

IBM System Storage



IBM System Storage DS8000 IBM Database Protection User's Guide

Version 1 Release 3

IBM System Storage



IBM System Storage DS8000 IBM Database Protection User's Guide

Version 1 Release 3

Note:

Before using this information and the product it supports, read the information in the **Safety and environmental notices** and **Notices** sections.

This edition replaces GC27-2133-01. This edition also applies to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2007, 2011.

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

Contents

About this guide v

Safety and Environmental notices . . . vii

Safety notices vii

Environmental notices viii

Chapter 1. IBM Database Protection. . . 1

Supported environments 3

IBM Database Protection operational limitations . . 4

Activating your machine and feature licenses using the DS CLI 6

Setting up your system to use IBM Database Protection 8

Chapter 2. Managing database protection on sites that have an IP connection 11

Adding data block validation to a single tablespace 13

Removing data block validation from a single tablespace 13

Changing the error reporting settings. 14

Adding data block validation to all database files. . 16

Removing data block validation from all database files 17

Extending the size of a tablespace - resize database data file 18

Extending the size of a tablespace - add database data file 19

Disabling data block validation for volumes . . . 21

Enabling data block validation for volumes. . . . 22

Clearing database extent configuration from volumes 23

Disabling data block validation for volume group 23

Enabling data block validation for volume group. . 24

Clearing database extent configuration from all the volumes managed by a volume group 25

Chapter 3. Database Protection commands 27

setdbcheck. 27

applydbcheck. 31

offloaddbcheck 32

managedbcheck 34

lsdbcheck 36

showfbvol 45

applykey 53

lskey 54

Chapter 4. IBM Database Protection system generated messages 57

Notices 59

Trademarks 60

Electronic emission notices 61

Taiwan contact information 64

Index 65

About this guide

This publication introduces the IBM Database Protection feature and provides instructions for setting up your system and common tasks for using the feature.

This publication provides descriptions of the following components:

- An overview of the IBM Database Protection feature and how it works in combination with the Oracle Hardware Assisted Resilient Data (HARD) initiative. This overview also provides instructions for preparing your system for the use of the IBM Database Protection feature. You can check with the guides that are associated with your system to ensure that the settings you need for Oracle databases, operating systems, and LVM are correct.
- Common tasks that allow you to take full advantage of the feature.
- Each DS CLI command that you use to make the feature work.

This publication is written for the storage system administrator who has extensive knowledge and experience in database administration and database server administration. It is also written for a user who understands the concepts of a command-line interface application, the knowledge to write scripts using the DS CLI commands, and also has a knowledge of the operating systems and the storage systems in the enterprise.

Safety and Environmental notices

This section contains information about safety notices that are used in this guide and environmental notices for this product.

Safety notices

Observe the safety notices when using this product. These safety notices contain danger and caution notices. These notices are sometimes accompanied by symbols that represent the severity of the safety condition.

Most danger or caution notices contain a reference number (Dxxx or Cxxx). Use the reference number to check the translation in the *IBM System Storage DS8000 Safety Notices*, P/N 98Y1543.

The sections that follow define each type of safety notice and give examples.

Danger notice




A danger notice calls attention to a situation that is potentially lethal or extremely hazardous to people. A lightning bolt symbol always accompanies a danger notice to represent a dangerous electrical condition. A sample danger notice follows:




DANGER: An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (D004)

Caution notice

A caution notice calls attention to a situation that is potentially hazardous to people because of some existing condition, or to a potentially dangerous situation that might develop because of some unsafe practice. A caution notice can be accompanied by one of several symbols:

If the symbol is...	It means...
	A generally hazardous condition not represented by other safety symbols.
	This product contains a Class II laser. Do not stare into the beam. (C029) Laser symbols are always accompanied by the classification of the laser as defined by the U. S. Department of Health and Human Services (for example, Class I, Class II, and so forth).
	A hazardous condition due to mechanical movement in or around the product.

If the symbol is...	It means...
	<p>This part or unit is heavy but has a weight smaller than 18 kg (39.7 lb). Use care when lifting, removing, or installing this part or unit. (C008)</p>

Sample caution notices follow:

Caution

The battery is a lithium ion battery. To avoid possible explosion, do not burn. Exchange only with the IBM-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM® has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM part number for the battery unit available when you call. (C007)

Caution

The system contains circuit cards, assemblies, or both that contain lead solder. To avoid the release of lead (Pb) into the environment, do not burn. Discard the circuit card as instructed by local regulations. (C014)

Caution

When removing the Modular Refrigeration Unit (MRU), immediately remove any oil residue from the MRU support shelf, floor, and any other area to prevent injuries because of slips or falls. Do not use refrigerant lines or connectors to lift, move, or remove the MRU. Use handholds as instructed by service procedures. (C016)

Caution

Do not connect an IBM control unit directly to a public optical network. The customer must use an additional connectivity device between an IBM control unit optical adapter (that is, fibre, ESCON®, FICON®) and an external public network . Use a device such as a patch panel, a router, or a switch. You do not need an additional connectivity device for optical fibre connectivity that does not pass through a public network.

Environmental notices

The environmental notices that apply to this product are provided in the *Environmental Notices and User Guide*, Z125-5823-xx manual. A copy of this manual is located on the publications CD.

Chapter 1. IBM Database Protection

The IBM Database Protection feature provides the highest level of protection for Oracle databases by detecting corrupted Oracle data and preventing it from being processed to storage. This section provides the necessary information to understand the purpose of the IBM Database Protection feature and how it works with the supported environments.

The IBM Database Protection feature complies with the Oracle Hardware Assisted Resilient Data (HARD) initiative, which provides an end-to-end data protection between an Oracle database and permanent storage devices. Figure 1 illustrates the many software and hardware layers that are involved from when an Oracle process on a server asks to write Oracle data blocks to a storage device.

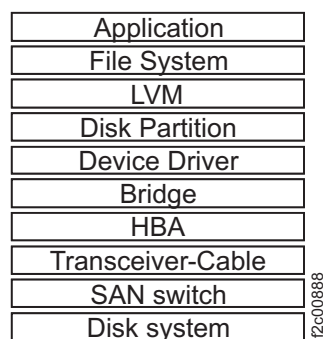


Figure 1. Many layers from the application to the disk

Data must pass through many software and hardware layers on its way to storage. It is possible for the data to become corrupted, in a rare occasion, caused by a malfunction in an intermediate layer. With the IBM Database Protection feature, an IBM DS8000 model can validate whether Oracle data blocks are consistent using the same logic that Oracle uses. This validation is done before the write request is processed. You can designate how the transaction is managed: either rejected and reported or processed and reported.

The IBM Database Protection feature works within the combination of Oracle and DS8000 storage control, with the DS CLI commands as the only interface between the two. The IBM Database Protection feature provides the following functions:

- Identifies and analyzes Oracle data locations and translates this information into spheres of logical block addresses (LBAs) on DS8000 volumes where Oracle data resides.
- Informs the DS8000 model that you want it to remember the location of the database in order to manage the data appropriately.
- Informs the DS8000 model that you want it to forget the location of the database.

The DS8000 processes the information that it receives from the DS CLI commands in the following manner:

- When a write request to a certain LBA comes from a host, the DS8000 checks to see if the data being committed to a DS volume belongs to the spheres where

Oracle data resides. If the data does belong, the DS8000 verifies that the contents of the data are valid as Oracle data blocks.

- If the result of the validation is negative, the DS8000 logs the event inside of the DS8000 and manages the transaction in the manner in which you have designated. Either the data is rejected or accepted for being written to disk.

The topics in this section provide the information that you must have to configure and maintain your IBM Database Protection feature so that the following levels of data protection are maintained:

- Detection and prevention of potential data corruption before it happens
- Prevention of the accidental overwriting of business-critical Oracle data
- Detection of any data corruption that occurs during backups or data lifecycle management

Terms

The following terms describe the IBM Database Protection feature and how it interacts with Oracle databases to provide data protection.

Checksum

A form of redundancy check, for protecting the integrity of data by detecting errors in data that are sent through time (storage). It works by adding the basic components of a message, typically the asserted bits, and storing the resulting value.

control files

Files of a database that store the status of the physical structure of the database. The control file is crucial to database operation.

DS volume

An open systems fixed block (FB) volume of data type 512 that is configured in the IBM DS8000.

data block validation

Validation check that is performed by the IBM Database Protection feature to compare the results to the original value, and (assuming that the values match) conclude that the data is probably not corrupted.

database extent

A contiguous region on a DS volume where Oracle data blocks are stored.

database extent definition

Defines the location of a database extent and parameters that include how write I/Os to the database extent are validated. The definition is stored in the DS8000 per volume.

database extent file

Database extent definitions offloaded from the DS8000 to a file in XML format. You can use this file to manipulate database extent definitions from multiple storage images or to manipulate offloaded database extent definitions in an offline environment; an environment disconnected from a network where a DS8000 hardware management console is attached.

LVM logical volume

A volume that is managed by the logical volume manager (LVM) of the host operating system

Oracle instance

Every running Oracle database is associated with an Oracle instance. When

a database is started on a database server (regardless of the type of computer), Oracle allocates a memory area called the System Global Area (SGA) and starts one or more Oracle processes. This combination of the SGA and the Oracle processes is called an Oracle instance.

redo log

A redo log file that is a record of all changes to the Oracle data files within each Oracle database.

tablespace

The lowest logical layer of the Oracle data structure. The tablespace consists of one or more datafiles. You can think of a tablespace as a file system on a set of disk drives.

Supported environments

To effectively use the IBM Database Protection feature, your system must meet the following supported environments.

The IBM Database Protection feature supports Oracle9i Database Release 2 (9iR2) and Oracle 10g Database Release 2 (10gR2), and can validate the data blocks of tablespaces, control files, and redo log files.

Supported Environments – Oracle 9iR2

The following table shows the combinations of logical volumes, raw disks, and multipathing software that the IBM Database Protection function supports with Oracle 9iR2, *where*

VxVM

Specifies VERITAS Volume Manager

DMP Specifies VERITAS dynamic multipathing

	HP-UX 11i (11.11)	HP-UX 11i v2 (11.23)	Sun Solaris 8	Sun Solaris 10
raw disks	Yes	Yes	Yes	Yes
raw logical volumes	HP LVM	HP LVM	VxVM	VxVM
raw logical volumes with multi-pathing	HP LVM + PV Links	HP LVM + PV Links	VxVM + DMP	VxVM + MPxIO
filesystem	No	No	No	No

Notes:

1. The restore daemon of the VERITAS VxVM DMP periodically checks the condition of paths. If each path is exposed to a connection loss within the periodic check time frame, the disk group is put into a disabled state. This can happen even if IBM Database Protection is not enabled because there is an Oracle application error. When you attempt to resolve this problem, check DMP setting and make the appropriate correction. If this does not work, consult the applicable VERITAS manual.
2. If VxVM version supports dmp_fast_recovery option, then you must set dmp_fast_recovery to Off.

3. For HP-UX 11iv2 (11.23), PHCO_35063 or later must be applied.
4. Microcode release 5.0 or later supports Oracle 9iR2 on DS8700.
Microcode Release 6.1 or later supports Oracle 9iR2 on DS8800.

Supported Environments – Oracle 10gR2

The following table shows the combinations of logical volumes, raw disks, and multipathing software that the IBM Database Protection function supports with Oracle 10gR2.

	HP-UX 11i v2 (11.23)	HP-UX 11i v3 (11.31)	Sun Solaris 10
raw disks	Yes	Yes	Yes
raw logical volumes	HP LVM	HP LVM	VxVM
raw logical volumes with multi-pathing	HP LVM + PV Links	HP LVM + PV Links	VxVM + MPxIO
filesystem	No	No	No

Note:

1. For HP-UX 11iv2 (11.23), PHCO_35063 or later must be applied.
2. Microcode Release 6.1 or later supports Oracle 10gR2 on DS8800 and DS8700.
3. On HP-UX 11iV3 (11.31), only legacy DSF (legacy style disk names like cXtYdZ) is supported. Persistent DSF (Agile disk name) is not supported.
4. To keep the compatibility with HP-UX 11iV2, PV Links is still required on HP-UX 11iV3.
5. On HP-UX 11iV3 (11.31), HP LVM volume group version 1 is supported. HP LVM volume group version 2 or later is not supported.

IBM Database Protection operational limitations

There are operational limitations that are associated with the use of the IBM Database Protection feature.

The following operational limitations can affect the IBM Database Protection feature:

- A tablespace, a control file, or a redo log cannot span across DS8000 and non-DS8000 storage
 - A tablespace, a control file, or a redo log cannot be part of a filesystem
 - A DS volume can have up to 32 database extent definitions
- A logical volume is made from LVM extents from DS volumes that form a volume (disk) group. An LVM extent is a sphere of contiguous LBAs on a DS volume, which is the minimum unit of allocation control.

Note: The HP LVM calls the unit of allocation control a physical extent and VERITAS Volume Manager (VxVM) calls it a subdisk.

A logical volume could have multiple LVM extents spread across DS volumes.

A database extent is a collection of contiguous extents that contains the entire or a portion of a single Oracle database file that is protected by the IBM Database Protection feature.

In the example shown in Figure 2, Logical Volume 1 (LV1) has two extents that are fragmented on the DS volume (LUN A), Logical Volume 2 (LV2) has two contiguous extents and Logical Volume 3 (LV3) has three contiguous extents. If you create a tablespace (TS1) so that it spans across LV1 and LV2 but not LV3, you have three database extents. The first database extent represents the first extent of LV1, the second database extent represents the first and the second extent of LV2, and the third database extent represents the second extent of LV1.

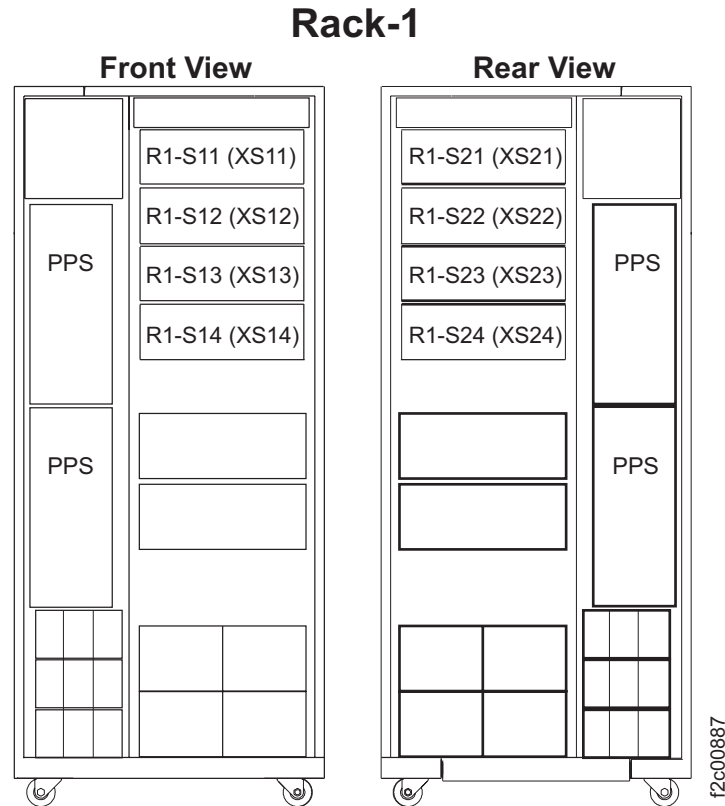


Figure 2. The concept of database extents

The DS CLI analyzes the space allocation on the DS volumes. If a DS volume has more than 32 database extents, none of the DS CLI commands that are associated with the IBM Database Protection feature can process.

