applications, such as a list of file systems that you provide.

Before and after snapshot creation, Tivoli Storage FlashCopy Manager can call a user exit that quiesces and resumes all applications that store data within those file systems.

When this command is called, it is also determined if the snapshot is retained locally (for disk-only backup) or backed up at a later time to Tivoli Storage Manager. As a backup method for the subsequent Tivoli Storage Manager backup, FlashCopy Manager for Custom Applications uses the Tivoli Storage Manager backup-archive client.

The following optional parameters can be used with the **fcmccli -f backup** command:

```
-I infile
-E preflash command
-Q postflash command
-s DEVICE_CLASS
```

-I *infile* specifies the name of a file that contains a list of all the objects that is processed by Tivoli Storage FlashCopy Manager.

-E *preflash command* specifies the name of a script or executable program that is called immediately before the snapshot. The pre-flash script is typically used to quiesce an application. The return code of the **preflash** command is evaluated as follows:

0 Successful. The Tivoli Storage FlashCopy Manager backup operation continues.

Any value other than 0

Unsuccessful. The Tivoli Storage FlashCopy Manager backup operation terminates.

-Q *postflash command* specifies the name of a script or executable program that is called immediately after the snapshot. The post-flash script is typically used to resume an application. The return code of the **postflash** command is evaluated as follows:

0 Successful. The Tivoli Storage FlashCopy Manager backup operation continues.

Any value other than 0

Unsuccessful. The Tivoli Storage FlashCopy Manager backup operation terminates.

-s *DEVICE_CLASS* specifies the name of the *DEVICE_CLASS* section in the profile that is used for the backup operation.

-f inquire

This command queries the backup repository and lists all available backups.

This command is of special interest in environments where multiple partitions reside on the same volume group, for volume sharing.

-f inquire_detail

This command queries the backup repository and lists all available backups.

This command is similar to **-f inquire** but prints additional information like usability states and background copy progress for each backup. This command is of special interest in environments where multiple partitions reside on the same volume group, for volume sharing.

-f delete

The delete function is used as part of the version control mechanism of Tivoli Storage FlashCopy Manager and can be called only by Tivoli Storage FlashCopy Manager itself or by a user. The delete function can be used only to delete full backups.

You can use the delete function to delete a snapshot. This task can take some time to process as it is carried out as a background asynchronous task. However, during this process the snapshot is no longer available for inquiry or restore operations. The snapshot backup remains visible in the storage device or GPFS file system until the snapshot is deleted by the background monitor.

The effect of the deletion on the snapshot or FlashCopy relations is dependent on the storage system and where applicable, the file system:

- IBM XIV Storage System, IBM System Storage N series, or NetApp, the snapshot is deleted asynchronously by the background monitor after the command is issued.
- IBM System Storage DS8000 and SAN Volume Controller the FlashCopy relationships between the source and target volumes are withdrawn after the command is issued. These relationships can be used for future backups. To delete these relationships, specify the -F option when you issue the delete command on these storage systems. The snapshot is deleted asynchronously by the background monitor.

The following example shows the command syntax to use as database instance owner on the production system:

```
./fcmcli -f delete [-F]
```

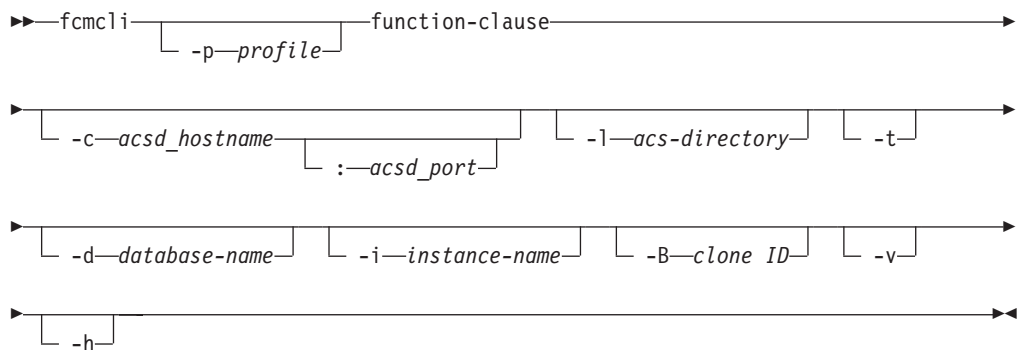
-f restore

For custom applications, you can use the **fccli -f restore** command to do a full or partial snapshot restore of the data that has been backed up.

- To restore a full snapshot, provide the backup ID of a particular snapshot backup by specifying the **-B backup-id** parameter. You can obtain the backup ID by using the **fccli -f inquire** command. To restore the latest backup, specify #NULL.
- To restore only a portion of the snapshot backup, Tivoli Storage FlashCopy Manager can also specify a list of files explicitly using the **-I <infile>** option. While Tivoli Storage FlashCopy Manager restores data at a volume level, additional data might be restored as part of the volume restore operation. You can use the **NEGATIVE_LIST** parameter to specify what action Tivoli Storage FlashCopy Manager takes in these situations.

Cloning commands

You can use the Tivoli Storage FlashCopy Manager command-line interface, **fccli**, to create and manage clones of DB2, Oracle, and SAP with Oracle databases. Cloning of DB2 pureScale and custom applications is not available.



Where:

-p profile

Full profile name. Default value: *INSTANCE_DIR/profile*

-c acsd_hostname

Name of the server where the management agent (acsd) is running. Default value: *localhost*.

acsd-port

TCP/IP port number or service name on which the management agent (acsd) is listening. Default value: *57328*.

-l acs-directory

Directory where the logs and shared directories are located. Default value: *ACS_DIR*.

-t Start trace on. Default value: Trace off.

-d database-name.

The name of the database.

-i instance-name

The name of the instance to apply action against. This parameter is required for the **-F** option. There are no limitations.

-B *clone ID*

The clone backup ID as displayed by **fccli -f inquire [_detail]** or **db2acsutil** command.

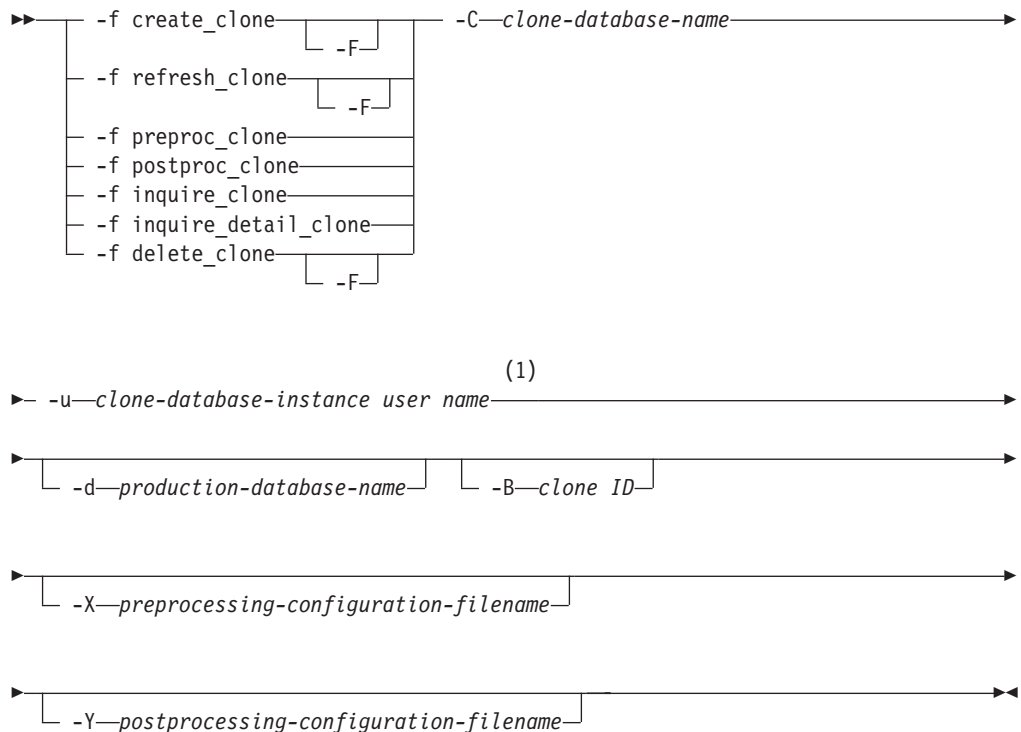
-v Show version.

-h Show help text.

The values for the function-clause parameter are described in the following sections.

FlashCopy cloning function-clauses

The following functions are supported by the fccli command option **-f** 'function' for FlashCopy cloning operations:



Notes:

- 1 This option is not required for **-f inquire_clone**, **-f inquire_detail_clone**, or **-f delete_clone** command.

Where:

- F** The force command option is optional. Depending on the cloning command it can have the following results:
 - delete_clone**: The force option causes the clone to be unmounted, marked as deleted, and also deletes the FlashCopy relationships. Otherwise, the **delete_clone** function unmounts the clone and marks it as deleted in the FlashCopy Manager repository.
 - create_clone, refresh_clone**: The force option deletes all backup versions that are older than the clone targets that are reused for the new or refreshed

clone. Otherwise, a failure can occur when there are backup versions older than the clone targets that are reused for the new or refreshed clone.

This option is valid for Storwize family and SAN Volume Controller Version 5.1, or later.

-C *clone-database-name*

The name of the cloned database on the clone system. This option must be specified for all cloning functions.

Specify a valid DB2 or Oracle database name. The *clone database name* can be the name of the production database or you can specify an alternative name.

Note: For DB2, the cloned database is only renamed and moved to the clone target instance, if the clone database name is different from the production database name.

-u *clone-database-instance user name*

Specify the user name of the clone instance owner. This option is required when the following functions are issued:

- **create_clone**
- **refresh_clone**
- **preproc_clone**
- **postproc_clone**

-d *production-database-name*

The name of the production database on the production system.

For Oracle, this option is not required. For DB2, it depends on the number of database entries in the database directory. If the DB2 database directory contains more than one entry, the **-d** production database name is required.

-B *clone ID*

The clone backup ID as displayed by **fcmlcli -f inquire [_detail]** or **db2acsutil** command.

-X *preprocessing-configuration-filename*

The name of the configuration file to be used with the preprocessing script. The preprocessing configuration file must be on the clone server.

-Y *postprocessing-configuration-filename.*

The name of the configuration file to be used with the postprocessing script. The postprocessing configuration file must be on the clone server.

The return code of the **fcmlcli** command is 0 if it finishes the request without an error or if there were no candidates for the request. The return code is 1 if one or more minor issues occur which are not critical but must be checked to prevent major issues later. Return code 2 indicates that an error occurred during the command execution.