- LVM-based mirroring or RAID-5 is not supported.

Note: The HP LVM or VxVM might create a hot-spare DS volume in the event that the access to the DS volume has been lost. The DS CLI is unable to keep track of the dynamic disk relocation; therefore, you might lose protection on those DS volumes.

- HP LVM cannot relocate bad blocks.

DS CLI does not account for a bad block relocation pool that you implicitly or explicitly reserve through the HP LVM **pvcreate** command. Do not allow HP LVM to accept the relocation of bad blocks. Ensure that you use a logical volume that you created with the HP LVM **lvcreate -r n** command.

Note: Because logical volume bad block relocation is not supported on HP-UX 11iv3, you do not need to use the **-r n** option with the **lvcreate** command on HP-UX 11iv3. The **-r n** option is allowed on HP-UX 11iv3 for backward compatibility.

- The size of an LVM extent or a LVM stripe size (when a logical volume is striped) for a logical volume must be an integral multiple of the Oracle block size of the Oracle data that is allocated on the logical volume.
- DS CLI commands that you use to analyze the space allocation must run under a user ID that has a root authority.
- A database extent definition that is set using the DS CLI commands is kept in the DS8000

The database extent definition that is kept in the DS8000 is nonvolatile. Even if you re-initialize the contents of a DS volume by using the operating system's format command, the database extent definition remains in the DS8000. For this reason, you must delete the database extent definitions on a DS volume when the DS volume is about to be taken from Oracle's control. Use the DS CLI **setdbcheck** command with the **-action remove** parameter to delete the database extent definitions.

Note: The database extent definitions are cleaned up when you use the DS CLI **rmfbvol** command to unconfigure the volume.

- The Oracle block size for database files under the database protection feature must be 512-bytes or 1 KB for redo log files (depending on the operating system), and 2 KB, 4 KB, 8 KB, 16 KB, or 32 KB for data files and control files.
- The database files on the system boot disk are not supported for a database server running on an HP-UX operating system.
- In the SUN Solaris 10 environment, each volume size must not exceed 1TB because of the limitation of VTOC disk.
- The IBM Database Protection feature supports standard volumes only. Space efficient volumes such as TSE (track space-efficient volume) or ESE (extent space-efficient volume) are not supported.
- The IBM Database Protection feature does not support any volumes managed by IBM System Storage Easy Tier.

Activating your machine and feature licenses using the DS CLI

Use the steps described in this task to activate your license activation codes. These codes must be activated before any configuration can be applied to your DS8000[®] network.

The following licenses can be activated depending on your purchase:

- Operating environment license for each storage unit that you own. (This license must be activated.)
- Copy Services, which can consist of the following features:
 - FlashCopy[®]
 - Remote mirror and copy
- Parallel access volumes (PAV)
- IBM HyperPAV (DS8000 only)
- IBM Database Protection (DS8000 only)
- IBM FlashCopy SE (DS8000 only)

There are multiple codes that are associated with these features. To obtain the information that you need to activate these licenses and features in your storage unit, go to the IBM Disk Storage Feature Activation (DSFA) website at:

www.ibm.com/storage/dsfa/

Download your codes onto a diskette in XML format. You can then import the codes from the XML file when you process the DS CLI **applykey** command.

Notes:

1. For DS8000, in most situations, the DSFA application can locate your 2244 or 239x license authorization record when you enter the DS8000 (2107) serial number and signature. However, if the 2244 license authorization record is not attached to the 2107 record, you must assign it to the 2107 record in the DSFA application. In this situation, you must have the 2244 or 239x serial number (which you can find on the License Function Authorization document).

The DS CLI **applykey** command activates the licenses for your storage unit. The DS CLI **lskey** command verifies which type of licensed features are activated for your storage unit.

Perform the following steps to activate your license activation codes:

1. Log in to the DS CLI in interactive command mode.
2. Issue the DS CLI **applykey** command at the dscli command prompt as follows. (This example presumes that your XML file is named "keys.xml" and it resides on a diskette in your A: drive):
dscli> applykey -file a:\keys.xml -dev IBM.2107-75FA120
3. Press Enter. When the process has completed, the following message is displayed:
Licensed Machine Code key xxxx, key xxxx successfully applied.
4. Verify that the keys have been activated for your storage unit by issuing the DS CLI **lskey** command as follows: lskey -dev IBM.2107-75FA120
5. Press Enter and the following type of report is displayed:

Activation key	Authorization level (TB)	Scope
Operating environment (OEL)	45	All
Remote mirror and copy (RMC)	25	All
Metro mirror (MM)	25	All
Global mirror (GM)	25	All
Metro/global mirror (MGM)	25	All
Remote mirror for z/OS® (RMZ)	25	CKD
Point in time copy (PTC)	25	All
Parallel access volumes (PAV)	100	CKD
IBM HyperPAV	On	CKD
IBM Database Protection	On	FB

Activation key	Authorization level (TB)	Scope
IBM FlashCopy SE	105	All

Setting up your system to use IBM Database Protection

Complete this task to ensure that you have the full use of the IBM Database Protection feature.

Your system must meet the following prerequisites before you can use the IBM Database Protection feature:

- For IBM DS8000 models, you must create the DS standard volumes that receive the benefit of the IBM Database Protection feature.
- You must activate your license activation code that you received from IBM to use the IBM Database Protection feature. Issue the DS CLI **applykey** command with the correct activation code.
- You must have the appropriate DS8000 licensed microcode bundle installed on your system.
- The Oracle software must be at one of the following levels:
 - Oracle 9i Database Release 2 (Oracle 9iR2)
 - Oracle 10g Database Release 2 (Oracle 10gR2)
- Your database server must run one of the following operating systems:
 - Sun Solaris 8 running on SPARC platform (Oracle 9iR2 only)
 - Sun Solaris 10 running on SPARC platform
 - HP-UX 11i (11.11) (Oracle 9iR2 only)
 - HP-UX 11i v2 (11.23)
 - HP-UX 11iv3 (11.31) (Oracle 10gR2 only)

The Table 1 summarizes the supported combinations of Oracle software level and operating system.

Table 1. Supported combinations of Oracle software level and operating system

	Oracle 9iR2	Oracle 10gR2
Sun Solaris 8 running on SPARC platform	Yes	No
Sun Solaris 10 running on SPARC platform	Yes	Yes
HP-UX 11i (11.11)	Yes	No
HP-UX 11iv2 (11.23)	Yes	Yes
HP-UX 11iv3 (11.31)	No	Yes

- Use IBM Database Protection only with the following database file types:
 - Data file (tablespace)
 - Control file
 - Redo log file

Notes:

1. None of these database file types can be allocated on a filesystem. Filesystems are not supported.
2. Temporary table space is not supported.

- You must install the DS CLI application on your database server.

To effectively use IBM Database Protection, ensure that the database server has an IP connection to the DS8000 hardware management console. If it does not, you must install the DS CLI application on another system that has an IP connection to the hardware management console. Then, to complete the setup for IBM Database Protection, you must work with the DS CLI database protection commands on both systems.

Note: When your database server runs more than one Oracle instance, do not share a volume group (HP LVM) or a disk group (VxVM) among the instances. You can avoid inconsistency when DS CLI commands are processed by not sharing groups.

The following high level steps list the actions that a person with administrator authority must complete before your system can use the IBM Database Protection feature. (Only persons with administrator authority must be assigned this authority in the DS user group designation, and they must also have administrator authority to work with your Oracle databases.)

1. Open a command line console of your operating system by using the administrator's login ID which has a root privilege of your operating system.
2. Ensure that the ORACLE_HOME and ORACLE_SID environment variables are set so that the DS CLI commands that are associated with the IBM Database Protection feature work.

This can be done at the command line console by entering:

- ORACLE_HOME=...; export ORACLE_HOME
- ORACLE_SID=...; export ORACLE_SID

Note: The database instance specified by the ORACLE_SID environment variable must be started before you use the DS CLI commands.

3. Check the value of the following parameters by using the `psql` command "show parameters".

The following information is displayed:

<code>db_block_checking</code>	string	TRUE
<code>db_block_checksum</code>	boolean	TRUE

If the parameters display a status of FALSE, you must set them to TRUE and restart the database instance.

Note: On Oracle 10g Database, each parameter definition was changed. But TRUE can be used to each parameter value for backward compatibility.

4. Log on to the DS CLI application in interactive mode. There are two reasons for starting DS CLI in the interactive mode:
 - To activate the license code for the IBM Database Protection feature.
 - For timing. Before you can use the DS CLI command to manage the databases, you must first start the Oracle database instances, especially the database instance that is accessed by the ORACLE_SID environment variable.
5. Issue the DS CLI **applykey** command to activate the license code for the IBM Database Protection feature. Enter the **applykey** command at the `dscli` command prompt with the following parameters and variables:

```
dscli>applykey -key key storage_image_ID
```

where *key* represents the code that activates the IBM Database Protection feature in your system.

Note: If you have made a new system purchase or have purchased several DS8000 licensed features, you can follow the instructions found in the **Activating your system and feature licenses using the DS CLI** topic.

6. Create the Oracle database files on the DS volumes by using Oracle database commands. To protect your database files with the IBM Database Protection feature, consider the following requirements:
 - You can apply database protection only to the following database file types:
 - Data file (tablespace)
 - Control file
 - Redo log file
 - The data under the database protection must be placed on the raw disks or raw logical volumes. The data on the filesystem cannot be protected.
 - If the location of a data file is under the control of HP LVM, you must change the timeout value of the logical volume to a non-zero value so that Oracle database can detect the error in the underlying layer. Use the HP LVM **lvchange** command to change the timeout value which fits your system configuration.

The following example shows how the timeout value is set to 4 minutes:

```
lvchange -t 240 /dev/vg_oradb/system_default
```

It is recommended that the timeout value for physical volumes should not change from the default value (zero).
7. Use the DS CLI database protection commands to apply database protection to the database files. You must have the Oracle administrator user ID (SYSDBA, or equivalent privilege) and password on hand.

Note: When the Oracle database uses Operating System Authentication, either one of the following conditions must be met:

- Make the root user's PRIMARY group the DBA group
- Use the **newgrp** command to change the root user's primary group to the DBA group before running the DS CLI **setdbcheck** and **lsdbcheck** commands.

Note: When an administrator executes Database Protection commands such as the **lsdbcheck** command with Oracle 10g Database Release 2, the CMUC00316E error might be reported. In this situation, it is recommended that execution access permission is set on every directory path from the root directory to the Oracle Home directory.

Example: When the Oracle Home directory is /app/ora10gr2/product/10.2.0/db_1, ensure that the following directories have execution access permission:

- /app/ora10gr2/product/10.2.0/db_1 (=Oracle Home)
- /app/ora10gr2/product/10.2.0/
- /app/ora10gr2/product/
- /app/ora10gr2/
- /app

Chapter 2. Managing database protection on sites that have an IP connection

This section provides the information that you need to configure and maintain your system so that the IBM Database Protection feature can fully use the Oracle data block validation feature.

The Oracle data block validation feature allows IBM Database Protection to detect the types of corruption that is caused by underlying disks, storage systems, or I/O systems. Before a data block is written to disk, a value is computed and stored in the block. When the block is subsequently read from disk, the value is recomputed and compared with the stored value. Thus IBM Database Protection prevents corrupted data from being written to permanent storage.

Your system must meet the following prerequisites before you can use the IBM Database Protection feature:

- For IBM DS8000 models, you must create the DS volumes that receive the benefit of the IBM Database Protection feature.
- You must activate your license activation code that you receive from IBM to use the IBM Database Protection feature. Issue the DS CLI **applykey** command with the correct activation code.
- You must have the appropriate DS8000 licensed microcode bundle installed on your system.
- The Oracle software must be at one of the following levels:
 - Oracle 9i Database Release 2 (Oracle 9iR2)
 - Oracle 10g Database Release 2 (Oracle 10gR2)
- Your database server must run one of the following operating systems:
 - Sun Solaris 8 running on SPARC platform (Oracle 9iR2 only)
 - Sun Solaris 10 running on SPARC platform
 - HP-UX 11i (11.11) (Oracle 9iR2 only)
 - HP-UX 11i v2 (11.23)
 - HP-UX 11iv3 (11.31) (Oracle 10gR2 only)
- Use IBM Database Protection only with the following database file types:
 - Data file (tablespace)
 - Control file
 - Redo log file

Notes:

1. None of these database file types can be allocated on a filesystem. Filesystems are not supported.
2. Temporary table space is not supported.

The major tasks that you perform to use IBM Database Protection involve that you put Oracle data under IBM Database Protection or remove the protection.

The DS CLI gathers the information about the relationship that exists between Oracle data and its locations on the DS volumes that are on the server where the database resides. DS CLI then performs transactions that affect the (based on

analysis) DS8000 through the DS8000 hardware management console. The former process requires DS CLI to have direct access to Ds volumes while the latter process requires IP network access to the hardware management console.