Issue cloning-related commands on the production system as the production database instance owner. The cloning commands must be issued from the `INSTANCE_DIR` directory where the Tivoli Storage FlashCopy Manager production files are located. The **fcmlcli** command identifies the name of the production database in the following order:

1. For Oracle databases, the value of the `ORACLE_SID` environment variable is used to identify the production database name. For DB2 databases, the DB2 database directory is used. If only one entry exists in the database directory, this entry is used to identify the production database name.

2. If the `-d production database name` option is specified, this value overwrites the value that is identified in the previous step. Also, this value is used to identify the production database name. The command-line option `-d` is optional for Oracle. Its use with DB2 depends on the number of database entries in the database directory. If more than one entry is in the DB2 database directory, the `-d` option is required.

For a DB2 database the cloned database is not moved to the clone target instance, when the target database name is identical to the production database name. If required to move the cloned database, rename the database by providing an alternative name. For example, two database instances are created on the clone server, the production instance that is named *db2prodins* and the clone instance named *db2cloneins*. To clone the production database *PROD* and move it to the clone target instance, issue the following command:

```
fcmcli -f create_clone -C CLONE -u db2cloneins -d PROD
```

-f create_clone

This command creates a clone database.

The following actions occur when a clone database is created:

1. A consistent online FlashCopy backup of the production database (including online log files) is created.
2. The FlashCopy backup is mounted on the clone system. The following actions occur during this mount operation:
 - The physical devices on the clone server operating system (used as target volumes during the FlashCopy backup) are configured.
 - The volume groups on the physical devices are imported.
 - These file systems on the imported volume groups are mounted when the clone database is created:
 - Database file systems
 - All additional file systems involved in a FlashCopy operation
3. The database on the clone system is recovered.
4. The database is renamed to match the name of the clone database that resides on the clone system.
5. The clone database is started on the clone system.
6. (Optional) Postprocessing scripts are run against the new clone database.

If the clone database on the clone system exists, it must be shut down and unmounted when issuing this function. An error message and return code 2 are issued if the clone database is not shut down and unmounted. This example shows the syntax as database instance owner on the production system:

```
./fcmcli -f create_clone -u <clone instance owner user name>  
-C <clone database name> [-F]
```

-f inquire_clone

This command queries a clone database for the list all available backups.

This command is of special interest in Tivoli Storage FlashCopy Manager cloning operations. The following parameters are also required to perform the **-f inquire_clone** operation:

-d database-name
-C *<clone db name>*

-f inquire_detail_clone

This command queries the backup repository and lists all available backups.

This command works like **-f inquire_clone**. In addition, the command prints additional information like usability states and background copy progress for each backup. This command is of special interest in Tivoli Storage FlashCopy Manager cloning operations. The following parameters are also required in order to run the **-f inquire_detail_clone** command:

-d database-name
-C *<clone db name>*

-f delete_clone

This command unmounts and deletes a clone database that is created with the **create_clone** or **refresh_clone** function. Optionally, preprocessing scripts can run against the clone database that is to be deleted.

The processing of this command is also dependent on the storage system:

- IBM XIV Storage System, IBM System Storage N series, or NetApp, the snapshot is deleted asynchronously by the background monitor after the command is issued.
- IBM System Storage DS8000 and SAN Volume Controller the FlashCopy relationships between the source and target volumes are withdrawn after the command is issued. These relationships can be used for future backups. To delete these relationships, specify the **-F** option when you issue the delete command on these storage systems. The snapshot is deleted asynchronously by the background monitor.

The clone database on the clone system must be shut down to delete the database. An error message and return code 2 are issued if the clone database is not shut down. This example shows the syntax as database instance owner on the production system:

```
./fcmcli -f delete_clone -C <clone database name> [-F]
```

-f preproc_clone

Before the clone database is refreshed, this command runs preprocessing scripts against the clone database on the clone system.

When running this command the clone database on the clone system must be running. If the clone database is unavailable, an error message and return code 2 is displayed. This example shows the syntax as database instance owner on the production system:

```
./fcmcli -f preproc_clone -u <clone instance owner user ID>  
-C <clone database name> -X <preprocessing configuration file>
```

-f postproc_clone

After a clone database is created, this command runs postprocessing scripts on the clone system against the clone database.

When this function runs, the new clone database on the clone system must be available. If the clone database is not available, an error message and return code 2 is displayed. This example shows the syntax as database instance owner on the production system:

```
./fcmcli -f postproc_clone -u <clone instance owner user ID>  
-C <clone database name> -Y <postprocessing configuration file>
```

-f refresh_clone

This command refreshes an existing clone database.

When you enter the **-f refresh_clone** command, the software completes the following steps:

1. (Optional) If provided, preprocessing scripts run against the clone database (using the **-X** cloning parameter). If the clone database is not available, an error message and a return code 2 are displayed. When creating the preprocessing scripts, verify that the last preprocessing script shuts down the clone database. If the script does not shut down the database, during the next step, the **refresh_clone** command cannot successfully run.
2. The clone database is unmounted. If the clone database is not shut down, an error message and a return code 2 are displayed.
3. A new clone database is created.
4. (Optional) Postprocessing scripts run against the new clone database.

If the **-X** and **-Y** cloning parameters are not specified, no preprocessing and postprocessing scripts run. The **refresh_clone** command requires both the following conditions to be true:

- A clone database must exist and must have been created with the **create_clone** function.
- The clone database must be mounted on the clone system.

If either of these conditions is not met, an error message and a return code 2 are displayed. The following example provides the syntax that a database instance owner can use when running the commands from the production system:

```
./fcmcli -f refresh_clone -u <clone instance owner user ID>  
-C <clone database name> [-X <preprocessing configuration file>]  
[-Y <postprocessing configuration file>] [-F]
```

Deleting Tivoli Storage FlashCopy Manager snapshot backups

Tivoli Storage FlashCopy Manager snapshot backups can be deleted from the snapshot repository.

Before you begin

Optionally, you can delete snapshot backups on DS8000 and SAN Volume Controller storage subsystems that contain a dedicated set of target volumes in one or more target sets. With IBM XIV Storage System, IBM System Storage N series, and NetApp storage solutions you can create as many snapshot backups as needed, and old backups are manually deleted. Old backups can also be deleted automatically by using the **MAX_VERSIONS** (**MAX_SNAPSHOT_VERSIONS**) parameter.

In a DB2 pureScale environment, you can create as many GPFS file system snapshot backups as needed, and manually delete old backups. You can automatically delete these snapshots by using the **MAX_VERSIONS** (**MAX_SNAPSHOT_VERSIONS**) parameter.

About this task

Manually delete a Tivoli Storage FlashCopy Manager snapshot backup by following the procedure.

1. Run the following command to unmount the file systems and export the volume groups on a backup system. This method is used when the backup that is using this target set is currently mounted. This step can be omitted if the backup is not currently mounted.

```
fccli -f unmount [-B <backupID>]
```

2. Based on the use of this target set, any existing source, and target FlashCopy relationships (such as INCR or NOCOPY) must be withdrawn. Run the appropriate command:

- (DB2) db2acsutil delete
- (Oracle) acsora -f delete -B <backupID>
- (Oracle in an SAP environment) backint -f delete -B <backupID>
- (Custom applications) fccli -f delete -B <backupID>

Note: (IBM XIV Storage System, IBM System Storage N series, and NetApp): These commands delete the snapshot backup in the Tivoli Storage FlashCopy Manager snapshot repository, and the snapshot on the storage system is also deleted.

Note: (DS8000 or SAN Volume Controller): These commands delete the snapshot backup in the Tivoli Storage FlashCopy Manager snapshot repository only. The source and target relations on DS8000 or SAN Volume Controller are not withdrawn.

Note: In a DB2 pureScale environment, these commands delete the GPFS file system snapshot in the Tivoli Storage FlashCopy Manager snapshot repository. The snapshot is deleted from the file system asynchronously by the background monitor.

To remove a target volume from a target set or to remove a complete target set, run the following steps to free up the target volumes:

1. Run the following command to unmount the file systems and export the volume groups on a backup system. This method is used when the backup that is using this target set is mounted:

```
fccli -f unmount [-B <backupID>]
```

This step can be omitted if the backup is not mounted.

2. Based on the use of this target set, any existing source, and target FlashCopy relationships (such as INCR or NOCOPY) must be withdrawn. Run the appropriate command:

- (DB2) db2acsutil delete options "DELETE_FORCE"
- (Oracle) acsora -f delete -F -B <backupID>
- (Oracle in an SAP environment) backint -f delete -F -B <backupID>
- (Custom applications) fccli -f delete -B <backupID> -F

The withdrawal of the source and target FlashCopy relationship is done by the Tivoli Storage FlashCopy Manager generic device agent, acsngen, as a background operation. This process can take up to 10 minutes. Do not try to reuse the target volumes before the actual process completes successfully.

Snapshot backup status in the Tivoli Storage FlashCopy Manager repository

Ensure that you routinely check the status of the Tivoli Storage FlashCopy Manager repository.

To check the status of snapshot backups in the Tivoli Storage FlashCopy Manager repository, use one of the following commands:

- (DB2) `fccli -f inquire[_detail]`
- (DB2) `db2acsutil query status`
- (Oracle) `acsora -f inquire[_detail]`
- (Oracle) `acsutil`
- (Oracle in an SAP environment) `backint -f inquire[_detail] -t volume|file -p <SAP Backint profile (.utl)>`
- (Oracle in an SAP environment) `acsutil`
- (Custom applications) `fccli -f inquire[_detail]`

When using the `inquire_detail` command with the appropriate tool, output similar to the following displays:

```
Type Partition Backup-ID TSM Backup-ID State
DevClass TargetSet Background Copy BytestobeFlashcopied
#BACKUP NODE0000 C01__A0FY303K6B IN-PROGRESS MIRROR1 1 3.000GB of 3.000GB
3.000GB

UsabilityStates :
REMOTELY_MOUNTABLE,REPETITIVELY_RESTORABLE,SWAP-RESTORABLE,PHYSICAL_PROTECTION,
FULL_COPY,TAPE_BACKUP_PENDING
```

Tip: The `db2acsutil query status` command does not show all information that is shown by the `inquire_detail` command. That is because `db2acsutil` is a tool delivered by DB2 which only knows a subset of all possible states that can be set by Tivoli Storage FlashCopy Manager.

Appendix E. Accessibility features for the Tivoli Storage Manager product family

Accessibility features help users who have a disability, such as restricted mobility or limited vision to use information technology products successfully.

Accessibility features

The IBM Tivoli Storage Manager family of products includes the following accessibility features:

- Keyboard-only operation using standard operating-system conventions
- Interfaces that support assistive technology such as screen readers

The command-line interfaces of all products in the product family are accessible.

Tivoli Storage Manager Operations Center provides the following additional accessibility features when you use it with a Mozilla Firefox browser on a Microsoft Windows system:

- Screen magnifiers and content zooming
- High contrast mode

The Operations Center and the Tivoli Storage Manager Server can be installed in console mode, which is accessible.

The Operations Center help system is enabled for accessibility. For more information, click the question mark icon on the help system menu bar.

Vendor software

The Tivoli Storage Manager product family 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.

IBM and accessibility

See the IBM Human Ability and Accessibility Center (<http://www.ibm.com/able>) for information about the commitment that IBM has to accessibility.

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:

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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 want 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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and `ibm.com`® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at <http://www.ibm.com/legal/copytrade.shtml>.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.



Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

SAP is a trademark or registered trademark of SAP AG in Germany and in several other countries.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.

Glossary

This glossary provides terms and definitions for Tivoli Storage Manager, Tivoli Storage FlashCopy Manager, and associated products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (<http://www.ibm.com/software/globalization/terminology>).

A

absolute mode

In storage management, a backup copy-group mode that specifies that a file is considered for incremental backup even if the file has not changed since the last backup. See also mode, modified mode.

access control list (ACL)

In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access mode

An attribute of a storage pool or a storage volume that specifies whether the server can write to or read from the storage pool or storage volume.

ACK See acknowledgment.

acknowledgment (ACK)

The transmission of acknowledgment characters as a positive response to a data transmission.

ACL See access control list.

activate

To validate the contents of a policy set and then make it the active policy set.

active-data pool

A named set of storage pool volumes that contain only active versions of client

backup data. See also server storage, storage pool, storage pool volume.

active file system

A file system to which space management has been added. With space management, tasks for an active file system include automatic migration, reconciliation, selective migration, and recall. See also inactive file system.

active policy set

The activated policy set that contains the policy rules currently in use by all client nodes assigned to the policy domain. See also policy domain, policy set.

active version

The most recent backup copy of a file stored. The active version of a file cannot be deleted until a backup process detects that the user has either replaced the file with a newer version or has deleted the file from the file server or workstation. See also backup version, inactive version.

activity log

A log that records normal activity messages that are generated by the server. These messages include information about server and client operations, such as the start time of sessions or device I/O errors.

adaptive subfile backup

A type of backup that sends only changed portions of a file to the server, instead of sending the entire file. Adaptive subfile backup reduces network traffic and increases the speed of the backup.

administrative client

A program that runs on a file server, workstation, or mainframe that administrators use to control and monitor the server. See also backup-archive client.

administrative command schedule

A database record that describes the planned processing of an administrative command during a specific time period. See also central scheduler, client schedule, schedule.

administrative privilege class

See privilege class.

administrative session

A period of time during which an administrator user ID communicates with a server to perform administrative tasks. See also client node session, session.

administrator

A person responsible for administrative tasks such as access authorization and content management. Administrators can also grant levels of authority to users.

agent node

A client node that has been granted proxy authority to perform operations on behalf of another client node, which is the target node.

aggregate

An object, stored in one or more storage pools, consisting of a group of logical files that are packaged together. See also logical file, physical file.

aggregate data transfer rate

A performance statistic that indicates the average number of bytes that were transferred per second while processing a given operation.

application client

A program that is installed on a system to protect an application. The server provides backup services to an application client.

archive

To copy programs, data, or files to another storage media, usually for long-term storage or security. See also retrieve.

archive copy

A file or group of files that was archived to server storage

archive copy group

A policy object containing attributes that control the generation, destination, and expiration of archived files. See also copy group.

archive-retention grace period

The number of days that the storage manager retains an archived file when the server is unable to rebind the file to an appropriate management class. See also bind.

association

The defined relationship between a client

node and a client schedule. An association identifies the name of a schedule, the name of the policy domain to which the schedule belongs, and the name of a client node that performs scheduled operations.

audit

To check for logical inconsistencies between information that the server has and the actual condition of the system. The storage manager can audit information about items such as volumes, libraries, and licenses. For example, when a storage manager audits a volume, the server checks for inconsistencies between information about backed-up or archived files that are stored in the database and the actual data that are associated with each backup version or archive copy in server storage.

authentication rule

A specification that another user can use to either restore or retrieve files from storage.

authority

The right to access objects, resources, or functions. See also privilege class.

authorization rule

A specification that permits another user to either restore or retrieve a user's files from storage.

authorized user

A user who has administrative authority for the client on a workstation. This user changes passwords, performs open registrations, and deletes file spaces.

AutoFS

See automounted file system.

automatic detection

A feature that detects, reports, and updates the serial number of a drive or library in the database when the path from the local server is defined.

automatic migration

The process that is used to automatically move files from a local file system to storage, based on options and settings that are chosen by a root user on a workstation. See also demand migration, threshold migration.

automounted file system (AutoFS)

A file system that is managed by an

automounter daemon. The automounter daemon monitors a specified directory path, and automatically mounts the file system to access data.

B

backup-archive client

A program that runs on a workstation or file server and provides a means for users to back up, archive, restore, and retrieve files. See also administrative client.

backup copy group

A policy object containing attributes that control the generation, destination, and expiration of backup versions of files. A backup copy group belongs to a management class. See also copy group.

backup retention grace period

The number of days the storage manager retains a backup version after the server is unable to rebind the file to an appropriate management class.

backup set

A portable, consolidated group of active versions of backup files that are generated for a backup-archive client.

backup set collection

A group of backup sets that are created at the same time and which have the same backup set name, volume names, description, and device classes. The server identifies each backup set in the collection by its node name, backup set name, and file type.

backup version

A file or directory that a client node backed up to storage. More than one backup version can exist in storage, but only one backup version is the active version. See also active version, copy group, inactive version.

bind To associate a file with a management class name. See also archive-retention grace period, management class, rebind.

C

cache To place a duplicate copy of a file on random access media when the server migrates a file to another storage pool in the hierarchy.

cache file

A snapshot of a logical volume created by Logical Volume Snapshot Agent. Blocks are saved immediately before they are modified during the image backup and their logical extents are saved in the cache files.

CAD See client acceptor daemon.

central scheduler

A function that permits an administrator to schedule client operations and administrative commands. The operations can be scheduled to occur periodically or on a specific date. See also administrative command schedule, client schedule.

client A software program or computer that requests services from a server. See also server.

client acceptor

A service that serves the Java applet for the web client to web browsers. On Windows systems, the client acceptor is installed and run as a service. On AIX, UNIX, and Linux systems, the client acceptor is run as a daemon.

client acceptor daemon (CAD)

See client acceptor.

client domain

The set of drives, file systems, or volumes that the user selects to back up or archive data, using the backup-archive client.

client node

A file server or workstation on which the backup-archive client program has been installed, and which has been registered to the server.

client node session

A session in which a client node communicates with a server to perform backup, restore, archive, retrieve, migrate, or recall requests. See also administrative session.

client option set

A group of options that are defined on

the server and used on client nodes in conjunction with client options files.

client options file

An editable file that identifies the server and communication method, and provides the configuration for backup, archive, hierarchical storage management, and scheduling.

client-polling scheduling mode

A method of operation in which the client queries the server for work. See also server-prompted scheduling mode.

client schedule

A database record that describes the planned processing of a client operation during a specific time period. The client operation can be a backup, archive, restore, or retrieve operation, a client operating system command, or a macro. See also administrative command schedule, central scheduler, schedule.

client/server

Pertaining to the model of interaction in distributed data processing in which a program on one computer sends a request to a program on another computer and awaits a response. The requesting program is called a client; the answering program is called a server.

client system-options file

A file, used on AIX, UNIX, or Linux system clients, containing a set of processing options that identify the servers to be contacted for services. This file also specifies communication methods and options for backup, archive, hierarchical storage management, and scheduling. See also client user-options file, options file.

client user-options file

A file that contains the set of processing options that the clients on the system use. The set can include options that determine the server that the client contacts, and options that affect backup operations, archive operations, hierarchical storage management operations, and scheduled operations. This file is also called the dsm.opt file. For AIX, UNIX, or Linux systems, see also client system-options file. See also client system-options file, options file.

closed registration

A registration process in which only an administrator can register workstations as client nodes with the server. See also open registration.

collocation

The process of keeping all data belonging to a single-client file space, a single client node, or a group of client nodes on a minimal number of sequential-access volumes within a storage pool.

Collocation can reduce the number of volumes that must be accessed when a large amount of data must be restored.

collocation group

A user-defined group of client nodes whose data is stored on a minimal number of volumes through the process of collocation.

commit point

A point in time when data is considered to be consistent.

communication method

The method by which a client and server exchange information. See also Transmission Control Protocol/Internet Protocol.

communication protocol

A set of defined interfaces that permit computers to communicate with each other.

compression

A function that removes repetitive characters, spaces, strings of characters, or binary data from the data being processed and replaces characters with control characters. Compression reduces the amount of storage space that is required for data.

configuration manager

A server that distributes configuration information, such as policies and schedules, to managed servers according to their profiles. Configuration information can include policy and schedules. See also enterprise configuration, managed server, profile.

conversation

A connection between two programs over a session that allows them to communicate with each other while processing a transaction. See also session.

copy backup

A full backup in which the transaction log files are not deleted so that backup procedures that use incremental or differential backups are not disrupted.

copy group

A policy object containing attributes that control how backup versions or archive copies are generated, where backup versions or archive copies are initially located, and when backup versions or archive copies expire. A copy group belongs to a management class. See also archive copy group, backup copy group, backup version, management class.

copy storage pool

A named set of volumes that contain copies of files that reside in primary storage pools. Copy storage pools are used only to back up the data that is stored in primary storage pools. A copy storage pool cannot be a destination for a backup copy group, an archive copy group, or a management class (for space-managed files). See also destination, primary storage pool, server storage, storage pool, storage pool volume.