When your DS CLI client has access to the DS volumes and the hardware management console, DS CLI seamlessly performs the internal tasks. When your database installation keeps the customer IP network separated from the storage administration network, you must have two DS CLI clients ready: the one is run on the database server and the other is run on a server that has an access to the hardware management console. Figure 3 and Figure 4 illustrate these two separate setups

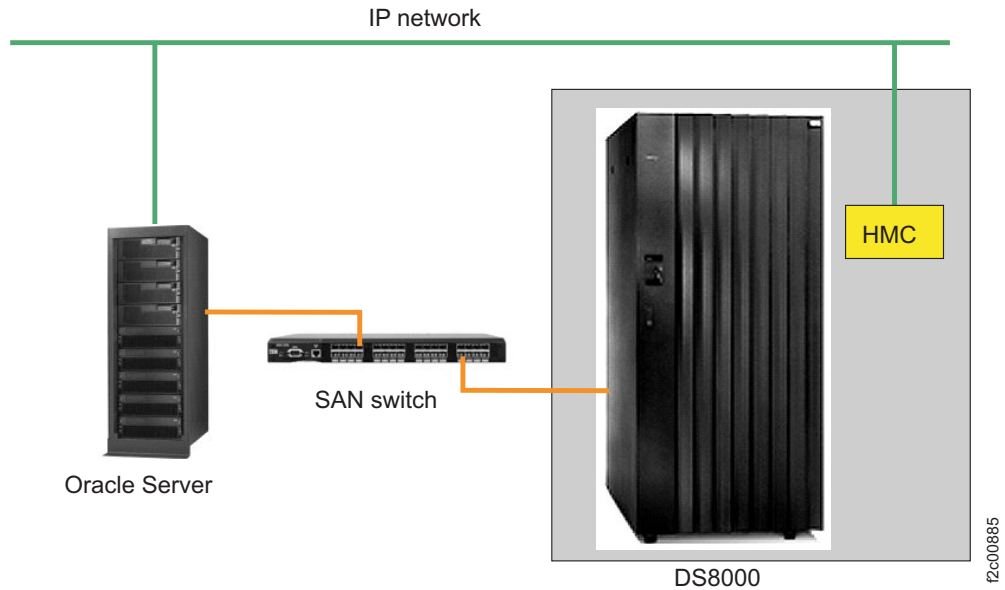


Figure 3. Direct access to IP network is available

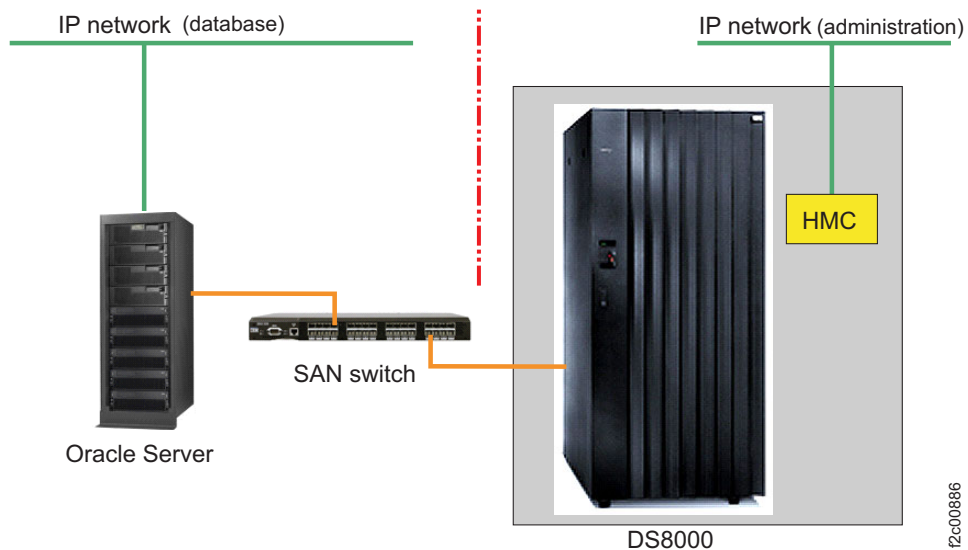


Figure 4. Direct access to IP network is not available

The tasks that are described in this section apply to the following situations:

- Adding the data block validation feature to a single tablespace

- Removing the data block validation feature from a single tablespace
- Changing the error reporting settings
- Adding data block validation to all the database files
- Removing data block validation from all the database files
- Extending a tablespace by resizing the database data file
- Extending a tablespace by adding database files
- Disabling data block validation for volumes
- Enabling data block validation for volumes
- Clearing database extent configuration from volumes
- Disabling data block validation for volume groups
- Enabling data block validation for volume groups
- Clearing database extent configuration from all the volumes managed by a volume group

Adding data block validation to a single tablespace

Complete this task to add data block validation to a single tablespace.

Ensure that you have performed all the prerequisites before you attempt this task.

A tablespace is like a file system on a set of disk drives. It is the lowest logical layer of the Oracle data structure. Data block validation is a validation check performed by the IBM Database Protection feature to compare the results to the original value and (assuming that the values match) to conclude that the data is not corrupted.

Perform the following step to add the data block validation to a single tablespace. The example command in this task is shown in two formats. The first format shows the type of information that the command requires. The second format is an example command with declared values for the variables.

Issue the **setdbcheck** command to add the data block validation feature to a single tablespace. Enter the **setdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>setdbcheck -dev storage_image_ID -dbuser username/password
-action add -ts tablespace
```

Example

```
dscli>setdbcheck -dev IBM.2107-99FA120 -dbuser sys/oracle
-action add -ts TS1
```

Note: The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **setdbcheck** command fails.

Removing data block validation from a single tablespace

Complete this task to remove the data block validation feature from a single tablespace.

Ensure that your system setup meets the requirements that are outlined in **Managing database protection on sites that have an IP connection**.

A tablespace is like a file system on a set of disk drives. It is the lowest logical layer of the Oracle data structure. The data block validation feature is a validation check that is performed by the IBM Database Protection feature to compare the validation results to the original value and (assuming that the sums match) to conclude that the data is not corrupted.

Perform the following step to remove the data block validation from a single tablespace. The example command in this task is shown in two formats. The first format shows the type of information that the command requires. The second format is an example command with declared values for the variables.

Issue the **setdbcheck** command to remove the data block validation feature from a single tablespace. Enter the **setdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>setdbcheck -dev storage_image_ID -dbuser username/password  
-action remove -ts tablespace
```

Example

```
dscli>setdbcheck -dev IBM.2107-99FA120 -dbuser sys/oracle  
-action remove -ts TS1
```

Notes:

1. The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **setdbcheck** command fails.
2. The **setdbcheck -action remove** command must be processed before removing the database file. Otherwise, the **setdbcheck** command cannot identify the storage space where the removed database file used to occupy. A reallocation of that same storage space can cause an unexpected error.
3. The number of database extents is limited to 32 per DS volume; leaving unnecessary database extents might result in a lack of database extents to enable database protection for some other database files.

Changing the error reporting settings

Complete this task to change how incorrect I/O errors that occur during the data block validation process are reported on a single tablespace. The change in settings can be done without disabling data block validation.

Ensure that your system setup meets the requirements that are outlined in **Managing database protection on sites that have an IP connection**.

IBM Database Protection allows you to select one of two methods to report Oracle data block validation I/O transaction errors. You can choose either reject I/O or log only. The following descriptions provide the information that you can use to make the best choice for your system.

Reject I/O

This method of reporting rejects the write requests and logs the event. The I/O requester on the database server determines that this event is an I/O error and takes the necessary action to retry the write request. The DS8000 logs the event and notifies the system administrator through email, SNMP trap notification, or by both, if your system is configured for this feature.

Note: The DS8000 manages the data block validation failure by rejecting the transaction and logging the event. This action prevents the DS8000 logging resource from being overwhelmed by continuous attempts to process the corrupted I/O transaction.

Reject I/O is the recommended method for reporting data block validation errors. You can set this method with the **setdbcheck** command using the **-erraction rejectio** parameter.

Log Only

This method of reporting processes the write request and logs the event. The corrupted I/O data is accepted into a database file that is under database protection as if IBM Database Protection did not work. However, the DS8000 storage system does log the event as an acceptance of a data block validation failure. Your system administrator is notified through email, SNMP trap notification, or both, if your system is configured for this feature.

You set the log only method of reporting with the **setdbcheck** command using the **-erraction logonly** parameter.

The **setdbcheck** command is primarily used to set the data protection for each database file (tablespace) and to designate how incorrect I/O errors are reported during the data block validation process. It is possible to change the way incorrect I/O errors are reported without affecting the tablespace by using the **-force** parameter with the **setdbcheck** command. If you attempt to change the way that the errors are reported and do not use the **-force** parameter, the command fails.

A tablespace is like a file system on a set of disk drives. It is the lowest logical layer of the Oracle data structure. The data block validation process is a validation check that is performed by the IBM Database Protection feature to compare the results to the original data value and (assuming that the values match) to conclude that the data is not corrupted.

Perform the following step to change the way that incorrect I/O errors are reported during the data block validation process. The example command in this task is shown in two formats. The first format shows the type of information that the command requires. The second format is an example command with declared values for the variables.

Issue the **setdbcheck** command with the **-force** parameter to change the way incorrect I/O errors are reported during the data block validation process. Enter the **setdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>setdbcheck -dev storage_image_ID -dbuser username/password  
-action add -erraction [logonly | rejectio -force -ts tablespace
```

Example

```
dscli>setdbcheck -dev IBM.2107-99FA120 -dbuser sys/oracle  
- action add -erraction rejectio -force -ts TS1
```

Notes:

1. The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **setdbcheck** command fails.

2. The **-action add** parameter is required when you are changing the error setting. This parameter directs the system to override the prior action.
3. The **-erraction logonly** parameter specifies that any incorrect I/O transaction during the data block validation process that causes an error is to be logged but not rejected.
4. The **-erraction rejectio** parameter specifies that any incorrect I/O transaction during the data block validation process is to be rejected in addition to being logged.
5. The **-force** parameter causes the system to accept the change in the data block validation I/O error reporting when you change from **-erraction logonly** to **-erraction rejectio** or **-erraction rejectio** to **-erraction logonly**.

Adding data block validation to all database files

Complete this task to add the data block validation feature to all supported database files.

Ensure that your system setup meets the requirements that are outlined in **Managing database protection on sites that have an IP connection**.

The data block validation process can be applied to all the database files that are managed by the IBM Database Protection feature. The following database files can be managed by the IBM Database Protection feature:

- Data file (tablespace)
- Control file
- Redo log file

Perform the following steps to add data block validation to all database files that are managed by the IBM Database Protection feature at once. The example commands in this task are shown in two formats. The first format shows the type of information that the command requires. The second format is an example command with declared values for the variables.

1. Issue the **setdbcheck** command without specifying any specific database file, to add the data block validation process to all database files that are managed by the IBM Database Protection feature. Enter the **setdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>setdbcheck -dev storage_image_ID -dbuser username/password
-action add
```

Example

```
dscli>setdbcheck -dev IBM.2107-99FA120 -dbuser sys/oracle
-action add
```

Note: The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **setdbcheck** command fails.

2. Issue the **lsdbcheck -l** command to view the database protection state and error action for each managed tablespace or database file. Enter the **lsdbcheck -l** command at the dscli command prompt with the following parameters and variables:

```
dscli>lsdbcheck -dev storage_image_ID -l -dbuser username/password
```

Example

```
dscli>lsdbcheck -dev IBM.2107-99FA120 -l -dbuser sys/oracle
```

Note: The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **lsdbcheck** command fails.

3. Issue the **showfbvol** command to view the number of database extents that are associated with the specified DS volume in the storage unit. Enter the **showfbvol** command at the dscli command prompt with the following parameters and variables:

```
dscli>showfbvol volume_ID
```

Example

```
dscli>showfbvol 1010
```

Removing data block validation from all database files

Complete this task to remove data block validation from all supported database files before you remove the whole database instance from the system.

Ensure that your system setup meets the requirements that are outlined in **Managing database protection on sites that have an IP connection**.

It is possible that you have applied the data block validation process to all the database files that are managed by the IBM Database Protection feature. The following database files can be managed by the IBM Database Protection feature:

- Data file (tablespace)
- Control file
- Redo log file

Perform the following steps to remove data block validation from all database files that are managed by the IBM Database Protection feature. The example commands in this task are shown in two formats. The first format shows the type of information that the command requires. The second format is an example command with declared values for the variables.

1. Issue the **setdbcheck** command with the **-action remove** parameter, but without specifying a specific database file, to remove the data block validation process from all the database files that are managed by the IBM Database Protection function. Enter the **setdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>setdbcheck -dev storage_image_ID -dbuser username/password  
-action remove
```

Example

```
dscli>setdbcheck -dev IBM.2107-99FA120 -dbuser sys/oracle  
-action remove
```

Notes:

- a. The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **setdbcheck** command fails.
- b. The **setdbcheck -action remove** command must be processed before you remove the database file. Otherwise, the **setdbcheck** command

cannot identify the storage space where the removed database file used to occupy. A reallocation of this same storage space can cause and unexpected error.

- c. The number of database extents is limited to 32 per DS volume; leaving unnecessary database extents might result in a lack of database extents to enable database protection for some other database files.
2. Issue the **lsdbcheck** command to view if the IBM Database Protection feature has been removed. Enter the **lsdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>lsdbcheck -dev storage_image_ID -dbuser username/password
```

Example

```
dscli>lsdbcheck -dev IBM.2107-99FA120 -dbuser sys/oracle
```

Note: The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **lsdbcheck** command fails.

Extending the size of a tablespace - resize database data file

Complete this task to extend the size of a tablespace. There are two methods you can use to do this: resize the database data file (only when you are using raw logical volume) or add a new database data file. This task describes how to use the resize the database data file method.

Ensure that your system setup meets the requirements that are outlined in **Managing database protection on sites that have an IP connection**. Also, you must ensure that the database instance is started up.

A tablespace is like a file system on a set of disk drives. It is the lowest logical layer of the Oracle data structure. There might be occasions when you need to extend the tablespace size. You can use one of the following methods to extend the tablespace size:

- Resize an existing database data file which forms the tablespace
- Add a new database data file to the tablespace

To use the resize the database data file method to extend the tablespace size, you must do the following:

1. Remove data block validation from the tablespace you are modifying.
2. Change the logical volume size.
3. Resize the database data file.
4. Add data block validation back to the tablespace you have modified.
5. Verify that data block validation has been added to the tablespace.

Perform the following steps to extend a tablespace by resizing the database data file. The example DS CLI commands in this task are shown in two formats. The first format shows the type of information that the command requires. The second format is an example command with declared values for the variables.

1. Issue the **setdbcheck** command to remove data block validation from the tablespace. Enter the **setdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>setdbcheck -dev storage_image_ID -dbuser username/password  
-action remove -ts tablespace
```

Example

```
dscli>setdbcheck -dev IBM.2107-99FA120 -dbuser sys/oracle  
-action remove -ts TS1
```

Note: The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **setdbcheck** command fails.

2. Use the Logical Volume Manager commands to change the logical volume size. Ensure that you keep enough space in the logical volume for the extended tablespace size.

For example, you might use the **lvextend** command if you are using an HP LVM.

3. Issue an SQL command to resize the database data file.

The following is an example of how to set the database data file in the raw logical volume `/dev/vg01/rlvol01` to 200 MB.