D**daemon**

A program that runs unattended to perform continuous or periodic functions, such as network control.

damaged file

A physical file in which read errors have been detected.

database backup series

One full backup of the database, plus up to 32 incremental backups made since that full backup. Each full backup that is run starts a new database backup series. A number identifies each backup series. See also database snapshot, full backup.

database snapshot

A complete backup of the entire database to media that can be taken off-site. When a database snapshot is created, the current database backup series is not interrupted. A database snapshot cannot have incremental database backups associated with it. See also database backup series, full backup.

data center

In a virtualized environment, a container that holds hosts, clusters, networks, and data stores.

data deduplication

A method of reducing storage needs by eliminating redundant data. Only one instance of the data is retained on storage media. Other instances of the same data are replaced with a pointer to the retained instance.

data manager server

A server that collects metadata information for client inventory and manages transactions for the storage agent over the local area network. The data manager server informs the storage agent with applicable library attributes and the target volume identifier.

data mover

A device that moves data on behalf of the server. A network-attached storage (NAS) file server is a data mover.

data storage-management application-programming interface (DSMAPI)

A set of functions and semantics that can monitor events on files, and manage and maintain the data in a file. In an HSM environment, a DSMAPI uses events to notify data management applications about operations on files, stores arbitrary attribute information with a file, supports managed regions in a file, and uses DSMAPI access rights to control access to a file object.

data store

In a virtualized environment, the location where virtual machine data is stored.

deduplication

The process of creating representative records from a set of records that have been identified as representing the same entities.

default management class

A management class that is assigned to a policy set. This class is used to govern backed up or archived files when a file is not explicitly associated with a specific management class through the include-exclude list.

demand migration

The process that is used to respond to an

out-of-space condition on a file system for which hierarchical storage management (HSM) is active. Files are migrated to server storage until space usage drops to the low threshold that was set for the file system. If the high threshold and low threshold are the same, one file is migrated. See also automatic migration, selective migration, threshold migration.

destination

A copy group or management class attribute that specifies the primary storage pool to which a client file will be backed up, archived, or migrated. See also copy storage pool.

device class

A named set of characteristics that are applied to a group of storage devices. Each device class has a unique name and represents a device type of disk, file, optical disk, or tape.

device configuration file

1. For a storage agent, a file that contains the name and password of the storage agent, and information about the server that is managing the SAN-attached libraries and drives that the storage agent uses.
2. For a server, a file that contains information about defined device classes, and, on some servers, defined libraries and drives. The information is a copy of the device configuration information in the database.

disaster recovery manager (DRM)

A function that assists in preparing and using a disaster recovery plan file for the server.

disaster recovery plan

A file that is created by the disaster recover manager (DRM) that contains information about how to recover computer systems if a disaster occurs and scripts that can be run to perform some recovery tasks. The file includes information about the software and hardware that is used by the server, and the location of recovery media.

domain

A grouping of client nodes with one or

more policy sets, which manage data or storage resources for the client nodes. See also policy domain.

DRM See disaster recovery manager.

DSMAPI

See data storage-management application-programming interface.

dynamic serialization

Copy serialization in which a file or folder is backed up or archived on the first attempt regardless of whether it changes during a backup or archive. See also shared dynamic serialization, shared static serialization, static serialization.

E

EA See extended attribute.

EB See exabyte.

EFS See Encrypted File System.

Encrypted File System (EFS)

A file system that uses file system-level encryption.

enterprise configuration

A method of setting up servers so that the administrator can distribute the configuration of one of the servers to the other servers, using server-to-server communication. See also configuration manager, managed server, profile, subscription.

enterprise logging

The process of sending events from a server to a designated event server. The event server routes the events to designated receivers, such as to a user exit. See also event.

error log

A data set or file that is used to record error information about a product or system.

estimated capacity

The available space, in megabytes, of a storage pool.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process. See also enterprise logging, receiver.

event record

A database record that describes actual status and results for events.

event server

A server to which other servers can send events for logging. The event server routes the events to any receivers that are enabled for the sending server's events.

exabyte (EB)

For processor, real and virtual storage capacities and channel volume, 2 to the power of 60 or 1 152 921 504 606 846 976 bytes. For disk storage capacity and communications volume, 1 000 000 000 000 000 000 bytes.

exclude

The process of identifying files in an include-exclude list. This process prevents the files from being backed up or migrated whenever a user or schedule enters an incremental or selective backup operation. A file can be excluded from backup, from space management, or from both backup and space management.

exclude-include list

See include-exclude list.

expiration

The process by which files, data sets, or objects are identified for deletion because their expiration date or retention period has passed.

expiring file

A migrated or premigrated file that has been marked for expiration and removal from storage. If a stub file or an original copy of a premigrated file is deleted from a local file system, or if the original copy of a premigrated file is updated, the corresponding migrated or premigrated file is marked for expiration the next time reconciliation is run.

extend

To increase the portion of available space that can be used to store database or recovery log information.

extended attribute (EA)

Names or value pairs that are associated with files or directories. There are three classes of extended attributes: user attributes, system attributes, and trusted attributes.

external library

A collection of drives that is managed by the media-management system other than the storage management server.

F**file access time**

On AIX, UNIX, or Linux systems, the time when the file was last accessed.

file age

For migration prioritization purposes, the number of days since a file was last accessed.

file device type

A device type that specifies the use of sequential access files on disk storage as volumes.

file server

A dedicated computer and its peripheral storage devices that are connected to a local area network that stores programs and files that are shared by users on the network.

file space

A logical space in server storage that contains a group of files that have been backed up or archived by a client node, from a single logical partition, file system, or virtual mount point. Client nodes can restore, retrieve, or delete their file spaces from server storage. In server storage, files belonging to a single file space are not necessarily stored together.

file space ID (FSID)

A unique numeric identifier that the server assigns to a file space when it is stored in server storage.

file state

The space management mode of a file that resides in a file system to which space management has been added. A file can be in one of three states: resident, premigrated, or migrated. See also migrated file, premigrated file, resident file.

file system migrator (FSM)

A kernel extension that intercepts all file system operations and provides any space management support that is required. If no space management support is required, the operation is passed to the

operating system, which performs its normal functions. The file system migrator is mounted over a file system when space management is added to the file system.

file system state

The storage management mode of a file system that resides on a workstation on which the hierarchical storage management (HSM) client is installed. A file system can be in one of these states: native, active, inactive, or global inactive.

frequency

A copy group attribute that specifies the minimum interval, in days, between incremental backups.

FSID See file space ID.

FSM See file system migrator.

full backup

The process of backing up the entire server database. A full backup begins a new database backup series. See also database backup series, database snapshot, incremental backup.

fuzzy backup

A backup version of a file that might not accurately reflect what is currently in the file because the file was backed up at the same time as it was being modified.

fuzzy copy

A backup version or archive copy of a file that might not accurately reflect the original contents of the file because it was backed up or archived the file while the file was being modified.

G

GB See gigabyte.

General Parallel File System (GPFS)

A high-performance shared-disk file system that can provide data access from nodes in a clustered system environment. See also information lifecycle management.

gigabyte (GB)

For processor storage, real and virtual storage, and channel volume, two to the power of 30 or 1,073,741,824 bytes. For disk storage capacity and communications volume, 1,000,000,000 bytes.

global inactive state

The state of all file systems to which space management has been added when space management is globally deactivated for a client node.

Globally Unique Identifier (GUID)

An algorithmically determined number that uniquely identifies an entity within a system. See also Universally Unique Identifier.

GPFS See General Parallel File System.

GPFS node set

A mounted, defined group of GPFS file systems.

group backup

The backup of a group containing a list of files from one or more file space origins.

GUID See Globally Unique Identifier.

H**hierarchical storage management (HSM)**

A function that automatically distributes and manages data on disk, tape, or both by regarding devices of these types and potentially others as levels in a storage hierarchy that range from fast, expensive devices to slower, cheaper, and possibly removable devices. The objectives are to minimize access time to data and maximize available media capacity. See also hierarchical storage management client, recall, storage hierarchy.

hierarchical storage management client (HSM client)

A client program that works with the server to provide hierarchical storage management (HSM) for a system. See also hierarchical storage management, management class.

HSM See hierarchical storage management.

HSM client

See hierarchical storage management client.

I

ILM See information lifecycle management.

image A file system or raw logical volume that is backed up as a single object.

image backup
A backup of a full file system or raw logical volume as a single object.

inactive file system
A file system for which space management has been deactivated. See also active file system.

inactive version
A backup version of a file that is either not the most recent backup version, or that is a backup version of a file that no longer exists on the client system. Inactive backup versions are eligible for expiration processing according to the management class assigned to the file. See also active version, backup version.

include-exclude file
A file containing statements to determine the files to back up and the associated management classes to use for backup or archive. See also include-exclude list.

include-exclude list
A list of options that include or exclude selected files for backup. An exclude option identifies files that should not be backed up. An include option identifies files that are exempt from the exclusion rules or assigns a management class to a file or a group of files for backup or archive services. See also include-exclude file.

incremental backup
The process of backing up files or directories, or copying pages in the database, that are new or changed since the last full or incremental backup. See also selective backup.

individual mailbox restore
See mailbox restore.

information lifecycle management (ILM)
A policy-based file-management system for storage pools and file sets. See also General Parallel File System.

inode The internal structure that describes the individual files on AIX, UNIX, or Linux

systems. An inode contains the node, type, owner, and location of a file.

inode number
A number specifying a particular inode file in the file system.

IP address
A unique address for a device or logical unit on a network that uses the Internet Protocol standard.

J

job file
A generated file that contains configuration information for a migration job. The file is XML format and can be created and edited in the hierarchical storage management (HSM) client for Windows client graphical user interface. See also migration job.

journal-based backup
A method for backing up Windows clients and AIX clients that exploits the change notification mechanism in a file to improve incremental backup performance by reducing the need to fully scan the file system.

journal daemon
On AIX, UNIX, or Linux systems, a program that tracks change activity for files residing in file systems.

journal service
In Microsoft Windows, a program that tracks change activity for files residing in file systems.

K

KB See kilobyte.

kilobyte (KB)
For processor storage, real and virtual storage, and channel volume, 2 to the power of 10 or 1,024 bytes. For disk storage capacity and communications volume, 1,000 bytes.

L

LAN See local area network.

LAN-free data movement

The movement of client data between a client system and a storage device on a storage area network (SAN), bypassing the local area network.

LAN-free data transfer

See LAN-free data movement.

leader data

Bytes of data, from the beginning of a migrated file, that are stored in the file's corresponding stub file on the local file system. The amount of leader data that is stored in a stub file depends on the stub size that is specified.

library

1. A repository for demountable recorded media, such as magnetic disks and magnetic tapes.
2. A collection of one or more drives, and possibly robotic devices (depending on the library type), which can be used to access storage volumes.

library client

A server that uses server-to-server communication to access a library that is managed by another storage management server. See also library manager.

library manager

A server that controls device operations when multiple storage management servers share a storage device. See also library client.

local

1. Pertaining to a device, file, or system that is accessed directly from a user system, without the use of a communication line. See also remote.
2. For hierarchical storage management products, pertaining to the destination of migrated files that are being moved. See also remote.

local area network (LAN)

A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

local shadow volume

Data that is stored on shadow volumes localized to a disk storage subsystem.