```
ALTER DATABASE DATAFILE '/dev/vg01/rlvol01' RESIZE 200M;
```

4. Issue the **setdbcheck** command to add data block validation back to the tablespace that you have modified. Enter the **setdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>setdbcheck -dev storage_image_ID -dbuser username/password  
-action add -erraction rejectio -ts tablespace
```

Example

```
dscli>setdbcheck -dev IBM.2107-99FA120 -dbuser sys/oracle -action add  
-erraction rejectio -ts TS1
```

Notes:

- a. The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **setdbcheck** command fails.
 - b. You must specify the **-erraction** parameter explicitly to what it was before you made the modification to the tablespace. Or, you can specify a different parameter if you want to use the other error reporting scheme.
5. Issue the **lsdbcheck** command to view the database protection state and error action for the tablespace. Enter the **lsdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>lsdbcheck -dev storage_image_ID -l -dbuser username/password  
-ts tablespace_name
```

Example

```
dscli>lsdbcheck -dev IBM.2107-99FA120 -l -dbuser sys/oracle -ts TS1
```

Note: The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **lsdbcheck** command fails.

Extending the size of a tablespace - add database data file

Complete this task to extend the size of a tablespace. There are two methods you can use to do this: resize the database data file (only when you are using raw logical volume) or add a new database data file. This task describes how to add a database data file to extend the size of a tablespace.

Ensure that your system setup meets the requirements that are outlined in **Managing database protection on sites that have an IP connection**. Also, you must ensure that the database instance is started up.

A tablespace is like a file system on a set of disk drives. It is the lowest logical layer of the Oracle data structure. There might be occasions when you need to extend the tablespace size. You can use one of the following methods to extend the tablespace size:

- Add a new database data file to the tablespace
- Resize an existing database data file which forms the tablespace

To use the add database file method to extend the tablespace size you must do the following:

1. Create the logical volume that you want to add to the tablespace.
2. Add the logical volume to the tablespace as a database data file.
3. Use the **-force** parameter to adjust the data block validation of the tablespace you have modified .
4. Verify that data block validation has been added to the tablespace.

Perform the following steps to extend a tablespace by adding a database data file. The example DS CLI commands in this task are shown in two formats. The first format shows the type of information that the command requires. The second format is an example command with declared values for the variables.

1. Create the logical volume that you want to add to the tablespace.
2. Issue the following SQL command to add a logical volume to the tablespace as a database data file.

```
ALTER TABLESPACE TS1 ADD DATAFILE '/dev/vg01/r1vo102'SIZE 100M;
```

Note: With this command you have increased the size of tablespace TS1 by 100M bytes.

3. Issue the **setdbcheck** command to add data block validation to the tablespace that you have modified. Enter the **setdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>setdbcheck -dev storage_image_ID -dbuser username/password  
-action add -erraction rejectio -ts tablespace -force
```

Example

```
dscli>setdbcheck -dev IBM.2107-99FA120 -dbuser sys/oracle  
-action add -erraction rejectio -ts TS1 -force
```

Notes:

- a. The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **setdbcheck** command fails.
 - b. The **-force** parameter is required because data block validation exists on the tablespace.
4. Issue the **lsdbcheck** command to view the database protection state and error action for the tablespace. Enter the **lsdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>lsdbcheck -dev storage_image_ID -l -dbuser username/password  
-ts tablespace_name
```

Example

```
dscli>lsdbcheck -dev IBM.2107-99FA120 -l -dbuser sys/oracle -ts TS1
```

Note: The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **lsdbcheck** command fails.

Disabling data block validation for volumes

Complete this task when you need to temporarily disable data block validation for specific DS volumes.

Ensure that your system setup meets the requirements that are outlined in **Managing database protection on sites that have an IP connection**. Also, you must ensure that the database instance is started and that the volumes contain the Oracle extents that allow the use of the IBM Database Protection feature.

The need to temporarily disable data block validation from a set of DS volumes might occur when you are restoring data from the media to the DS volumes that are under the database protection. This action avoids the unexpected I/O transaction errors that can occur when using the data block validation process.

Perform the following steps to temporarily disable data block validation for a set of DS volumes. The example DS CLI commands in this task are shown in two formats. The first format shows the type of information that the command requires. The second format is an example command with declared values for the variables.

1. Issue the **managedbcheck** command to temporarily disable data block validation from a specified set of DS volumes. Enter the **managedbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>managedbcheck -dev storage_image_ID -volume volume_ID  
-action disable
```

Example

```
dscli>managedbcheck -dev IBM.2107-99FA120 -volume 0100-01FF -action disable
```

Notes:

- a. The **-volume** parameter allows you to specify multiple volumes and volumes within a range value. However, when you specify multiple volumes, you must separate each volume number with a comma and no space between the numbers.
- b. You cannot use the **-volume** parameter and the **-volgrp** parameter in the same command.

When this command processes successfully, you receive the following message:

```
CMUC00281I The definition of database extents for the volume IDs or  
volume group IDs that you have specified has been temporarily disabled.
```

2. Issue the **lsdbcheck** command to identify the database files affected by the **managedbcheck** command on the DS volumes that you wanted to disable. Enter the **lsdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>lsdbcheck -dev storage_image_ID -l -dbuser username/password  
-state temporarilydisabled
```

Example

```
dscli>lsdbcheck -dev IBM.2107-99FA120 -l -dbuser sys/oracle -state  
temporarilydisabled
```


Note: The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **lsdbcheck** command fails.

Enabling data block validation for volumes

Complete this task to enable data block validation for the DS volumes that were temporarily disabled from using the IBM Database Protection feature.

Ensure that your system setup meets the requirements that are outlined in **Managing database protection on sites that have an IP connection**. Also, you must ensure that the database instance is started.

After you have temporarily disabled data block validation from a set of DS volumes and successfully restored your data, you must enable data block validation for these volumes.

Perform the following steps to enable data block validation for the set of DS volumes where you have temporarily disabled data block validation. The example DS CLI commands in this task are shown in two formats. The first format shows the type of information that the command requires. The second format is an example command with declared values for the variables.

1. Issue the **managedbcheck** command to enable data block validation for those DS volumes where you have temporarily disabled the data block validation process. Enter the **managedbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>managedbcheck -dev storage_image_ID -volume volume_ID  
-action enable
```

Example

```
dscli>managedbcheck -dev IBM.2107-99FA120 -volume 0100-01FF -action enable
```

Notes:

- a. The **-volume** parameter allows you to specify multiple volumes and volumes within a range value. However, when you specify multiple volumes, you must separate each volume number with a comma and no space between the numbers.
- b. You cannot use the **-volume** parameter and the **-volgrp** parameter in the same command.

When this command processes successfully, you receive the following message:

```
CMUC00282I The definition of database extents for the volume IDs or  
volume group IDs that you have specified has been enabled.
```

2. Issue the **lsdbcheck** command to view the database protection state for the database files. This is a verification step to ensure that the process of the **managedbcheck** command on the DS volumes that you want to enable restores the database protection state. Enter the **lsdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>lsdbcheck -dev storage_image_ID -l -dbuser username/password
```

Example

```
dscli>lsdbcheck -dev IBM.2107-99FA120 -l -dbuser sys/oracle
```

Note: The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **lsdbcheck** command fails.

Clearing database extent configuration from volumes

Complete this task to clear all database extent configurations from DS volumes whose database extents have lost consistency with the current Oracle database configuration. All the database extents set for the specified volumes are removed.

Ensure that your system setup meets the requirements that are outlined in **Managing database protection on sites that have an IP connection**. Also, you must ensure that the database instance is started.

In time you might want to perform a maintenance function on the database extents that have lost consistency with the current Oracle database configuration. This allows you to create a configuration. All the database extents set for the specified volumes are removed.

Perform the following steps to clear all database extent configurations from DS volumes whose database extents have lost consistency with the current Oracle database configuration. The example DS CLI commands in this task are shown in two formats. The first format shows the type of information that the command requires. The second format is an example command with declared values for the variables.

Issue the **managedbcheck** command to clear all database extent configurations from the DS volumes that you specify. Enter the **managedbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>managedbcheck -dev storage_image_ID -volume volume_ID  
-action clear
```

Example

```
dscli>managedbcheck -dev IBM.2107-99FA120 -volume 0100-01FF -action clear
```

Notes:

1. The **-volume** parameter allows you to specify multiple volumes and volumes within a range value. However, when you specify multiple volumes, you must separate each volume number with a comma and no space between the numbers.
2. You cannot use the **-volume** parameter and the **-volgrp** parameter in the same command.

When this command processes successfully, you receive the following message:

```
CMUC00283I The definition of database extents for the volume IDs or  
volume group IDs that you have specified has been cleared.
```

Disabling data block validation for volume group

Complete this task when you need to temporarily disable data block validation for the group of DS volumes managed by a DS volume group.

Ensure that your system setup meets the requirements that are outlined in **Managing database protection on sites that have an IP connection**. Also, you must ensure that the database instance is started up and that the volumes in the DS volume group contain the Oracle extents that allow the use of the IBM Database Protection feature.

The need to temporarily disable data block validation from a DS volume group might occur when you are restoring data from the media to the DS volumes under

the database protection. This action avoids the unexpected I/O transaction errors that can occur when using the data block validation process.

Perform the following steps to temporarily disable data block validation for a DS volume group. The example DS CLI commands in this task are shown in two formats. The first format shows the type of information that the command requires. The second format is an example command with declared values for the variables.

1. Issue the **managedbcheck** command to temporarily disable data block validation from a specified DS volume group. Enter the **managedbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>managedbcheck -dev storage_image_ID -volgrp volume_group_ID
        -action disable
```

Example

```
dscli>managedbcheck -dev IBM.2107-99FA120 -volgrp V11 -action disable
```

Notes:

- a. The **-volgrp** parameter allows you to specify multiple volume groups. However, when specifying multiple volume groups, you must separate each volume group number with a comma and no space between the numbers.
- b. You cannot use the **-volgrp** parameter and the **-volume** parameter in the same command.

When this command processes successfully, you receive the following message:

```
CMUC00281I The definition of database extents for the volume IDs or
volume group IDs that you have specified has been temporarily disabled.
```

2. Issue the **lsdbcheck** command to identify the database files affected by the **managedbcheck** command on the DS volumes that you wanted to disable. Enter the **lsdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>lsdbcheck -dev storage_image_ID -l -dbuser username/password
        -state temporarilydisabled
```

Example

```
dscli>lsdbcheck -dev IBM.2107-99FA120 -l -dbuser sys/oracle -state
temporarilydisabled
```

Note: The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **lsdbcheck** command fails.

Enabling data block validation for volume group

Complete this task to enable data block validation for the DS8000 volume group that was temporarily disabled from using the IBM Database Protection feature.

Ensure that your system setup meets the requirements that are outlined in **Managing database protection on sites that have an IP connection**. Also, you must ensure that the database instance is started.

After you have temporarily disabled data block validation for DS8000 volume group and successfully restored your data, you must enable data block validation for the volume group.

Perform the following steps to enable data block validation for the DS8000 volume group where you have temporarily disabled the data block validation process. The example DS CLI commands in this task are shown in two formats. The first format shows the type of information that the command requires. The second format is an example command with declared values for the variables.

1. Issue the **managedbcheck** command to enable data block validation for those DS8000 volume groups where you have temporarily disabled the data block validation process. Enter the **managedbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>managedbcheck -dev storage_image_ID -volgrp volume__group_ID  
-action enable
```

Example

```
dscli>managedbcheck -dev IBM.2107-99FA120 -volgrp V11 -action enable
```

Notes:

- a. The **-volgrp** parameter allows you to specify multiple volume groups. However, when you specify multiple volume groups, you must separate each volume group number with a comma and no space between the numbers.
- b. You cannot use the **-volgrp** parameter and the **-volume** parameter in the same command.

When this command processes successfully, you receive the following message:

```
CMUC00282I The definition of database extents for the volume IDs or  
volume group IDs that you have specified has been enabled.
```

2. Issue the **lsdbcheck** command to view the database protection state for the database files. This is a verification step to ensure that the process of the **managedbcheck** command on the volumes that you want to enable restores the database protection state. Enter the **lsdbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>lsdbcheck -dev storage_image_ID -l -dbuser username/password
```

Example

```
dscli>lsdbcheck -dev IBM.2107-99FA120 -l -dbuser sys/oracle
```

Note: The **-dbuser** parameter specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **lsdbcheck** command fails.

Clearing database extent configuration from all the volumes managed by a volume group

Complete this task to clear all database extent configuration from DS volume groups whose database extents have lost consistency with the current Oracle database configuration. All the database extents set for the specified volume groups are removed.

Ensure that your system setup meets the requirements that are outlined in **Managing database protection on sites that have an IP connection**. Also, you must ensure that the database instance is started.

In time you might want to perform a maintenance function on the database extents that have lost consistency with the current Oracle database configuration. This allows you to create a configuration. All the database extents set for the specified volume groups are removed.

Perform the following steps to clear all database extent configuration from DS volume groups whose database extents have lost consistency with the current Oracle database configuration. The example DS CLI commands in this task are shown in two formats. The first format shows the type of information that the command requires. The second format is an example command with declared values for the variables.

Issue the **managedbcheck** command to clear all database extents from the DS volume groups that you specify. Enter the **managedbcheck** command at the dscli command prompt with the following parameters and variables:

```
dscli>managedbcheck -dev storage_image_ID -volgrp volume_Group_ID  
-action clear
```

Example

```
dscli>managedbcheck -dev IBM.2107-99FA120 -volgrp V11 -action clear
```

Notes:

1. The **-volgrp** parameter allows you to specify multiple volume groups. However, when you specify multiple volume groups, you must separate each volume group number with a comma and no space between the numbers.
2. You cannot use the **-volgrp** parameter and the **-volume** parameter in the same command.

When this command processes successfully, you receive the following message:

```
CMUC00283I The definition of database extents for the volume IDs or  
volume group IDs that you have specified has been cleared.
```

Chapter 3. Database Protection commands

This section contains commands that are used to perform database protection functions.

Use the following commands to configure the database protection feature:

- **setdbcheck**
- **applydbcheck**
- **managedbcheck**
- **offloaddbcheck**
- **lsdbcheck**

The **setdbcheck** command sets the database protection for each database file and includes the opportunity for you to designate how you want incorrect I/O transaction errors treated.

The **applydbcheck** command applies the database extent definitions stored in the database extent file to each storage image. This command is not a standalone command. It is always used as part of a scenario that requires the use of 3 commands, either **offloaddbcheck**, **setdbcheck**, and **applydbcheck** or **offloaddbcheck**, **managedbcheck**, and **applydbcheck**. (The **offloaddbcheck**, **managedbcheck**, and **applydbcheck** command combination applies when you must apply a previously offloaded database extent configuration, after you enable or disable database protection, or after you clear database extent definitions for some or all of the volumes or volume groups.)

The **managedbcheck** command temporarily disables database protection and then is used to re-enable the protection. The command is also used to clean up the database extent configuration on storage images that have lost consistency with the current Oracle database configuration.

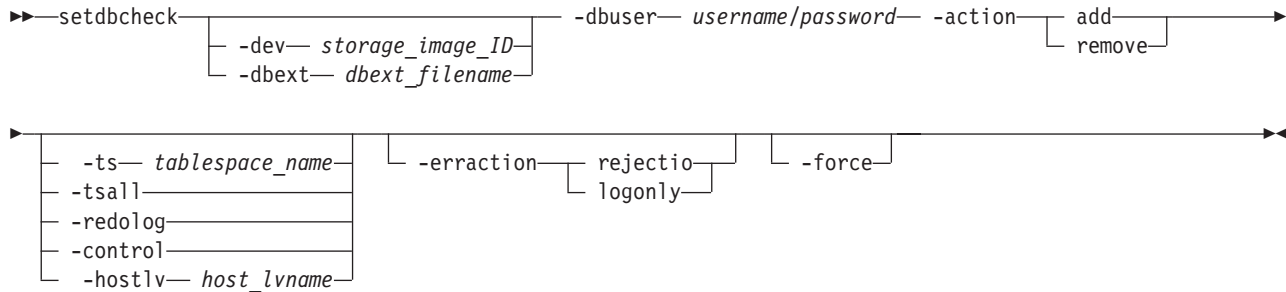
The **offloaddbcheck** extracts the database extent configuration from a storage image to a designated database extent file.

The **lsdbcheck** command displays a report that lists the database protection state and error action per database file. In addition, the command lists the device names and DS volumes where the database file is located.

setdbcheck

The **setdbcheck** command sets the database protection for each database file and allows you to designate how an incorrect I/O transaction is managed. You do not need to use any other commands to set the data protection on a database file if the following conditions apply: the whole region of target database files are allocated on DS volumes from a single storage image and your database server has an IP network connection to a hardware management console that manages the storage image. If either of these conditions do not exist, you must use the **setdbcheck** command with the **offloaddbcheck** and **applydbcheck** commands to gather and apply database extent definitions. Only a person with administrator authority can

initiate this command. This command can only be used on an HP-UX 11i (11.11), HP-UX 11i v2 (11.23), HP-UX 11i v3 (11.31), Sun Solaris 10, or Sun Solaris 8 operating system.



Parameters

Note:

1. Ensure that the following environment variables are set before you use the IBM database protection commands:
 - ORACLE_HOME
 - ORACLE_SID
2. With large configurations of Oracle database, the **setdbcheck** command might take long time to complete.

-dev *storage_image_ID* | **-dbext** *dbext_filename*

(Optional) Specifies the storage image ID or the database extent file.

Notes:

1. If you do not specify the storage image ID, the default value for the *dev* variable in your profile file is used.
2. If you specify the **-dbext** parameter, the value for the **-dev** parameter is ignored.
3. You cannot use the **-dev** parameter with the **-dbext** parameter.

The database extent file must already exist to use the **-dbext** parameter. The database extent configuration is retrieved from the specified database extent file, and the command makes changes to the same file based on the **-action** parameter. Also, the updated database extent file must be applied to actual volumes by using the **applydbcheck** command in order for the changes to take effect.

If the database extent file is not specified, the database extent configuration is retrieved from a storage image that is specified by the **-dev** parameter or the *dev* specified in your profile and reapplied to the storage image.

-dbuser *username/password*

(Required) Specifies the user ID and the password that has been used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization. Otherwise, the **setdbcheck** command fails.

Note: When the Oracle database uses Operating System Authentication, either one of the following conditions must be met:

- Make the root user's PRIMARY group the DBA group

- Use the **newgrp** command to change the root user's primary group to the DBA group before running the **setdbcheck** command.

Every running Oracle database is associated with an Oracle instance. When a database is started on a database server (regardless of the type of computer), Oracle allocates a memory area called the System Global Area (SGA) and starts one or more Oracle processes. This combination of the SGA and the Oracle processes is called an Oracle instance.

-action add | -action remove

(Required) Specifies whether database protection on a database file is enabled or disabled as follows:

-action add

Specifies that database extent definitions be added for the specified database file to activate database protection.

-action remove

Specifies that database extent definitions be removed for the specified database file to deactivate database protection for that file.

-erraction rejectio | -erraction logonly

(Optional) Specifies how the system responds to the database server if the data block validation detects a corruption in data. You can specify that the system take one of the following actions:

-erraction rejectio

The database server receives an error response from the DS8000 for the request of irregular write I/O and the corrupted data won't be written to disk. The error will be recorded in DS storage error log, and an e-mail notification or an SNMP alert (or both) will be sent from DS8000 hardware management console to the designated computer. This is the default action if the **-erraction** parameter is not specified.

-erraction logonly

The database server does not receive an error response from the DS8000 for the request of an irregular write I/O, and the corrupted data is written to disk. The error is recorded in the DS storage error log, and an e-mail notification or an SNMP alert (or both) are sent from the DS8000 hardware management console to the designated computer.

Note: The destination of e-mail notification and SNMP alert must also be configured on the hardware management console.

-ts *tablespace_name* | -tsall | -redolog | -control | -hostlv *host_lvname*
(Optional) Specifies the database files to be processed.

You can specify one of these parameters per command use:

-ts *tablespace_name*

Use this parameter to specify that a designated tablespace be processed.

-tsall

Use this parameter to specify that all tablespace files be processed.

-redolog

Use this parameter to specify that all redo log files be processed.

-control

Use this parameter to specify that all control files be processed.

-hostlv *host_lvname*

Use this parameter to specify that a designated LVM logical volume be processed. This parameter can only be used with **-action remove** parameter.

If none of the previous parameters are specified, all of the database files of the Oracle instance specified by the ORACLE_SID environment variable are processed.

-force

(Optional) Specifies that the database extents be set for the database file even if the current protection setting is in an inconsistent state. For example, you might have an inconsistent state for a database file because you extended the size of the database file. Issuing a command with the **-force** parameter helps you to recover the database protection state from an inconsistent state. Issue the following command to recover from an inconsistent state:

```
dscli>setdbcheck -dbuser (username/password) -action add -erraction rejectio  
-force
```

Example

Invoking the setdbcheck command

```
dscli>setdbcheck -dev IBM.2107-1300861  
-dbuser (username/password) -action add -ts user1_data -erraction rejectio  
Date/Time: Wed Apr 25, 2006 11:45:08 AM JST IBM DSCLI Version:  
5.3.0.0 DS: IBM.2107-1300861
```

```
CMUC00287I setdbcheck: Database extents have been added to the database  
extent configuration on the storage image for TS:TS1 and database  
protection has been enabled for the specified database entity.
```

User tips when you cannot use setdbcheck as a stand-alone command

When either of the following conditions exist, issue the **setdbcheck** command as one of three commands that enable the database protection for your database files:

- The Oracle database server does not have a direct network connection to a hardware management console that manages the storage image. This storage image is associated with volumes where the target database files are allocated.
- The target database files are allocated on volumes from multiple storage images.

To enable the database protection for your database files, issue multiple commands as follows:

1. Issue the **offloadbcheck** command to retrieve the current database extent configurations from all associated storage images to a database extent file. These commands must be invoked from a host system that has IP connection to a hardware management console that manages the target storage images.

```
dscli> offloadbcheck -dev IBM.2107-1300861 -volgrp v11 dbext.xml  
dscli> offloadbcheck -dev IBM.2107-1300862 -volgrp v12 -append dbext.xml
```

2. Issue the **setdbcheck** command to update the database extents that have been extracted in the definition file. This command must be invoked on the database server.

```
dscli> setdbcheck -dbuser ... -ts TS1 -action add -erraction rejectio  
-dbext dbext.xml  
dscli> setdbcheck -dbuser ... -ts TS2 -action add -erraction rejectio  
-dbext dbext.xml
```


3. Issue the **applydbcheck** command to apply the updated database extents that are stored in the database extent file to each storage image. You must invoke this command from a host system that has an IP connection to a hardware management console that manages the target storage images.

```
dsccli> applydbcheck -dev IBM.2107-1300861 dbext.xml
dsccli> applydbcheck -dev IBM.2107-1300862 dbext.xml
```

applydbcheck

The **applydbcheck** command applies the database extent definitions stored in the database extent file to each storage image. This command is not a standalone command. It is always used as part of a scenario that requires the use of three commands, either **offloaddbcheck**, **setdbcheck**, and **applydbcheck** or **offloaddbcheck**, **managedbcheck**, and **applydbcheck**. (The **offloaddbcheck**, **managedbcheck**, and **applydbcheck** command combination applies when you must apply a previously offloaded database extent configuration, after you enable or disable database protection, or after you clear database extent definitions for some or all of the volumes or volume groups.)

```

▶▶—applydbcheck—┬── -dev— storage_image_ID ┬── -volume—volume_ID[...], ┬── dbext_filename ─▶▶
                  └── -volgrp—volume_group_ID[...], └──

```

Parameters

The **applydbcheck** command is used in one of the following circumstances:

- You want to apply the updated database extents stored in the database extent file to each storage image. To get to this point you must first issue the **offloaddbcheck** command, followed by the **setdbcheck** command, and then issue the **applydbcheck** command.
- You want to restore the previous database extent definitions to the storage image after some maintenance work has been done. To get to this point you must first issue the **offloaddbcheck** command, followed by the **manangedbcheck** command, and then issue the **applydbcheck** command.

-dev storage_image_ID

(Optional) Specifies the storage image ID, which consists of manufacturer, machine type, and serial number.

Note: If you do not specify the storage image ID where the volumes or volume groups reside, the default value specified for the *devid* variable in your profile file is used.

-volume volume_ID [...]

(Optional) Specifies the volume or volumes where the database extents are applied as defined in the database extent file.

You can specify multiple volumes and volumes within a range value, however, you must designate them as follows:

Range of volumes

Provide the beginning number, followed by a dash (-), and the ending number (for example: 0100-010f)

Multiple volumes

Provide each volume number followed by a comma without a blank between the values (for example: 023f,0300,3100)

Mixed range and multiple volumes

Provide these values on the command line (for example:
0100-010f,0200-023f,0300)

Notes:

1. You cannot specify the **-volume** *volume_ID* and **-volgrp** *volume_group_ID* parameters together
2. CKD volumes and 520P or 520U fixed block volumes are ignored when you specify the **-volume** *volume_ID* parameter
3. Volumes from multiple storage images are not processed even if you specify the volumes in fully qualified ID format
4. If the **-volume** or **-volgrp** parameter values are not specified, all the database extents defined in the specified database extent file are applied.

-volgrp *volume_group_ID*[...]

(Optional) Specifies that the system examine the volumes associated with the designated volume group and apply the value for the number of associated database extents. The volume group ID must be for 512 fixed block volumes only.

Note: You can specify a volume group ID of V20 to indicate all fixed block volumes.

Multiple volume groups can be specified as long as you separate the volume group numbers with a comma and not blank space between the volume group numbers (for example, V5,V12).

You cannot specify the **-volume** *volume_ID* and **-volgrp** *volume_group_ID* parameters together.

If the **-volume** or **-volgrp** parameter values are not specified, all the database extents defined in the specified database extent file are applied.

dbext_filename

(Required) Specifies the name of the database extent definition file from which the database extent definitions are applied.

Example

Invoking the applydbcheck command

```
dscli>applydbcheck -dev IBM.2107-1300861  
-volume 1000-100F TS1
```

```
Date/Time: Wed Apr 25, 2006 11:45:08 AM JST IBM DSCLI Version:  
5.3.0.0 DS: IBM.2107-1300861
```

```
CMUC00280I The definition in the database extents file has been  
applied successfully.
```

offloaddbcheck

The **offloaddbcheck** command extracts the database extent configuration from a storage image to a designated database extent file.

```
►►—offloaddbcheck—┐ —volume—volume_ID[,...]—┐ —append—  
└ —dev— storage_image_ID ┘ └ —volgrp—volume_group_ID[,...]—┘ └ —quiet—┘ ►
```

Parameters

Notes:

1. The **offloadbcheck** command is primarily used in the following circumstances:
 - The database server is isolated from the network where the DS8000 hardware management console is connected.
 - The database files are allocated on volumes that are located on multiple storage images.
2. Use the **setdbcheck** command to set database protection if the database server has direct network connection to a hardware management console that manages the target storage image and volumes.

-dev *storage_image_ID*

(Optional) Specifies the storage image ID, which consists of manufacturer, machine type, and serial number.

Note: If you do not specify the storage image ID where the volumes or volume groups reside, the default value for the *dev* variable in your profile file is used.

-volume *volume_ID* [...]| **-volgrp** *volume_group_ID*[...]

(Required - one or the other of these parameters is required but cannot be used together on the same command line)

-volume specifies that the system offload the database extents for the designated volume or volumes.

-volgrp specifies that the system offload database extents from all volumes that belong to the designated volume group.

Note: You can specify a volume group ID of V20 to indicate all fixed block volumes.

You can specify multiple volumes and volumes within a range value or multiple volume groups, however, these must be designated as follows:

Range of volumes

Provide the beginning number, followed by a dash (-), and the ending number (for example: 0100-010f)

Multiple volumes

Provide each volume number followed by a comma without a blank between the values (for example: 023f,0300,3100)

Mixed range and multiple volumes

Provide these values on the command line (for example: 0100-010f,0200-023f,0300)

Multiple volume groups

Provide each volume group number followed by a comma without a blank between the values (for example: V5,V12)

Notes:

1. CKD volumes and 520P or 520U fixed block volumes are ignored when you specify the **-volume** *volume_ID* parameter

2. Volumes from multiple storage images are not processed even if you specify the volumes in fully qualified ID format

-append | -quiet

(Optional) **-append** specifies that the extracted database extent configuration be added to the designated database extent definition file.

Note: You cannot use this parameter with the **-quiet** parameter.

(Optional) **-quiet** specifies that the confirmation prompt for overwriting the existing database extent definition file be suppressed.

Note: You cannot use this parameter with the **-append** parameter.

dbext_filename

(Required) Specifies the name of the database extent definition file where the extracted database extent definitions are recorded. The file must be in XML format, and it should not be manually edited.