LOFS See loopback virtual file system.

logical file

A file that is stored in one or more server storage pools, either by itself or as part of an aggregate. See also aggregate, physical file, physical occupancy.

logical occupancy

The space that is used by logical files in a storage pool. This space does not include the unused space created when logical files are deleted from aggregate files, so it might be less than the physical occupancy. See also physical occupancy.

logical unit number (LUN)

In the Small Computer System Interface (SCSI) standard, a unique identifier used to differentiate devices, each of which is a logical unit (LU).

logical volume

A portion of a physical volume that contains a file system.

logical volume backup

A back up of a file system or logical volume as a single object.

Logical Volume Snapshot Agent (LVSA)

Software that can act as the snapshot provider for creating a snapshot of a logical volume during an online image backup.

loopback virtual file system (LOFS)

A file system that is created by mounting a directory over another local directory, also known as mount-over-mount. A LOFS can also be generated using an automounter.

LUN See logical unit number.

LVSA See Logical Volume Snapshot Agent.

M

macro file

A file that contains one or more storage manager administrative commands, which can be run only from an administrative client using the MACRO command. See also Tivoli Storage Manager command script.

mailbox restore

A function that restores Microsoft Exchange Server data (from IBM Data Protection for Microsoft Exchange backups) at the mailbox level or mailbox-item level.

managed object

A definition in the database of a managed server that was distributed to the managed server by a configuration manager. When a managed server subscribes to a profile, all objects that are associated with that profile become managed objects in the database of the managed server.

managed server

A server that receives configuration information from a configuration manager using a subscription to one or more profiles. Configuration information can include definitions of objects such as policy and schedules. See also configuration manager, enterprise configuration, profile, subscription.

management class

A policy object that users can bind to each file to specify how the server manages the file. The management class can contain a backup copy group, an archive copy group, and space management attributes. See also bind, copy group, hierarchical storage management client, policy set, rebind.

maximum transmission unit (MTU)

The largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the maximum transmission unit for Ethernet is 1500 bytes.

MB See megabyte.

media server

In a z/OS® environment, a program that provides access to z/OS disk and tape

storage for Tivoli Storage Manager servers that run on operating systems other than z/OS.

megabyte (MB)

For processor storage, real and virtual storage, and channel volume, 2 to the 20th power or 1,048,576 bytes. For disk storage capacity and communications volume, 1,000,000 bytes.

metadata

Data that describes the characteristics of data; descriptive data.

migrate

To move data to another location, or an application to another computer system.

migrated file

A file that has been copied from a local file system to storage. For HSM clients on UNIX or Linux systems, the file is replaced with a stub file on the local file system. On Windows systems, creation of the stub file is optional. See also file state, premigrated file, resident file, stub file.

migration

The process of moving data from one computer system to another, or an application to another computer system.

migration job

A specification of files to migrate, and actions to perform on the original files after migration. See also job file, threshold migration.

migration threshold

High and low capacities for storage pools or file systems, expressed as percentages, at which migration is set to start and stop.

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.

mode

A copy group attribute that specifies whether to back up a file that has not been modified since the last time the file was backed up. See also absolute mode, modified mode.

modified mode

In storage management, a backup copy-group mode that specifies that a file

is considered for incremental backup only if it has changed since the last backup. A file is considered a changed file if the date, size, owner, or permissions of the file have changed. See also absolute mode, mode.

mount limit

The maximum number of volumes that can be simultaneously accessed from the same device class. The mount limit determines the maximum number of mount points. See also mount point.

mount point

A logical drive through which volumes are accessed in a sequential access device class. For removable media device types, such as tape, a mount point is a logical drive associated with a physical drive. For the file device type, a mount point is a logical drive associated with an I/O stream. See also mount limit.

mount retention period

The maximum number of minutes that the server retains a mounted sequential-access media volume that is not being used before it dismounts the sequential-access media volume.

mount wait period

The maximum number of minutes that the server waits for a sequential-access volume mount request to be satisfied before canceling the request.

MTU See maximum transmission unit.

N

Nagle algorithm

An algorithm that reduces congestion of TCP/IP networks by combining smaller packets and sending them together.

named pipe

A type of interprocess communication that permits message data streams to pass between peer processes, such as between a client and a server.

NAS file server

See network-attached storage file server.

NAS file server node

See NAS node.

NAS node

A client node that is a network-attached

storage (NAS) file server. Data for the NAS node is transferred by a NAS file server that is controlled by the network data management protocol (NDMP). A NAS node is also called a NAS file server node.

native file system

A file system that is locally added to the file server and is not added for space management. The hierarchical storage manager (HSM) client does not provide space management services to the file system.

native format

A format of data that is written to a storage pool directly by the server. See also non-native data format.

NDMP

See Network Data Management Protocol.

NetBIOS (Network Basic Input/Output System)

A standard interface to networks and personal computers that is used on local area networks to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not have to handle the details of LAN data link control (DLC) protocols.

network-attached storage file server (NAS file server)

A dedicated storage device with an operating system that is optimized for file-serving functions. A NAS file server can have the characteristics of both a node and a data mover.

Network Basic Input/Output System

See NetBIOS.

Network Data Management Protocol (NDMP)

A protocol that allows a network storage-management application to control the backup and recovery of an NDMP-compliant file server, without installing vendor-acquired software on that file server.

network data-transfer rate

A rate that is calculated by dividing the total number of bytes that are transferred by the data transfer time. For example, this rate can be the time that is spent transferring data over a network.

node A file server or workstation on which the

backup-archive client program has been installed, and which has been registered to the server.

node name

A unique name that is used to identify a workstation, file server, or PC to the server.

node privilege class

A privilege class that gives an administrator the authority to remotely access backup-archive clients for a specific client node or for all clients in a policy domain. See also privilege class.

non-native data format

A format of data that is written to a storage pool that differs from the format that the server uses for operations. See also native format.

O

offline volume backup

A backup in which the volume is locked so that no other system applications can access it during the backup operation.

online volume backup

A backup in which the volume is available to other system applications during the backup operation.

open registration

A registration process in which users can register their workstations as client nodes with the server. See also closed registration.

operator privilege class

A privilege class that gives an administrator the authority to disable or halt the server, enable the server, cancel server processes, and manage removable media. See also privilege class.

options file

A file that contains processing options. See also client system-options file, client user-options file.

originating file system

The file system from which a file was migrated. When a file is recalled, it is returned to its originating file system.

orphaned stub file

A file for which no migrated file can be found on the server that the client node is

contacting for space management services. For example, a stub file can be orphaned when the client system-options file is modified to contact a server that is different than the one to which the file was migrated.

P

packet In data communication, a sequence of binary digits, including data and control signals, that are transmitted and switched as a composite whole.

page A defined unit of space on a storage medium or within a database volume.

partial-file recall mode

A recall mode that causes the hierarchical storage management (HSM) function to read just a portion of a migrated file from storage, as requested by the application accessing the file.

password generation

A process that creates and stores a new password in an encrypted password file when the old password expires. Automatic generation of a password prevents password prompting.

path An object that defines a one-to-one relationship between a source and a destination. Using the path, the source accesses the destination. Data can flow from the source to the destination, and back. An example of a source is a data mover (such as a network-attached storage [NAS] file server), and an example of a destination is a tape drive.

pattern-matching character

See wildcard character.

physical file

A file that is stored in one or more storage pools, consisting of either a single logical file, or a group of logical files that are packaged together as an aggregate. See also aggregate, logical file, physical occupancy.

physical occupancy

The amount of space that is used by physical files in a storage pool. This space includes the unused space that is created when logical files are deleted from aggregates. See also logical file, logical occupancy, physical file.

plug-in

A separately installable software module that adds function to an existing program, application, or interface.

policy domain

A grouping of policy users with one or more policy sets, which manage data or storage resources for the users. The users are client nodes that are associated with the policy domain. See also active policy set, domain.

policy privilege class

A privilege class that gives an administrator the authority to manage policy objects, register client nodes, and schedule client operations for client nodes. Authority can be restricted to certain policy domains. See also privilege class.

policy set

A group of rules in a policy domain. The rules specify how data or storage resources are automatically managed for client nodes in the policy domain. Rules can be contained in management classes. See also active policy set, management class.

premigrated file

A file that has been copied to server storage, but has not been replaced with a stub file on the local file system. An identical copy of the file resides both on the local file system and in server storage. Premigrated files occur on UNIX and Linux file systems to which space management has been added. See also file state, migrated file, resident file.

premigrated files database

A database that contains information about each file that has been premigrated to server storage.

premigration

The process of copying files that are eligible for migration to server storage, but leaving the original file intact on the local file system.

premigration percentage

A space management setting that controls whether the next eligible candidates in a file system are premigrated following threshold or demand migration.

primary site

A physical or virtual site that is made up of hardware, network, and storage resources. Typically, production operations run at the primary site. Data can be replicated to a secondary site for disaster recovery and failover operations. See also secondary site.

primary storage pool

A named set of volumes that the server uses to store backup versions of files, archive copies of files, and files migrated from client nodes. See also copy storage pool, server storage, storage pool, storage pool volume.

privilege class

A level of authority that is granted to an administrator. The privilege class determines which administrative tasks the administrator can perform. See also authority, node privilege class, operator privilege class, policy privilege class, storage privilege class, system privilege class.

profile

A named group of configuration information that can be distributed from a configuration manager when a managed server subscribes. Configuration information can include registered administrator IDs, policies, client schedules, client option sets, administrative schedules, storage manager command scripts, server definitions, and server group definitions. See also configuration manager, enterprise configuration, managed server.

profile association

On a configuration manager, the defined relationship between a profile and an object such as a policy domain. Profile associations define the configuration information that is distributed to a managed server when it subscribes to the profile.

protected site

See primary site.

Q

quota

1. For HSM on AIX, UNIX, or Linux systems, the limit (in megabytes) on the amount of data that can be migrated and premigrated from a file system to server storage.
2. For HSM on Windows systems, a user-defined limit to the space that is occupied by recalled files.