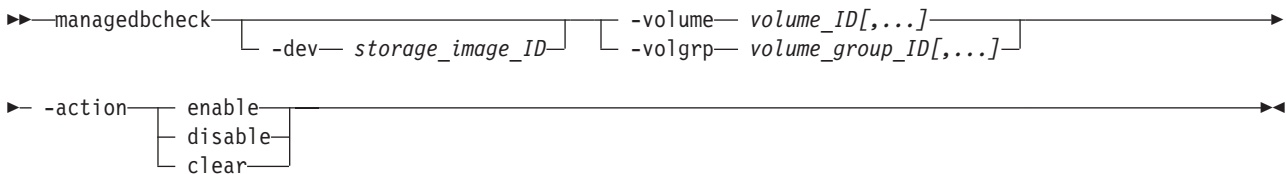
Example

Invoking the offloaddbcheck command

```
dsccli>offloaddbcheck -volume 0000 perftest
Date/Time: March 23, 2007 6:41:38 PM JST IBM DSCCLI Version: R10g.UT-20070223
DS: IBM.2107-7597721
CMUC00279W The file name that you have specified refers to an existing file.
Do you want to overwrite the file? [y/n]: y
CMUC00278I offloaddbcheck: The database extent configuration on the storage
image has been offloaded successfully to the database extents file
dbext.xml.
```

managedbcheck

The **managedbcheck** command temporarily disables database protection and then is used to re-enable the protection. The command is also used to clean up the database extent configuration on storage images that have lost consistency with the current Oracle database configuration.



Parameters

A typical use of the **-action [enable | disable]** parameter is to restore backup images of volumes or volume groups from other storage devices that do not initially use the IBM Database Protection validation rules. If you do not disable the validation functions, some of the I/O is rejected, and the backup image fails to correctly restore. Therefore, you must provide a script that accomplishes the following tasks:

1. Disable the database protection for the affected volumes or volume groups
2. Restore the data to the volumes or volume groups that are affected
3. Enable the database protection for the affected volumes or volume groups

You can use the **-action clear** parameter to perform maintenance on the database extents that have lost consistency with the current Oracle database configuration.

Because this command processes database extents on a per volume basis, not a per database file, careless use of this command can cause inconsistent configuration of database protection and unexpected write I/O failure. Ensure that you issue the **lsdbcheck** command after processing the **managedbcheck** command to verify that the protection states of the related database files are correct.

-dev *storage_image_ID*

(Optional) Specifies the storage image ID, which consists of manufacturer, machine type, and serial number.

Note: If you do not specify the storage image ID where the volumes or volume groups reside, the default value for the *dev* variable in your profile file is used.

-volume *volume_ID* [...]| **-volgrp** *volume_group_ID*[,...]

(Required - one or the other of these parameters is required but cannot be used together on the same command line)

-volume specifies that the system offload the database extents for the designated volume or volumes.

-volgrp specifies that the system offload database extents from all volumes that belong to the designated volume group.

Note: You can specify a volume group ID of V20 to indicate all fixed block volumes.

You can specify multiple volumes and volumes within a range value or multiple volume groups, however, these must be designated as follows:

Range of volumes

Provide the beginning number, followed by a dash (-), and the ending number (for example: 0100-010f)

Multiple volumes

Provide each volume number followed by a comma without a blank between the values (for example: 023f,0300,3100)

Mixed range and multiple volumes

Provide these values on the command line (for example: 0100-010f,0200-023f,0300)

Multiple volume groups

Provide each volume group number followed by a comma without a blank between the values (for example: V5,V12)

Notes:

1. CKD volumes and 520P or 520U fixed block volumes are ignored when you specify the **-volume** *volume_ID* parameter
2. Volumes from multiple storage images are not processed even if you specify the volumes in fully qualified ID format

-action *enable* | *disable* | *clear*

(Required) Specifies that one of the following actions be initiated on the specified volumes or volume groups:

enable

Specifies that the database protection feature be reactivated on the specified volumes or volume groups.

disable

Specifies that the database protection feature be disabled on the specified volumes or volume groups.

clear

Specifies that maintenance be performed on the database extents that have lost consistency with the current Oracle database configuration. All the database extents set for the specified volumes or volume groups are removed.

Example

Invoking the managedbcheck command

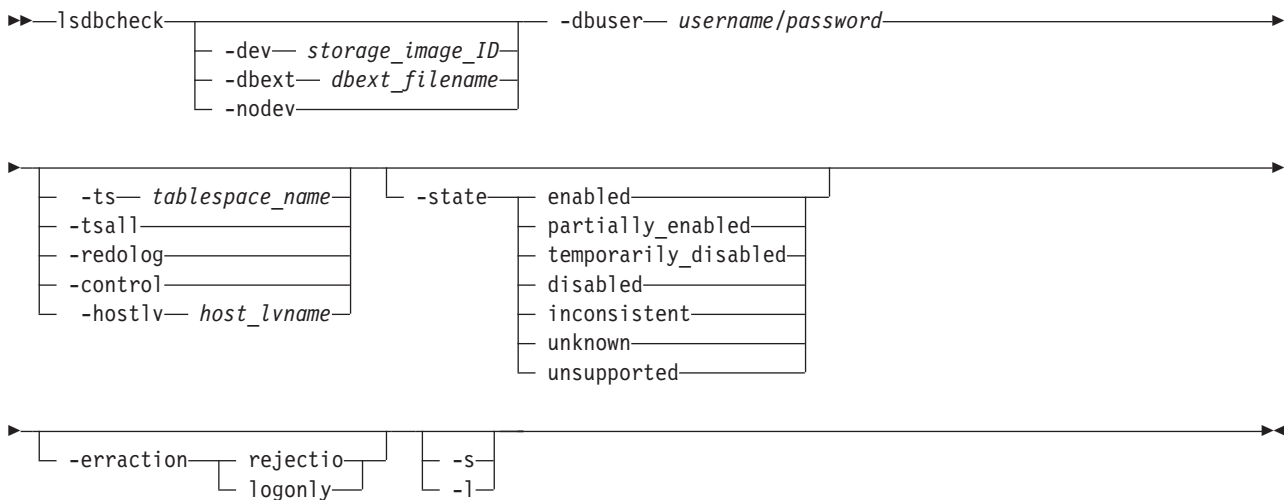
```
dscli>managedbcheck -dev IBM.2107-1300861  
-volume 1000-1003 -action clear
```

```
Date/Time: Wed Apr 25, 2006 11:45:08 AM JST IBM DSCLI Version:  
5.3.0.0 DS: IBM.2107-1300861
```

```
CMUC00000I managedbcheck: DB extents on the specified volumes are all  
cleared successfully.
```

lsdbcheck

The **lsdbcheck** command displays a report that lists the database protection state and error action per database file. In addition, the command lists the device names and DS volumes where the database file is located. Only a person with administrator authority can initiate this command. This command can only be used on an HP-UX 11i (11.11), HP-UX 11i v2 (11.23), HP-UX 11i v3 (11.31), Sun Solaris 10, or Sun Solaris 8 operating systems.



Parameters

Note:

1. You must ensure that the following environment variables are set before you can use the IBM database protection commands:
 - ORACLE_HOME

- ORACLE_SID

2. With large configurations of Oracle database, the **lsdbcheck** command might take long time to complete.

-dev *storage_image_ID* | **-dbext** *dbext_filename* | **-nodev**

(Optional) Specifies the storage image ID or the database extent file.

Notes:

1. If you do not specify the storage image ID, the default value for the *devid* variable in your profile file is used.
2. If you specify the **-dbext** parameter, the value for the **-dev** parameter is ignored.
3. You cannot use the **-dev**, **-dbext**, or **-nodev** parameters together.

The database extent file must exist to use the **-dbext** parameter.

If the database extent file is not specified, the database protection configuration is retrieved from a storage image that is specified by the **-dev** parameter or the *devid* specified in your profile and reapplied to the storage image.

-nodev specifies that the query for a storage image ID be suppressed. Instead a query is done on all database files and a report that lists all the volumes that are associated with the database files is displayed.

Note: The State column of the report displays a state of unknown for each volume if the **-dbext** *dbext_filename* parameter is specified. If the **-dbext** *dbext_filename* parameter is not specified, the State column displays a state of unsupported for each volume.

-dbuser *username/password*

(Required) Specifies the user ID and password that is used to log in to an Oracle instance. The user ID must contain the Oracle SYSDBA authorization; otherwise, the **lsdbcheck** command fails.

Note: When the Oracle database uses Operating System Authentication, either one of the following conditions must be met:

- Make the root user's PRIMARY group the DBA group
- Use the **newgrp** command to change the root user's primary group to the DBA group before running the **lsdbcheck** command.

Every running Oracle database is associated with an Oracle instance. When a database is started on a database server (regardless of the type of computer), Oracle allocates a memory area called the System Global Area (SGA) and starts one or more Oracle processes. This combination of the SGA and the Oracle processes is called an Oracle instance.

-ts *tablespace_name* | **-tsall** | **-redolog** | **-control** | **-hostlv** *host_lvname*
(Optional) Specifies the database files that you want to query.

You can specify only one of these parameters per command use:

-ts *tablespace_name*

Specifies the tablespace that you want to query.

-tsall

Specifies that you want to query all tablespace files.

-redolog

Specifies that you want to query all redo log files.

-control

Specifies that you want to query all control files.

-hostlv *host_lvname*

Specifies that you want to query the designated LVM logical volume.

If none of the previous parameters are specified, all the database files of the Oracle instance specified by the ORACLE_SID environment variable, are processed.

-state | *enabled* | *partially_enabled* | *temporarily_disabled* | *disabled* | *inconsistent* | *unknown* | *unsupported*

(Optional) Specifies that the system display a list of all database files that meet the criteria of the specified database protection state. The criteria for each database protection state are as follows:

enabled

The database file has enabled database protection and there is no inconsistency between the configuration of the database file and database extents that are defined for the database file.

partially_enabled

Some regions of the database file have enabled validation, but other regions have not. The other attributes of the database extents are consistent with the database file.

temporarily_disabled

All the regions of the database file are disabled temporarily from validation.

disabled

Database protection for the database file is disabled. Disabled can also mean that database extents are defined for the database file.

inconsistent

The configuration of the database file does not match the number of database extents set for the database.

unknown

The protection state of the database file cannot be determined from the database extents that are available from the storage image or from a specified database extent definition file.

unsupported

The database file is configured on a non-DS volume, on a filesystem, or on a volume managed by unsupported logical volume manager, or the attributes of the LVM logical volume are unsupported. For additional information about why there is a status of unsupported, view the Reason column of the generated report.

-erraction *rejectio* | *logonly*

(Optional) Specifies that the system display a list of all database files that are set to take the specified action on error. You can specify that the system take one of the following actions:

rejectio

The database server receives an error response from the DS8000 for the request of an irregular write I/O transaction and the corrupted data is not written to disk. The error is also recorded inside the DS8000, and an email notification or an SNMP alert (or both) are sent from the DS8000 hardware management console to the designated computer.

logonly

The database server does not receive an error response from the DS8000 for a request to process an irregular write I/O transaction, and the corrupted data is written to disk. The error is also recorded inside the DS8000, and an email notification or an SNMP alert (or both) are sent from the DS8000 hardware management console to the designated computer.

-s

(Optional) Specifies that the names of the tablespaces, redo log files, and control files be displayed. You cannot use the **-s** and the **-l** parameters together.

-l

(Optional) Specifies that all information that can be generated by the report be displayed. You cannot use the **-l** and the **-s** parameters together.

Example

For this command and all other DS CLI list commands, the results are shown in table format for clarity. The actual reports do not display as tables.

The following examples show how to invoke the **lsdbcheck** command to display the database protection state for all available database files and how to display volumes that are related to a tablespace without retrieving database extents. In each case, the **-l** parameter specifies that a detailed report be displayed.

Invoking the lsdbcheck command to display the database protection state for all available database files

```
dsccli>lsdbcheck -dev IBM.2107-75FA120 -l -dbuser (username/password)
```

The resulting output

Date/Time: Wed Apr 25, 2006 11:45:08 AM JST IBM DSCCLI Version: 5.3.0.0
DS: IBM.2107-75FA120

Name	Filetype	State	ErrAction	Reason	DevName	Volume
TS1	Tablespace	Enabled	Reject I/O	-	/dev/ vg01/ts1	IBM.2107- 7577561 /0901 IBM.2107- 7577561 /0902
TS2	Tablespace	Enabled	Log Only	-	/dev/ vg03/ts2	IBM.2107- 7577561 /0903 IBM.2107- 7577561 /0904
TS3	Tablespace	Unsup- ported	-	File System	/dev/ vg00/lvol4	-
/dev/ vg03/log	Redolog File	Disabled	-	-	/dev/ vg03/log	IBM.2107- 7577561 /0905 IBM.2107- 7577561 /0906

Name	Filetype	State	ErrAction	Reason	DevName	Volume
/dev/vg04/ctrl	Control File	Disabled	-	-	/dev/vg04/ctrl	IBM.2107-7577561/0907 IBM.2107-7577561/0908

Invoking the lsdbcheck command to display the volumes that are related to a tablespace without retrieving database extents

```
dscli>lsdbcheck -nodev -l -dbuser (username/password) -ts TS1
```

The resulting output

Date/Time: Wed Apr 25, 2006 11:45:08 AM JST IBM DSCLI Version: 5.3.0.0
DS: IBM.2107-75FA120

Name	Filetype	State	ErrAction	Reason	DevName	Volume
TS1	Tablespace	Unknown	-	-	/dev/ts1	IBM.2107-7577561/0901 IBM.2107-7577561/0902

Report field definitions

Name Specifies the name of the tablespace, redo log file or control file.

Filetype

Specifies the database file type.

State Specifies the database validation state. One of the following values can be displayed:

enabled

The database file has database protection enabled and there is no inconsistency between the configuration of the database file and database extents defined for the database file.

partially_enabled

Some regions of the database file have enabled validation, but other regions have not. The other attributes of the database extents are consistent with the database file.

temporarily_disabled

All the regions of the database file are disabled temporarily from validation.

disabled

Database protection for the database file is disabled. Disabled can also mean that database extents are defined for the database file.

inconsistent

The configuration of the database file does not match the number of database extents set for the database.

unknown

The protection state of the database file cannot be determined from

the database extents that are available from the storage image or from a specified database extent definition file.

unsupported

The database file is configured on a non-DS volume, on a filesystem, or on a volume managed by unsupported logical volume manager, or the attributes of the LVM logical volume are unsupported. For additional information about why there is a status of unsupported, view the Reason column of the report.

ErrAction

Specifies the error action set for the database file. When a State reason of Enabled, Temporarily Disabled, or Partially Enabled is displayed, one of the following values is specified in this field:

Reject I/O

The database server receives an error response from the DS8000 for the request of an irregular write I/O transaction and the corrupted data is not written to disk. The error is also recorded inside the DS8000, and an email notification or an SNMP alert (or both) are sent from the DS8000 hardware management console to the designated computer.

Log Only

The database server does not receive an error response from the DS8000 for a request to process an irregular write I/O transaction, and the corrupted data is written to disk. The error is also recorded inside the DS8000, and an email notification or an SNMP alert (or both) are sent from the DS8000 hardware management console to the designated computer.

Note: For a given log type ("Reject I/O" or "Log Only"), the system logs the first 2 errors in a 15 minute window, not to exceed a total of 5 errors for the box and that log type in a 2 hour window.

If the State reason is reported as Disabled, Inconsistent, Unsupported, or Unknown, the ErrAction column displays a null (-) value.

Reason

Specifies the reason for a State value of unsupported. If the state value is anything other than unsupported, a null (-) value is displayed in the Reason column.

If the State value is unsupported, one of the following reason values is displayed:

Version

Indicates that the database file is configured with an unsupported version of Oracle database software. The supported database versions are Oracle9i Database Release 2 and Oracle 10g Database Release 2.

Volume

Indicates that the database file is configured on unsupported volumes, and the volumes are not configured for use on a DS8000 model type.

File System

Indicates that the database file is configured on a file system. (A

file system [often also written as filesystem] is a method for storing and organizing computer files and the data they contain to make it easy to find and access them.)

DB BlockSize

Indicates that the block size of database file is not supported. The supported database block size is 512 bytes, 1 KB, 2 KB, 4 KB, 8 KB, 16 KB, or 32 KB.

HostLV Size

Indicates that the database file is configured on a LVM logical volume whose size is less than a minimum size.

PE Size

Indicates the size of allocation unit used by Logical Volume Manager is not a multiple of the database block size.

Stripe Size

Indicates that the database file is located on a LVM logical volume which distributes the data to multiple DS volumes by using the stripe method, and the stripe size is not a multiple of the database block size.

DB File Type

Indicates that the database file type is not supported, and that it is not a tablespace, redo-log file, or a control file.

RAID Type

Indicates that the database file is configured on an unsupported software RAID.

Note: This is not a RAID type for DS volumes.

LE Size

Indicates that the logical extent size of the LVM logical volume where database file is located is unsupported.

No Datafile

Indicates that the tablespace is not associated with any database data file.

Map Error

Indicates that there is a failure to get database mapping information. Check to see if your LVM configuration is supported.

Path Unavailable

Indicates that the database protection state is unknown because of one of the following circumstances:

- All of the host I/O paths used to query one of the volumes on which the database file is located are temporarily unavailable.
- The issuer of the command does not have the authorization to query volume information.

Volume Info unavailable

Indicates that the volume information needed to determine the database protection state of the database file is unavailable from the specified database extent file or from the specified storage image.

DevName

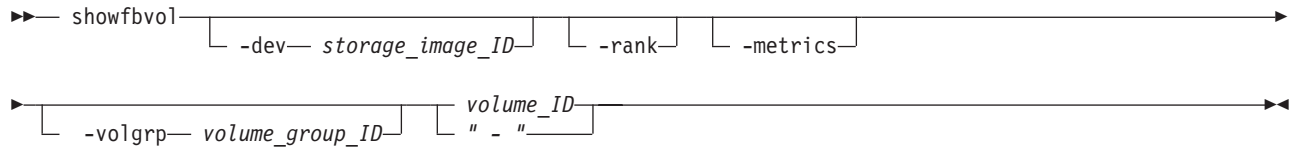
Specifies the local device name where the database file is located.

Volume

Specifies a list of volume IDs that are displayed in fully qualified format.

showfbvol

The **showfbvol** command displays detailed properties for an individual volume. This command can also be used to display the performance metrics of a fixed block volume.



Parameters

-dev *storage_image_ID*

(Optional) Specifies the storage image ID, which consists of manufacturer, machine type, and serial number.

-rank

(Optional) Specifies that a rank extents table is to be displayed. This table displays the set of ranks that the logical volume has extents configured on and the number of extents for that logical volume.

Note: This parameter cannot be used with the **-metrics** or **-volgrp** parameters.

-metrics

(Optional) Displays volume ID and performance metrics for the specified volume.

Notes:

1. All performance counts are an accumulation since the most recent counter wrap or counter reset. Volume performance counters are reset on a power-up sequence. Volume performance counters are reset by a server failover and failback sequence.
2. Do not use this parameter with the **-rank** parameters.

-volgrp *volume_group_ID*

(Required if you do not specify the *volume_ID* parameter.) Specifies that the fixed block volumes that are associated with the designated volume group ID are to be displayed.

Notes:

1. You can only use the **-volgrp** parameter when you are doing a query for performance metrics.
2. Do not use the **-volgrp** parameter with the *volume_ID* parameter.
3. Do not use the **-volgrp** parameter with the **-rank** parameters.

volume_ID | **-**

(Required if you do not specify the **-volgrp** parameter.) Displays information for the specified volume. This parameter accepts a fully qualified volume ID, which consists of the *storage_image_ID* or a shortened version without the

storage image ID, if you specify the **-dev** parameter. The volume ID is a 32 bit number that can be represented as four hexadecimal digits in the form of *XYZZ* where:

X Specifies the address group, 0–F.

XY Specifies the logical subsystem number, 00 - FE.

ZZ Specifies the volume number, 00 - FF.

If you use the dash (-), the specified value is read from standard input. However, you cannot use the dash (-) while you are in the DS CLI interactive command mode.

Note: Do not use the *volume_ID* parameter with the **-volgrp** parameter.

Example

For this command and all other DS CLI show commands, the results are shown in table format to provide clarity. The actual reports do not display as tables.

The following tables represent the headers that are displayed on the output reports that are associated with the **showfbvol** command using the **-rank** parameter. When the rank parameter is specified, a rank extents table is also displayed. It appears at the end of the regular report.

Invoking the showfbvol to show volume properties

Note: The example output is based on using the **showfbvol** command for a 1.0 (Binary) GB volume.

```
dscli> showfbvol
-dev IBM.2107-1300861 -rank 6000
```

The resulting output

Name	ID	acc state	data state	config state	device MTM	data type	addrgrp
My_ volume _6000	6000	Online	Normal	Normal	2107-900	FB 512	6

extpool	exts	captype	cap (2^30B)	cap (10^9B)	cap (blocks)	volgrp	ranks
P0	1	DS	1.0	–	2097152	V2	3

extpool	exts	captype	cap (2^30B)	cap (10^9B)	cap (blocks)	volgrp	ranks	dbexts
P0	1622	DS	1622.0	-	3401580544	-	2	0

sam	repcapalloc	eam	reqcap (blocks)
Standard	-	rotateexts	2097152

realextents	virtualextents	migrating	perfrp	migratingfrom	resgrp
1	0	0	PG0	-	RG0

Rank extents

Rank	Extents
R0	1
R2	2

Report field definitions (*-metrics* parameter not specified)

Name

Specifies the nickname that you assigned for this volume object.

ID Specifies the unique identifier that is assigned to this volume object.

Accstate

One of the following access states are displayed: Online or Fenced.

Online

The logical volume is accessible to a host.

Fenced

The logical volume is in the volume fenced state and is not accessible to the host.

Datastate

One of the following data states are displayed:

Normal

None of the other data states apply. The access state is Online.

Pinned

Specifies that none of the other data states apply and the logical volume has one or more pinned non-retryable tracks. The access state is Online.

Read only

Indicates that the logical volume can be read but not written to because one or more extents on the logical volume are on a rank in the read only data state. The access state is Online.

Inaccessible

Indicates that one or more extents that are associated with the logical volume are on a rank that is in the inaccessible data state. The access state is Fenced.

Virtual space fault

Specifies that the logical volume has a storage allocation method of extent space-efficient or track space-efficient. There was not enough available space to convert a virtual logical track to a real logical track. The access state is Online.

Indeterminate data loss

Specifies that the following data states do not apply and that one of the following conditions has occurred:

Data states that do not apply:

- Rank failed
- Rank repairing
- Rank repaired
- Global inaccessible
- Global lost data

Conditions - one of the following conditions has occurred:

- Committed write data was lost before it was destaged and the track identifiers that are associated with the data are unknown.
- Data was lost that indicated extents on the logical volume were active FlashCopy targets.

The access state is Fenced.

Rank failed

Indicates that one or more extents that are associated with the logical volume are on a rank that is in the Failed data state. The access state is Fenced. This data state changes to Rank repairing if the rank changes to the Rank repairing state through use of the repair array function.

Rank Repairing

Indicates that one or more extents that are associated with the logical volume are on ranks in the repairing data state. The access state is Fenced.

Rank Repaired

Indicates that one or more extents that are associated with the logical volume are on ranks that were in the repairing state, but are not in the repairing state now. The access state is Fenced.

Global inaccessible

Specifies that the global metadata that is associated with the logical volume configuration is inaccessible. Some of the data that is associated with the logical volume might be inaccurate. The access state is Fenced.

Global lost

Specifies that global metadata that is associated with the logical volume configuration has been lost. As a result, some of the data that is associated with the logical volume might be inaccurate. The access state is Fenced.

NVS data inaccessible

Specifies that active nonvolatile storage (NVS) data is inaccessible for one or more logical volumes of an LSS group. The logical volumes in the LSS group cannot be made accessible. The access state is Fenced.

Configstate

One of the following configuration states are displayed:

Normal

Indicates that there are no logical volume configuration operations in progress.

Configuring

Indicates that the logical volume is in the process of being configured for the first time.

Reconfiguring

Indicates that the logical volume is in the process of allocating or deallocating extents due to a modification of the requested capacity attribute after initial creation.

Migrating

Indicates that the logical volume is in the process of performing dynamic volume relocation to a specified extent pool.

Deconfiguring

Indicates that the logical volume is in the process of being deleted.

Configuration error

Indicates that the initial configuration did not complete successfully. This state reflects an internal error condition and not an error in the request to create the volume. If you have a volume in this state, use the **rmfbvol** command to delete each volume listed with the configuration state of "configuration error".

Reconfiguration error

Indicates that the reconfiguration request did not complete successfully.

Migration error

Indicates that the dynamic volume relocation operation was ended during processing.

Deconfiguration error

Indicates that a request to delete a volume did not complete successfully. This state reflects an internal error condition and not an error in the request to remove the volume. To correct this state, you must reissue the **rmfbvol** command for the designated volume.

deviceMTM

Indicates the volume device type and the machine type. The volume MTM is determined by the fixed block volume data type and the volume capacity (in GB). The machine type is either 2107 or 1750; however, the MTM can be any one of the following depending on your system:

2107-900

Indicates a standard 2107 volume.

1750-500

Indicates a standard 1750 volume.

xxxx-A0x

The *xxxx* is 2107 or 1750; the A0 indicates a System i protected volume (for example, 2107-A01 or 1750-A07).

xxxx-A8x

The *xxxx* is 2107 or 1750; the A8 indicates a System i unprotected volume (for example, 2107-A81 or 1750-A87).

Datatype

Indicates the volume data type setting. One of the following values is displayed:

- FB 512
- FB 520P
- FB 520U

Addrgrp

Specifies the address group that contains the designated volume object. An address group ID is one hexadecimal character (0 - F).

Extpool

Specifies the extent pool ID. Volume extents are allocated from this extent pool ID.

Exts

Specifies the number of real and virtual extents used by the designated volume ID.

Capttype

Indicates capacity unit type used at volume creation. One of the following values is displayed:

ESS

The capacity unit is 10^9 B.

DS The capacity unit is 2^{30} B.

DS/ESS

The capacity unit is 2^{30} B or 10^9 B.

Blocks

The capacity unit 512 B.

iSeries

The capacity unit was not specified at volume creation. This fixed block volume was created for iSeries.

Cap (2³⁰B)

Specifies the size of volume that is available for host system access in 2^{30} B (binary GB) unit.

Note: "-" (null) is displayed if the capacity unit type of the volume is ESS (captype=ESS)

Cap (10⁹B)

Specifies the size of volume that is available for host system access in 10^9 B (decimal GB) unit.

Note: "-" (null) is displayed if the capacity unit type of the volume is DS (captype=DS)

Cap blocks

Indicates the quantity of volume logical blocks that are available for host system access.

Volgrp

Specifies the volume groups (excluding default volume groups) that a volume belongs to.

Multiple volume groups that are associated with the volume are separated by a comma.

A null (-) is displayed if there are no volume groups that are associated with the volume.

Unknown is displayed if information about the volume groups is not available.

Ranks

Specifies the number of ranks that the volume resides on.

dbexts

Specifies the number of database extents associated with the specified volume in the storage unit. If the specified volume is not 512 B fix block volume, a null (-) value is displayed.

SAM

Specifies the storage allocation method. The following values are displayed:

standard

Designates that the system fully allocated the volume with real extents at volume creation time. An inquiry on a DS6000 model always reports this value.

tse

Designates that a track space-efficient logical volume contains a set of virtual extents that are associated with the space-efficient storage in the same extent pool. Physical space for a given logical track on a track

space-efficient logical volume is dynamically allocated and deallocated from the repository in the space-efficient storage.

ese Designates that an extent space efficient logical volume is provisioned with a set of virtual extents that are associated with the space efficient storage in the same extent pool. Physical space for an extent space efficient logical volume is dynamically allocated and deallocated from the extent pool.

Note: IBM Database protection feature supports standard volumes only.

Repcapalloc

Specifies the allocated physical repository capacity of the track space-efficient storage. This value is calculated on the available repository capacity as a result of writes to the track space-efficient volume. This value is displayed in the format of X.Y, where X is whole GB (1 GB = 2³⁰ B) and Y represents tenths of a GB, which is limited to a single digit (0 - 9).

Note:

1. A null (-) value is displayed in this column if the value displayed in the SAM column is not TSE.
2. A null (-) value is displayed for the DS6000.

EAM

Specifies the extent allocation method that is to be used if the volume is migrated or expanded. One of the following values is displayed:

legacy Designates that the volume was created before the use of the current algorithm. **Legacy** is always the reported value for a DS6000 model.

rotateexts

Specifies that the extents for each new logical volume are allocated across all available ranks, and is also known as storage-pool striping. This value is the default.

rotatevols

Specifies that the extents for each new logical volume are allocated from each successive rank. This means that the extents for a particular volume will be allocated from one rank, while the extents for the next volume will be allocated from the next successive rank, and so on.

managed

Specifies that the extents are currently managed by Easy Tier, and the extents for any new volumes are initially allocated across all available ranks in the lowest tier of storage.