R

randomization

The process of distributing schedule start times for different clients within a specified percentage of the schedule's startup window.

raw logical volume

A portion of a physical volume that is comprised of unallocated blocks and has no journaled file system (JFS) definition. A logical volume is read/write accessible only through low-level I/O functions.

rebind

To associate all backed-up versions of a file with a new management class name. For example, a file that has an active backup version is rebound when a later version of the file is backed up with a different management class association. See also bind, management class.

recall To copy a migrated file from server storage back to its originating file system using the hierarchical storage management client. See also selective recall.

receiver

A server repository that contains a log of server and client messages as events. For example, a receiver can be a file exit, a user exit, or the server console and activity log. See also event.

reclamation

The process of consolidating the remaining data from many sequential-access volumes onto fewer, new sequential-access volumes.

reclamation threshold

The percentage of space that a sequential-access media volume must

have before the server can reclaim the volume. Space becomes reclaimable when files are expired or are deleted.

reconciliation

The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recovery log

A log of updates that are about to be written to the database. The log can be used to recover from system and media failures. The recovery log consists of the active log (including the log mirror) and archive logs.

recovery site

See secondary site.

register

To define a client node or administrator ID that can access the server.

registry

A repository that contains access and configuration information for users, systems, and software.

remote

For hierarchical storage management products, pertaining to the origin of migrated files that are being moved. See also local.

resident file

On a Windows system, a complete file on a local file system that might also be a migrated file because a migrated copy can exist in server storage. On a UNIX or Linux system, a complete file on a local file system that has not been migrated or premigrated, or that has been recalled from server storage and modified.

restore

To copy information from its backup location to the active storage location for use. For example, to copy information from server storage to a client workstation.

retention

The amount of time, in days, that inactive

backed-up or archived files are kept in the storage pool before they are deleted. Copy group attributes and default retention grace periods for the domain define retention.

retrieve

To copy archived information from the storage pool to the workstation for use. The retrieve operation does not affect the archive version in the storage pool. See also archive.

root user

A system user who operates without restrictions. A root user has the special rights and privileges needed to perform administrative tasks.

S

SAN See storage area network.

schedule

A database record that describes client operations or administrative commands to be processed. See also administrative command schedule, client schedule.

scheduling mode

The type of scheduling operation for the server and client node that supports two scheduling modes: client-polling and server-prompted.

scratch volume

A labeled volume that is either blank or contains no valid data, that is not defined, and that is available for use. See also volume.

script A series of commands, combined in a file, that carry out a particular function when the file is run. Scripts are interpreted as they are run. See also Tivoli Storage Manager command script.

secondary site

A physical or virtual site that is made up of the hardware, network, and storage resources that support the recovery needs of the primary site. When a failure occurs at the primary site, operations can continue at the secondary site. See also primary site.

Secure Sockets Layer (SSL)

A security protocol that provides communication privacy. With SSL, client/server applications can

communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

selective backup

The process of backing up certain files or directories from a client domain. The files that are backed up are those that are not excluded in the include-exclude list. The files must meet the requirement for serialization in the backup copy group of the management class that is assigned to each file. See also incremental backup.

selective migration

The process of copying user-selected files from a local file system to server storage and replacing the files with stub files on the local file system. See also demand migration, threshold migration.

selective recall

The process of copying user-selected files from server storage to a local file system. See also recall, transparent recall.

serialization

The process of handling files that are modified during backup or archive processing. See also shared dynamic serialization, shared static serialization, static serialization.

server A software program or a computer that provides services to other software programs or other computers. See also client.

server options file

A file that contains settings that control various server operations. These settings affect such things as communications, devices, and performance.

server-prompted scheduling mode

A client/server communication technique where the server contacts the client node when tasks must be done. See also client-polling scheduling mode.

server storage

The primary, copy, and active-data storage pools that are used by the server to store user files such as backup versions, archive copies, and files migrated from hierarchical storage management client nodes (space-managed files). See also active-data pool, copy storage pool, primary storage pool, storage pool volume, volume.

session

A logical or virtual connection between two stations, software programs, or devices on a network that allows the two elements to communicate and exchange data for the duration of the session. See also administrative session.

session resource usage

The amount of wait time, processor time, and space that is used or retrieved during a client session.

shadow copy

A snapshot of a volume. The snapshot can be taken while applications on the system continue to write data to the volumes.

shadow volume

The data stored from a snapshot of a volume. The snapshot can be taken while applications on the system continue to write data to the volumes.

shared dynamic serialization

A value for serialization that specifies that a file must not be backed up or archived if it is being modified during the operation. The backup-archive client retries the backup or archive operation a number of times; if the file is being modified during each attempt, the backup-archive client will back up or archive the file on its last try. See also dynamic serialization, serialization, shared static serialization, static serialization.

shared library

A library device that is used by multiple storage manager servers. See also library.

shared static serialization

A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. The client attempts to retry the operation a number of times. If the file is in use during each attempt, the file is not backed up or archived. See also dynamic serialization, serialization, shared dynamic serialization, static serialization.

snapshot

An image backup type that consists of a point-in-time view of a volume.

space-managed file

A file that is migrated from a client node by the hierarchical storage management

(HSM) client. The HSM client recalls the file to the client node on demand.

space management

See hierarchical storage management.

space monitor daemon

A daemon that checks space usage on all file systems for which space management is active, and automatically starts threshold migration when space usage on a file system equals or exceeds its high threshold.

sparse file

A file that is created with a length greater than the data it contains, leaving empty spaces for the future addition of data.

special file

On AIX, UNIX, or Linux systems, a file that defines devices for the system, or temporary files that are created by processes. There are three basic types of special files: first-in, first-out (FIFO); block; and character.

SSL See Secure Sockets Layer.

stabilized file space

A file space that exists on the server but not on the client.

stanza A group of lines in a file that together have a common function or define a part of the system. Stanzas are usually separated by blank lines or colons, and each stanza has a name.

startup window

A time period during which a schedule must be initiated.

static serialization

A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. If the file is in use during the first attempt, the backup-archive client cannot back up or archive the file. See also dynamic serialization, serialization, shared dynamic serialization, shared static serialization.

storage agent

A program that enables the backup and restoration of client data directly to and from storage attached to a storage area network (SAN).

storage area network (SAN)

A dedicated storage network tailored to a

specific environment, combining servers, systems, storage products, networking products, software, and services.

storage hierarchy

A logical order of primary storage pools, as defined by an administrator. The order is typically based on the speed and capacity of the devices that the storage pools use. The storage hierarchy is defined by identifying the next storage pool in a storage pool definition. See also storage pool.

storage pool

A named set of storage volumes that is the destination that is used to store client data. See also active-data pool, copy storage pool, primary storage pool, storage hierarchy.

storage pool volume

A volume that has been assigned to a storage pool. See also active-data pool, copy storage pool, primary storage pool, server storage, volume.

storage privilege class

A privilege class that gives an administrator the authority to control how storage resources for the server are allocated and used, such as monitoring the database, the recovery log, and server storage. See also privilege class.

stub

A shortcut on the Windows file system that is generated by the hierarchical storage management (HSM) client for a migrated file that allows transparent user access. A stub is the sparse file representation of a migrated file, with a reparse point attached.

stub file

A file that replaces the original file on a local file system when the file is migrated to storage. A stub file contains the information that is necessary to recall a migrated file from server storage. It also contains additional information that can be used to eliminate the need to recall a migrated file. See also migrated file, resident file.

stub file size

The size of a file that replaces the original file on a local file system when the file is migrated to server storage. The size that is specified for stub files determines how

much leader data can be stored in the stub file. The default for stub file size is the block size defined for a file system minus 1 byte.

subscription

In a storage environment, the process of identifying the subscribers to which the profiles are distributed. See also enterprise configuration, managed server.

system privilege class

A privilege class that gives an administrator the authority to issue all server commands. See also privilege class.

T

tape library

A set of equipment and facilities that support an installation's tape environment. The tape library can include tape storage racks, mechanisms for automatic tape mounting, a set of tape drives, and a set of related tape volumes mounted on those drives.

tape volume prefix

The high-level-qualifier of the file name or the data set name in the standard tape label.

target node

A client node for which other client nodes (called agent nodes) have been granted proxy authority. The proxy authority allows the agent nodes to perform operations such as backup and restore on behalf of the target node, which owns the data.

TCA See trusted communications agent.

TCP/IP

See Transmission Control Protocol/Internet Protocol.

threshold migration

The process of moving files from a local file system to server storage based on the high and low thresholds that are defined for the file system. See also automatic migration, demand migration, migration job, selective migration.

throughput

In storage management, the total bytes in the workload, excluding overhead, that are backed up or restored, divided by elapsed time.

timeout

A time interval that is allotted for an event to occur or complete before operation is interrupted.

Tivoli Storage Manager command script

A sequence of Tivoli Storage Manager administrative commands that are stored in the database of the Tivoli Storage Manager server. The script can run from any interface to the server. The script can include substitution for command parameters and conditional logic. See also macro file, script.

tombstone object

A small subset of attributes of a deleted object. The tombstone object is retained for a specified period, and at the end of the specified period, the tombstone object is permanently deleted.

Transmission Control Protocol/Internet Protocol (TCP/IP)

An industry-standard, nonproprietary set of communication protocols that provides reliable end-to-end connections between applications over interconnected networks of different types. See also communication method.

transparent recall

The process that is used to automatically recall a migrated file to a workstation or file server when the file is accessed. See also selective recall.

trusted communications agent (TCA)

A program that handles the sign-on password protocol when clients use password generation.

U

UCS-2 A 2-byte (16-bit) encoding scheme based on ISO/IEC specification 10646-1. UCS-2 defines three levels of implementation: Level 1-No combining of encoded elements allowed; Level 2-Combining of encoded elements is allowed only for Thai, Indic, Hebrew, and Arabic; Level 3-Any combination of encoded elements are allowed.

UNC See Universal Naming Convention.

Unicode

A character encoding standard that supports the interchange, processing, and

display of text that is written in the common languages around the world, plus many classical and historical texts.

Unicode-enabled file space

A file space with a name that follows the Unicode standard and is compatible with any locale on multilingual workstations.

Universally Unique Identifier (UUID)

The 128-bit numeric identifier that is used to ensure that two components do not have the same identifier. See also Globally Unique Identifier.

Universal Naming Convention (UNC)

The server name and network name combined. These names together identify the resource on the domain.

UTF-8 Unicode Transformation Format, 8-bit encoding form, which is designed for ease of use with existing ASCII-based systems. The CCSID value for data in UTF-8 format is 1208. See also UCS-2.

UUID See Universally Unique Identifier.

V
validate

To check a policy set for conditions that can cause problems if that policy set becomes the active policy set. For example, the validation process checks whether the policy set contains a default management class.

version

A backup copy of a file stored in server storage. The most recent backup copy of a file is the active version. Earlier copies of the same file are inactive versions. The number of versions retained by the server is determined by the copy group attributes in the management class.

virtual file space

A representation of a directory on a network-attached storage (NAS) file system as a path to that directory.

virtual mount point

A directory branch of a file system that is defined as a virtual file system. The virtual file system is backed up to its own file space on the server. The server processes the virtual mount point as a separate file system, but the client operating system does not.

virtual volume

An archive file on a target server that represents a sequential media volume to a source server.

volume

A discrete unit of storage on disk, tape or other data recording medium that supports some form of identifier and parameter list, such as a volume label or input/output control. See also scratch volume, server storage, storage pool, storage pool volume.

volume history file

A file that contains information about volumes that have been used by the server for database backups and for export of administrator, node, policy, or server data. The file also has information about sequential-access storage pool volumes that have been added, reused, or deleted. The information is a copy of volume information that is recorded in the server database.

Volume Shadow Copy Service (VSS)

A set of Microsoft application-programming interfaces (APIs) that are used to create shadow copy backups of volumes, exact copies of files, including all open files, and so on.

VSS See Volume Shadow Copy Service.

VSS Backup

A backup operation that uses Microsoft Volume Shadow Copy Service (VSS) technology. The backup operation produces an online snapshot (point-in-time consistent copy) of Microsoft Exchange data. This copy can be stored on local shadow volumes or on Tivoli Storage Manager server storage.

VSS Fast Restore

An operation that restores data from a local snapshot. The snapshot is the VSS backup that resides on a local shadow volume. The restore operation retrieves the data by using a file-level copy method.

VSS Instant Restore

An operation that restores data from a local snapshot. The snapshot is the VSS backup that resides on a local shadow volume. The restore operation retrieves

the data by using a hardware assisted restore method (for example, a FlashCopy operation).

VSS offloaded backup

A backup operation that uses a Microsoft Volume Shadow Copy Service (VSS) hardware provider (installed on an alternate system) to move IBM Data Protection for Microsoft Exchange data to the Tivoli Storage Manager server. This type of backup operation shifts the backup load from the production system to another system.

VSS Restore

A function that uses a Microsoft Volume Shadow Copy Service (VSS) software provider to restore VSS Backups (IBM Data Protection for Microsoft Exchange database files and log files) that reside on Tivoli Storage Manager server storage to their original location.

W**wildcard character**

A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace the wildcard character.

workload partition (WPAR)

A partition within a single operating system instance.

workstation

A terminal or personal computer at which a user can run applications and that is usually connected to a mainframe or a network.

worldwide name (WWN)

A 64-bit, unsigned name identifier that is unique.

WPAR See workload partition.

WWN See worldwide name.

Index

Special characters

ACS_DIR 140
ACS_REPOSITORY 142
ACSD 140
ADMIN_ASSISTANT 142
APPLICATION_TYPE 143, 149, 154, 158
ASM_INSTANCE_ID 164, 187
ASM_INSTANCE_USER 164, 187
ASM_ROLE 164, 187
ASNODENAME 187
BACKUP_DESTINATION 164
BACKUP_HOST_NAME 171, 181, 184, 186
BACKUP_METHOD 187, 198
BACKUPIDPREFIX 143, 149, 154, 158
BUFFER_SIZE 187
CATALOG_DATABASE_USERNAME 164
CATALOG_DATABASE_CONNECT_STRING 164
CLONE_DATABASE 171, 176
COPYSERVICES_CERTIFICATEFILE 171, 176
COPYSERVICES_COMMPROTOCOL 171, 176
COPYSERVICES_HARDWARE_TYPE 171, 176, 186
 CLONE_DATABASE 181, 184
COPYSERVICES_PRIMARY_SERVERNAME 171, 176
COPYSERVICES_SECONDARY_SERVERNAME 171, 176
COPYSERVICES_SERVERNAME 171, 181, 184
COPYSERVICES_SERVERPORT 171, 176
COPYSERVICES_TIMEOUT 171, 176
COPYSERVICES_USERNAME 171, 176, 181, 184
DATABASE_BACKUP_INCREMENTAL_LEVEL 187
DATABASE_BACKUP_MSGLOG_FILE 164
DATABASE_BACKUP_SCRIPT_FILE 164
DATABASE_CONTROL_FILE_RESTORE 164
DATABASE_MEMORY 187
DATABASE_SCHEMA 165
DB2_ALIAS 194
DB2_AUTH_TYPE 194
DB2_PRODUCTION_SERVER 194
DB2_USERNAME 194
DBPARTITIONNUM 187
DEVICE_CLASS 143, 149, 154, 158, 165, 194
DMS_OPT 187
DSM_DIR 187
DSM_LOG 187
FLASH_DIR_LIST 165
FLASHCOPY_TYPE 171, 176
GENERIC 158
GLOBAL_SYSTEM_IDENTIFIER 165
GLOBAL_SYSTEM_IDENTIFIER 143, 149, 154
INFILE 143, 158
LVM_FREEZE_THAW 143, 149, 154, 158, 165
 TARGET_DATABASE_SUSPEND 199
MAX_VERSIONS 143, 149, 154, 158, 194
MODE 187
NEGATIVE_LIST 143, 149, 158, 165
NUM_BUFFERS 187
NUM_SESSIONS 187
NUMBER_BACKUPS_IN_PARALLEL 187
NUMBER_GPFS_CONCURRENT_TASKS 186
OPTIONS 187
OVERWRITE_DATABASE_PARAMETER_FILE 165
OVERWRITE_DATABASE_PARAMETER_FILE 187

PARALLEL_BACKUP 187
PARALLEL_RESTORE 187
PARALLELISM 187
PARTITION_GROUP 143, 149
PATH_TO_XCLI 171
POST_FLASH_CMD 143, 158, 194
PRE_FLASH_CMD 143, 158, 194
PROFILE 187
RECON_INTERVAL 171, 176, 181, 184
REPOSITORY_LABEL 142
RESTORE_FORCE 171, 176
STORAGE_SYSTEM_ID 171, 176, 181, 184
SVC_CLEAN_RATE 171, 176
SVC_COPY_RATE 171, 176
SVC_GRAIN_SIZE 176
TARGET_DATABASE_HOME 164
TARGET_DATABASE_PARAMETER_FILE 165
TARGET_DATABASE_SID 164
TARGET_DATABASE_USERNAME 164
TARGET_DATABASE_PARAMETER_FILE 164
TARGET_DATABASE_PASSWORD_FILE 164
TARGET_DATABASE_SUSPEND 143, 149
TARGET_NAMING 171, 176
TARGET_SETS 171, 176
TIMEOUT_<PHASE> 143, 149, 154, 158
TIMEOUT_CLOSE 165
TIMEOUT_COMPLETERESTORE 165
TIMEOUT_FLASH 143, 149, 154, 158, 165
TIMEOUT_FLASHRESTORE 165
TIMEOUT_PARTITION 165
TIMEOUT_PHASE 143
TIMEOUT_PREPARE 165
TIMEOUT_VERIFY 165
TRACE 140
TSM_BACKUP 143, 149, 154, 158, 194
USE_WRITABLE_SNAPSHOTS 171
VENDOR_BIN 187
VENDOR_LIB 187
VENDOR_PATH 187
VENDOR_PROFILE 187
VIRTUALFSNAME 187
VOLUME_MGR 143, 149
VOLUMES_DIR 171
VOLUMES_FILE 171, 176

A

accessibility features 293
acsd 252
ACSD 142
acsgen 254
acsora 273
acsutil 277
administrative commands 241
APAR 119
application agents
 acsora 5
 backint 5
 fcmcli 5
ASM
 DS8000 environment 16

ASM (*continued*)

- failure groups 94
- DEVICE_CLASS** 72
- planning 15
- ASM cloning 16
- ASM failure group 16
- Asynchronous Remote Mirroring 33
- audience xii

B

- background daemons
 - description 252
- backing up DB2 82
- backint
 - description 275
- BACKINT
 - parameters 207
- backup
 - starting 93
 - to Tivoli Storage Manager 259
 - to Tivoli Storage Manager server 83
- backup cluster 25
- backup commands 81, 265
- backup environment
 - backup servers
 - assignment 72
 - determining 22
 - prerequisites 23
 - clone servers
 - assignment 72
 - determining 22
 - prerequisites 23
- installation
 - non-remote 42
 - remote 40
- preparing
 - backup servers 21
 - clone servers 21
- backup procedure
 - custom application 93
 - DB2 81, 84
 - serial mode 82
 - to Tivoli Storage Manager server 83
 - DB2 database
 - parallel mode 82
 - DB2 HADR server 84
 - DB2 pureScale 84
 - DB2 standby server 84
 - file system 93
 - fully automated backup 87
 - GPFS 84
 - Oracle 86, 87
 - to Tivoli Storage Manager server 86
 - Oracle in an SAP environment
 - automated backup 93
 - SAP with Oracle 87
- backup server
 - virtual machine 26
- block device mapping 21
- BR*TOOLS
 - description 275

C

- CA certificate 248
- capacity planning 8
- changing passwords 247
- CIM
 - acsgen 254
 - generic device agent 254
 - log files 126
 - trace files 126
- CLIENT 143, 149, 154, 158
- clone devices
 - DS8000 29
 - SAN Volume Controller 29
 - Storwize family 29
- clone server
 - virtual machine 26
- cloning
 - commands 284
 - configuration files 115
 - target volumes file (.fct)
 - parameter settings 205
- CLONING 165
- cluster
 - backup cluster 25
- command line interface
 - f delete** 266
 - f inquire_detail** 266
 - f inquire** 266
 - f restore** 266
 - backup** 282
 - create_clone** 287
 - delete_clone** function 288
 - delete** 283
 - inquire_clone** 288
 - inquire_db2standby** 273
 - inquire_detail_clone** 288
 - inquire_detail_db2standby** 273
 - inquire_detail** 283
 - inquire** 283
 - mount** 258
 - postproc_clone** function 289
 - preproc_clone** 288
 - refresh_clone** 289
 - restore_db2standby** 273
 - unmount** 258
 - restore function for custom applications 284
- commands
 - preproc_clone** 288
 - administrative 241
 - backup 265
 - cloning 284
 - custom applications 279
 - delete 265
 - inquire 265
 - restore 265
- communication ports 9
- configuration 53, 55, 58, 62
- Configuration 53
- configuration files
 - configuration file 135
 - password file 207
- configuring 56, 59, 63
 - remote mirroring 76
- console mode
 - installation 43