- (null)

A null (-) value is displayed if the extent allocation method does not apply, for example, track space-efficient logical volumes.

Reqcap (blocks)

Specifies the requested quantity of volume logical block (for example, 3339).

Note: A value of 0 is displayed for the DS6000.

real extents

Specifies the number of real extents used by the logical volume.

virtual extents

Specifies the number of virtual extents used by the logical volume.

migrating

The number of extents for this volume that are currently being migrated.

migratingfrom

A list of one or more extent pool IDs where the extents are migrating from. If there are no migrating extents, a dash "-" is displayed. Unknown is displayed if information about the extent pool IDs is not available.

perfgrp

Specifies the performance group ID that the volume is assigned to. The performance group ID begins with the letters *PG* and ends with a decimal number.

resgrp

Specifies the resource group ID that the volume is assigned to. The resource group ID begins with the letters *RG* and ends with a decimal number.

Report field definitions (-rank parameter specified)

Rank (Rank Extent table)

Specifies the rank ID.

Extents (Rank Extents table)

Specifies the number of extents for the volume on the rank.

Example

For this command and all other DS CLI show commands, the results are shown in table format to provide clarity. The actual reports do not display as tables.

The following tables represent the headers that are displayed on the output reports that are associated with the **showfbvol** command using the **-metrics** parameter.

Invoking the showfbvol to show performance metrics

```
dscli> showfbvol -metrics IBM.2107-75FA120/0101
```

The resulting output

ID	Date	norm rdrqts	norm rdhits	norm write req	norm write hits	seq read reqs	seq read hits	seq write req
IBM. 2107- 75FA120 /0101	10/11 /04 02:23:49	10000	10000	10000	10000	10000	10000	10000

seqwrite- hits	cachfwr- reqs	cachfwr- hits	cachfw- reqs	cachfw- hits	inbcach- load	bypass- cach	seq DASD trans
10000	10000	10000	10000	10000	10000	10000	10000

DASD- trans	cache- trans	NVS- spadel	norm write ops	seqwrite- ops	rec cache mis	qwrite- prots	CKDir- trkac
10000	10000	10000	10000	10000	10000	10000	0

CKD irtrk hits	cachsp- delay	timelow- ifact	phread	phwrite	phwrite	phbyte- read	phbyte- writ
0	10000	10000	10000	10000	10000	10000	10000

recmo- reads	sfile trk reads	contam- wrts	PPRC- trks	NVS- spallo	time- phread	timeph- write	byte- read
10000	0	0	10000	10000	10000	10000	10000

bytewrit	timeread	timewrite	zHPFRead	zHPFWrite
10000	10000	10000	-	-

zHPFPrefetchReq	zHPFPrefetchHit	GMCollisions- SidefileCount	GMCollisions- SendSyncCount
0	0	0	0

Report field definitions (*-metrics* parameter specified)

ID Specifies the unique identifier that is assigned to this volume object.

Date

Specifies the current time stamp for the volume performance counters.

normrdrqts

Specifies Search/Read Normal I/O Requests.

normrdhits

Specifies Search/Read Normal I/O Requests instances.

normwritereq

Specifies Write Normal I/O Requests.

normwritehits

Specifies DASD Fast Write I/O Request instances.

seqreadreqs

Specifies Search/Read Sequential I/O Requests.

seqreadhits

Specifies Search/Read Sequential I/O Request instances.

seqwritereq

Specifies Write Sequential I/O Requests.

seqwritehits

Specifies DASD Fast Write Sequential I/O Request instances.

cachfwrreqs

Specifies Search/Read Cache Fast Write I/O Requests.

cachfwrhits

Specifies Search/Read Cache Fast Write I/O Request instances.

cachfwreqs

Specifies Cache Fast Write I/O Requests.

cachfwhits

Specifies Cache Fast Write I/O Requests instances.

inbcachload
Specifies Inhibit Cache Loading I/O Requests that operate with DASD.

bypasscach
Specifies Bypass Cache I/O Requests.

seqDASDtrans
Specifies Sequential DASD to Cache Transfer Operations.

DASDtrans
Specifies DASD to Cache Transfer Operation Count.

cachetrans
Specifies Cache to DASD Transfer Operation Count.

NVSspadel
Specifies DASD Fast Write Operations Delayed Due to nonvolatile storage Space Constraints.

normwriteops
Specifies Normal 'DASD Fast Write' Write Operation Counts.

seqwriteops
Specifies Sequential Access 'DASD Fast Write' Write Operation Counts.

reccachemis
Specifies Number of record cache Read Misses.

qwriteprots
Specifies Quick Write Promotes.

CKDirtrkac
Specifies Irregular Track Accesses. A 0 (zero) value is displayed for a fixed block volume.

CKDirtrkhits
Specifies Irregular Track Accesses instances. A 0 (zero) value is displayed for a fixed block volume.

cachspdelay
Specifies Operations Delayed Due To Cache Space Constraints.

timelowifact
Specifies Milliseconds of lower interface I/O activity for the indicated device.

phread
Specifies Physical Storage Read Operations.

phwrite
Specifies Physical Storage Write Operations.

phbyteread
Specifies Physical Storage Bytes Read in 128 KB increments.

phbytewrit
Specifies Physical Storage Bytes Written in 128 KB increments.

recmoreads
Specifies Record Mode Read Operations.

sfiletrkreads
Specifies the Number of tracks read from the Concurrent Copy or XRC Sidefile. A 0 (zero) value is displayed for a fixed block volume.

contamwrts

Specifies the Number of Contaminating writes for a Concurrent Copy or XRC volume. A 0 (zero) value is displayed for a fixed block volume.

PPRCtrks

Specifies the Number of tracks or portion of tracks that were transferred to the secondary device of a PPRC pair.

NVSspallo

Specifies the NVS Space Allocations.

timephread

Specifies the Physical Storage Read Response Time in 16 ms increments.

timephwrite

Specifies the Physical Storage Write Response Time in 16 ms increments.

byteread

Specifies the number of Bytes read in 128 KB increments.

bytewrit

Specifies the number of Bytes written in 128 KB increments.

timeread

Specifies the accumulated response time for all read operations.

timewrite

Specifies the accumulated response time for all write operations.

zHPFRead

Specifies the HPF Read I/O Requests for volume performance statistics.

zHPFWrite

Specifies the HPF Write I/O Requests for volume performance statistics.

zHPFPrefetchReq

Specifies the number of HPF Pre-fetch I/O requests.

zHPFPrefetchHit

Specifies the number of HPF Pre-fetch I/O request hits.

GMCollisionsSidefileCount

Specifies the number of Global Mirror Collisions sidefile.

GMCollisionsSendSyncCount

Specifies the number of Global Mirror Collisions Send Synchronous Count.

applykey

The **applykey** command applies the licensed machine code (LMC) activation keys for a storage server.

You can enter the LMC keys manually, or you can import the keys from an XML file. The file that contains the LMC keys must be downloaded from an IBM website.

```

▶▶ applykey [-key key [...]] [-file file_name] [" - " storage_image_ID]

```

-key *key* [...]

This parameter is required if the **-file** parameter is not specified.

-file *file_name*

This parameter is required if the **-key** parameter is not specified.

```
storage_image_ID | -
```

If you use the dash (-), the specified value is read from standard input.

Example

```
dsccli> applykey -file keys.xml IBM.2107-75FA120
```

Iskey

The **lskey** command only displays the keys that are installed. Refer to the *IBM System Storage DS8000 Introduction and Planning Guide* for more information on how to choose which keys are needed and how to acquire them.



Parameters

(Required) Specifies the storage image ID for which to view a list of activated features. The ID includes manufacturer, type, and serial number.

If you use the dash (-), the specified value is read from standard input.

However, you cannot use the dash (-) if you are using the DS CLI interactive command mode.

Example

The following table shows example activation keys. Some activation keys are not listed in the example. The **lskey** command displays only the keys that are installed.

An invocation example

```
dscli> lskey IBM.2107-75FA120
```

The resulting output

Activation key	Authorization level (TB)	Scope
Parallel access volumes (PAV)	On	CKD
Point in time copy (PTC)	On	All
Global Mirror (GM), (not available for DS6000 models)	25	All
HyperPAV (not available for DS6000 models)	On	CKD
Metro/Global Mirror (MGM),	25	All
Metro Mirror (MM), (not available for DS6000 models)	25	All
Remote mirror and copy (RMC)	25	All
Remote mirror for z/OS (RMZ)	25.1	CKD
Operating Environment (OEL)	45	All
IBM database protection (not available for DS6000 models)	On	FB
IBM FlashCopy SE (not available for DS6000 models)	25	All

Report field definitions

Activation key

Specifies the type of LMC activation key that is activated for the storage image.

Authorization Level (TB)

Specifies the capacity of the specified license feature. The quantity is displayed in terabytes (TB). One of the following values is displayed:

- Value in terabytes
- **On** if the license is for the maximum capacity, or **Off** if the license is for zero capacity

Scope Specifies the storage type for the designated license: fixed block (FB), count key data (CKD), or All. Parallel access volumes, Remote Mirror for z/OS, and HyperPAV display only the values CKD or All.

Chapter 4. IBM Database Protection system generated messages

When you use the DS CLI commands that are associated with the IBM Database Protection feature and the management console, messages are generated regarding the application processes, status, and errors.

The user interface and the supporting software issue three types of messages:

Informational messages

These messages are identified by the letter *I* at the end of the message identifier. They provide information about system activities as they take place. For instance, an informational message might report that a volume was successfully created. No user action is necessary.

Warning messages

These messages are identified by the letter *W* at the end of the message identifier. They warn that user-activated activities might have consequences that you do not anticipate. Warning messages normally provide you the opportunity to continue an activity or to cancel it.

Error messages

These messages are identified by the letter *E* at the end of the message identifier. They indicate that an error has occurred. See the explanations and recommended that are actions associated with the messages in the Messages book to resolve a problem.

The messages that are associated with the IBM Database Protection feature begin with the number CMUC00268E and flow sequentially to the last associated message number. See the IBM System Storage DS8000 Information Center for the messages details.

Notices

The information provided by this media supports the products and services described with consideration for the conditions described herein.

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 give you any license to these patents. You can send license inquiries to:

*IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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 measurement 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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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.

Trademarks

This topic lists trademarks that appear in this information.

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 by going to the Copyright and trademark information website.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Electronic emission notices

This section contains the electronic emission notices or statements for the United States and other countries.

Federal Communications Commission statement

This explains the Federal Communications Commission's (FCC) statement.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device might not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

European Union Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of European Union (EU) Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Responsible Manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European community contact:

IBM Technical Regulations, Department M456
IBM-Allee 1, 71137 Ehningen, Germany
Tel: +49 7032 15-2937
E-mail: tjahn@de.ibm.com

Germany Electromagnetic compatibility directive

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)." Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland
Technical Regulations, Department M456

IBM-Allee 1, 71137 Ehningen, Germany
Tel: +49 7032 15-2937
e-mail: tjahn@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

**Japanese Voluntary Control Council for Interference (VCCI)
class A statement**

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用する
と電波妨害を引き起こすことがあります。この場合には使用者が適切な対策
を講ずるよう要求されることがあります。 VCCI-A

Translation:

This is a Class A product based on the standard of the VCCI Council. If this
equipment is used in a domestic environment, radio interference may occur, in
which case, the user may be required to take corrective actions.

**Japanese Electronics and Information Technology Industries
Association (JEITA) statement**

Japanese Electronics and Information Technology Industries Association (JEITA)
Confirmed Harmonics Guideline (products less than or equal to 20 A per phase)

高調波ガイドライン適合品

Japanese Electronics and Information Technology Industries Association (JEITA)
Confirmed Harmonics Guideline with Modifications (products greater than 20 A per phase)

高調波ガイドライン準用品

**Korea Communications Commission (KCC) Electromagnetic
Interference (EMI) Statement**

이 기기는 업무용(A급)으로 전자파적합기기로서
판매자 또는 사용자는 이 점을 주의하시기
바라며, 가정외의 지역에서 사용하는 것을 목
적으로 합니다.

12c01252

Russia Electromagnetic Interference (EMI) Class A Statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

rusemi

Taiwan Class A compliance statement

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

tailemi

Taiwan contact information

This topic contains the product service contact information for Taiwan.

IBM Taiwan Product Service Contact Information:
IBM Taiwan Corporation
3F, No 7, Song Ren Rd., Taipei Taiwan
Tel: 0800-016-888

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

f2c00790

Index

A

applydbcheck 31

C

commands

- applydbcheck 31
- lsdbcheck 36
- managedbcheck 34
- offloadbcheck 32
- setdbcheck 28
- showfbvol 43

E

eam (extent allocation method)
showfbvol 43

I

IBM Database protection

- environments 3
- overview 1

IBM Database Protection

- adding data block validation 13
- adding database block validation to
 - all database files 16
- changing error reporting 14
- clearing database extent
 - configuration 23
- clearing extent configuration 25
- disabling for DS volumes 21
- disabling for volume groups 23
- enabling for DS volumes 22
- enabling for volume group 24
- extend tablespace - database data
 - file 18, 20
- messages 57
- operational limitations 4
- removing from all database files 17
- removing the database block
 - validation 13
- reporting methods 14
- setup 8

L

logonly 14
lsdbcheck 36

M

managedbcheck 34
managing data block validation

- adding to all database files 16
- adding to single tablespace 13
- changing error reporting 14

managing data block validation

(*continued*)

- clearing database extent
 - configuration 23
- clearing extent configuration 25
- disabling for DS volumes 21
- disabling for volume groups 23
- enabling for DS volumes 22
- enabling for volume group 24
- extend tablespace - database data
 - file 18, 20
- overview 11
- removing from all database files 17
- removing from single tablespace 13

O

offloadbcheck 32

R

rejectio 14

S

setdbcheck 28
showfbvol 43

- eam (extent allocation method) 43
- tse 43

T

Trademarks 60
tse

- showfbvol 43

Readers' comments — we would like to hear from you

IBM System Storage
IBM System Storage DS8000 IBM Database Protection
User's Guide
Version 1 Release 3

Publication No. GC27-2133-02

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Send your comments to the address on the reverse side of this form.

If you would like a response from IBM, please fill in the following information:

Name

Address

Company or Organization

Phone No.

Email address



Cut or Fold
Along Line

Fold and Tape

Please do not staple

Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Information Development
Department 61C
9032 South Rita Road
Tucson, AZ 85775-4401



Fold and Tape

Please do not staple

Fold and Tape

Cut or Fold
Along Line



Printed in USA

GC27-2133-02