- control files
 - cloning files
 - description 115
 - profile
 - structure 135
 - updating 198
- SAP BR*Tools configuration profile (.sap)
 - description 218
- target volumes file (.fct)
 - cloning parameter settings 205
 - description 199
 - DS8000 parameter settings 203
 - SAN Volume Controller parameter settings 204
 - Storwize family parameter settings 204
- custom application
 - examples
 - profile 238
- custom applications 62
- custom applications configuration 63

D

- database cloning
 - commands 113
 - description 4
 - Oracle Data Guard 114
 - postprocessing 115
 - preprocessing 115
 - process 113
- DB2 53
 - backup history file 105
 - commands 265
 - environment 10
 - examples
 - disk layout 223
 - profile 224, 226
 - LIST HISTORY command 105
 - SAP environment 13
 - vendor options 265
- DB2 configuration 56
- DB2 HADR standby server
 - examples
 - profile 239
- DB2 pureScale
 - configuration 243
 - High Availability 2
 - protection 2
- DB2STANDBY 194
- defining LUNs
 - DS8000 66
- defining target sets
 - DB2
 - multi-partition 70
 - single partition 70
 - naming convention 71
 - Oracle 70
 - profile 71
- defining virtual disks
 - SAN Volume Controller 67
 - Storwize family 67
- delete commands 265
- deleting
 - snapshot backup 289
- developerWorks wiki 119
- device agents
 - acsd 5
 - acsgen 5

- device agents (*continued*)
 - CIM adapter 5
 - command-line interface 5
 - offload agent 5
 - query capacity 5
 - volume group takeover script 5
- DEVICE_CLASS
 - device* 72, 171
 - parameters 72
- devices
 - DS8000 29
 - IBM System Storage N series
 - NetApp 28
 - preparing 28
 - IBM XIV Storage System
 - preparing 26
 - SAN Volume Controller 29, 32
 - storage
 - log files 126
 - setting up 65
 - trace files 126
 - Storwize family 29, 32
- disability 293
- disk layout
 - examples
 - DB2 223
 - Oracle environment 227
 - Oracle in an SAP environment 230
 - sample 230
- DPF
 - backup modes 82
- DS8000
 - defining LUNs 66
 - examples
 - target volumes file 234
 - target volumes file mirror setup 237
 - planning 29
 - target volumes file (.fct)
 - parameter settings 203

E

- encryption
 - SP 800-131A 65
- environment
 - ASM 16
 - backup servers 21
 - assignment 72
 - determining 22
 - prerequisites 23
 - clone servers 21
 - assignment 72
 - determining 22
 - prerequisites 23
 - DB2 10
 - Oracle 14
 - Oracle in an SAP environment 13
 - SAP on DB2 13
- examples
 - custom application
 - profile 238
 - DB2
 - disk layout 223
 - profile 224
 - DB2 HADR standby server
 - profile 239

examples (*continued*)

- DB2 pureScale
 - profile 226
- Oracle ASM environment
 - profile 229
- Oracle environment
 - disk layout 227
 - profile 228
- Oracle in an SAP environment
 - disk layout 230
 - profile for disk only 231
- RMAN backup script 230
- SAP with Oracle environment
 - profile for offload 232, 234
- target volumes file
 - DS8000 234
 - DS8000 mirror setup 237
 - SAN Volume Controller 235
 - Storwize family 235

F

- fcmcli 259
 - restore function for custom applications 284
- FlashCopy 2
- FlashCopy backup
 - reconciliation 36
- fmquery
 - description 251
- fully automated backup 87

G

- generic device agent 254
- GLOBAL 140
- Global Mirror 33
- glossary 299
- GSKit
 - configuring 216
 - FIPS 216
 - installing 216
- guest operating system 20

I

- IBM Knowledge Center xii
- individual mirrors 94
- inquire commands 265
- installation
 - backup server
 - non-remote 42
 - remote 40
 - console mode 43
 - description 39
 - prerequisites 10, 79
 - production server 40
 - silent mode 43
- installation planning 53
- installation setup script
 - DB2 pureScale 243
- Internet Protocol Version 6 133
- introduction 1

K

- keyboard 293
- Knowledge Center xii
- KVM 21

L

- log files
 - CIM 126
 - GPFS 127
 - storage subsystems 126
 - summary 120
 - Tivoli Storage FlashCopy Manager 122
 - Tivoli Storage Manager for ERP 127

M

- management agent 252
- Metro Mirror 33
- migrating 48
- mirroring
 - examples
 - DS8000 target volumes file 237
 - individual 94
 - LVM 19, 94
 - DEVICE_CLASS** 72
 - Oracle ASM 72
 - overview 19
- multi-partition
 - target set definitions 70
- multipath
 - KVM check 21

N

- naming convention 71
- new xiii

O

- OFFLOAD 187
- offload agent
 - tape_backup** 262
 - update_status** 263
 - description 259
- OFFLOAD_DB2STANDBY 198
- option files
 - Tivoli Storage Manager
 - and Data Protection for Oracle 220
- Oracle 58
 - ASM environment 16
 - profile example 229
 - commands 273
 - environment 14
 - disk layout example 227
 - profile example 228
 - SAP environment
 - disk layout example 230
 - profile example for disk only 231
 - profile example for offload 232, 234
 - troubleshooting 130
 - miscellaneous errors 132
 - variables
 - troubleshooting 132
- ORACLE 164

- Oracle ASM
 - failure groups 94
 - DEVICE_CLASS** 72
 - preparing 15
- Oracle configuration 59
- overview 1

P

- parameters
 - ACS_DIR** 207
 - ACSD** 207
 - ALLOW_FULL_FILE_BACKUP** 207
 - BACKUPIDPREFIX** 207
 - DEVICE_CLASS** 74, 207
 - GLOBAL_SYSTEM_IDENTIFIER** 207
 - INCREMENTAL_CATALOG_CONNECT_STRING** 207
 - INCREMENTAL_CATALOG_USER** 207
 - INCREMENTAL_CHANNELS** 207
 - INCREMENTAL_LEVEL** 207
 - INCREMENTAL** 207
 - LVM_FREEZE_THAW** 207
 - MAX_SNAPSHOT_VERSIONS** 207
 - TARGET_DATABASE_SUSPEND** 207
 - TIMEOUT_<PHASE>** 207
 - TIMEOUT_FLASH** 207
 - TRACE, TRACEFILE** 207
 - TSM_BACKUP_FROM_SNAPSHOT** 207
- password administration 247
- password file 207
- planning 7
 - capacity 8
 - checklist 7
- preinstallation checklist 53
- preinstallation planning 7
- prerequisite checker 7
- prerequisites
 - backup servers 23
 - clone servers 23
 - hardware 10, 79
 - software 10, 79
- problem determination
 - general procedure 119
 - Oracle environment 130
 - miscellaneous errors 132
 - Oracle variables 132
- product support 119
- production cluster 25
- production environment
 - installing 40
- profile
 - example for disk only
 - Oracle in an SAP environment 231
 - example for offload
 - SAP with Oracle environment 232, 234
- examples
 - custom application 238
 - DB2 224, 226
 - DB2 HADR standby server 239
 - Oracle ASM environment 229
 - Oracle environment 228
- structure 135
- target set definitions 71
 - naming convention 71
- updating 198
- publications xii
- pureScale 55, 82

Q

- query managed capacity (fmquery)
 - description 251

R

- reconciliation
 - FlashCopy backup 36
- repository
 - snapshot backup
 - status 291
- restore
 - Oracle in an SAP environment 108
- restore commands 265
- restore function for custom applications
 - fcmlcli 284
- restore procedure
 - custom application 108
 - DB2 103
 - DB2 HADR server 103
 - DB2 pureScale 103
 - DB2 standby server 103
 - file system 108
 - GPFS 103
 - native Oracle 105
 - snapshot restore
 - procedure 105
- restoring
 - Oracle databases 106, 107
- RMAN backup script
 - example 230

S

- SAN Volume Controller
 - examples
 - target volumes file 235
 - planning 29
 - target volumes file (.fct)
 - parameter settings 204
- SAP BR*Tools configuration profile (.sap)
 - description 218
- Service Management Console 119
- setup script 53, 55, 58, 62
 - description 241
- silent mode installation 43
- snapshot 2
 - mounting 256
 - unmounting 256
- snapshot backup 97
 - deleting 289
 - modes with DPF partitions 82
- repository
 - status 291
- snapshot devices
 - DS8000 29
 - SAN Volume Controller 29
 - Storwize family 29
- Snapshot Object Manager, acsutil 277
- snapshot restore
 - procedure 105
- status
 - repository 291
- storage solutions
 - preparing 26

- storage subsystems
 - DS8000
 - defining LUNs 66
 - log files 126
 - preparing
 - IBM XIV Storage System 26
 - NetAppIBM System Storage N series 28
 - SAN Volume Controller 32
 - Storwize family 32
 - SAN Volume Controller
 - defining virtual disks 67
 - setting up 65
 - Storwize family
 - defining virtual disks 67
 - trace files 126
- Storwize family
 - examples
 - target volumes file 235
 - planning 29
 - target volumes file (.fct)
 - parameter settings 204
- Synchronous Remote Mirroring 33

T

- target set definitions
 - DB2
 - multi-partition 70
 - single partition 70
 - files 69
 - naming convention 69, 71
 - Oracle 70
 - profile 71
- target volumes file
 - examples
 - DS8000 234
 - DS8000 mirror setup 237
 - SAN Volume Controller 235
 - Storwize family 235
- target volumes file (.fct)
 - description 199
 - parameter settings
 - cloning 205
 - DS8000 203
 - SAN Volume Controller 204
 - Storwize family 204
- Tivoli Storage FlashCopy Manager
 - snapshot restore
 - procedure 105
 - starting backups automatically 93
- Tivoli Storage FlashCopy Manager Oracle in an SAP environment (backint)
 - description 275
- Tivoli Storage FlashCopy Manager Oracle in an SAP environment BR*TOOLS
 - description 275
- Tivoli Storage Manager
 - backup to Tivoli Storage Manager server 83
 - integration 259
- Tivoli Storage Manager for ERP
 - log files 127
 - trace files 127
- trace files
 - CIM 126
 - storage subsystems 126
 - summary 120
 - Tivoli Storage FlashCopy Manager 122

- trace files (*continued*)
 - Tivoli Storage Manager for ERP 127
- troubleshooting 130
 - general procedure 119
 - Oracle environment 130
 - miscellaneous errors 132
 - Oracle variables 132

U

- upgrade
 - production server 45
- upgrading
 - migrating 48
 - process 39
- usability states 97

V

- V4.1.1 xiii
- virtual machine 20



Product Number: 5608-W07
5641-A06
5724-X94

Printed in USA