IBM Tivoli Storage Manager for Databases
Version 6.3

Data Protection for Oracle for UNIX and Linux Installation and User's Guide

SC27-4019-00

IBM Tivoli Storage Manager for Databases
Version 6.3

Data Protection for Oracle for UNIX and Linux Installation and User's Guide

SC27-4019-00

Note:
Before using this information and the product it supports, read the information in "Notices" on page 63.

This edition applies to Version 6.3 of IBM Tivoli Storage Manager for Databases: Data Protection for Oracle for AIX, Linux, HP-UX, or Solaris (product number 5608-E04) and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters.

© Copyright IBM Corporation 1998, 2011.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Tables v

Preface vii
About this publication vii
Who should read this publication vii
Publications vii
Tivoli Storage Manager publications viii
Tivoli Storage FlashCopy Manager publications. . x
Support information x
Getting technical training xi
Searching knowledge bases xi
Contacting IBM Software Support xiii
What to do when you encounter a problem . . . xv
Conventions used in this book xvii
Typeface conventions xvii
Reading syntax diagrams xvii

New for Data Protection for Oracle Version 6.3 xxi

Chapter 1. Data Protection for Oracle overview 1
Tivoli Storage Manager overview 1
Overview of Data Protection for Oracle 2
RMAN and Data Protection for Oracle. 2
LAN-free data transfer 3
Migration and coexistence 3

Chapter 2. Installing 5
Installing Data Protection for Oracle 5
Installation prerequisites 5
Installing Data Protection for Oracle on AIX 64-bit 8
Installing Data Protection for Oracle on 64-bit HP-UX Itanium 10
Installing Data Protection for Oracle on Linux x86 12
Installing Data Protection for Oracle on Linux x86_64 13
Installing Data Protection for Oracle on Linux zSeries 64-bit 15
Installing Data Protection for Oracle on 64-bit Solaris SPARC 17

Chapter 3. Configuring Data Protection for Oracle 21
Quick configuration with default settings 21
Configuring Data Protection for Oracle 23
1. Define Data Protection for Oracle options in the tdpo.opt file 23
2. Register the Data Protection for Oracle node to a Tivoli Storage Manager server 26
3. Define Tivoli Storage Manager options in the client options file 27
4. Define Tivoli Storage Manager policy requirements 32
5. Initialize the password with a Tivoli Storage Manager server 33

Chapter 4. Protecting Oracle Server data 35
Using RMAN and Data Protection for Oracle . . . 35
Invoking RMAN. 35
Scripts 36
Using the Duplex Copy function 38
Removing old backups 40
Using the Tivoli Storage Manager scheduler with Data Protection for Oracle 40
Example: setting up a schedule 41
Querying backup objects 44
Using data deduplication with Data Protection for Oracle 44
Overview of data deduplication 44
Setting up Data Protection for Oracle for client-side data deduplication 45
Determining total data reduction 46

Chapter 5. Data Protection for Oracle reference. 49
Data Protection for Oracle utilities. 49
Command line syntax and characteristics . . . 49
TDPOCONF 50
TDPOSYNC 52

Appendix. Accessibility features for the Tivoli Storage Manager product family . 61

Notices 63
Trademarks 65

Glossary 67

Index 89

© Copyright IBM Corp. 1998, 2011

Tables

1. Tivoli Storage Manager server publications viii
2. Tivoli Storage Manager storage agent publications viii
3. Tivoli Storage Manager client publications ix
4. Tivoli Storage Manager data protection publications ix
5. IBM Tivoli Storage Manager troubleshooting and tuning publications ix
6. Tivoli Storage FlashCopy Manager publications x
7. AIX 64-bit Default Installation Directories 8
8. Data Protection for Oracle AIX 64-bit, Utilities, Languages, and Tivoli Storage Manager API Package Names 8
9. HP-UX Itanium 64-bit Default Installation Directories 10
10. Data Protection for Oracle 64-bit and Tivoli Storage Manager installable files and packages. 10
11. Linux x86 Default Installation Directories 12
12. Data Protection for Oracle Linux x86 and Tivoli Storage Manager installable files and packages 12
13. Linux x86_64 Default Installation Directories 13
14. Data Protection for Oracle Linux x86_64 and Tivoli Storage Manager installable files and packages 14
15. Linux zSeries (64-bit environment) Default Installation Directories 15
16. Data Protection for Oracle Linux zSeries (64-bit environment) and Tivoli Storage Manager installable files and packages. 16
17. Solaris SPARC 64-bit Default Installation Directories 17
18. Data Protection for Oracle 64-bit and Tivoli Storage Manager installable files and packages. 18

© Copyright IBM Corp. 1998, 2011

Preface

The subject of this publication is Data Protection for Oracle, a component of the IBM® Tivoli® Storage Manager for Databases product.

About this publication

This publication contains information about installing, configuring, administering, and using IBM Tivoli Storage Manager for Databases: Data Protection for Oracle.

Data Protection for Oracle performs online or offline backups of Oracle 11g databases to Tivoli Storage Manager storage. This integration with the RMAN Media Management API maximizes the protection of data, thus providing a comprehensive storage management solution.

Tivoli Storage Manager is a client-server licensed product that provides storage management services in a multiplatform computer environment.

Who should read this publication

The target audience for this publication includes system installers, system users, Oracle database administrators, Tivoli Storage Manager administrators, and system administrators.

In this book, it is assumed that you have an understanding of the following applications:

- Oracle server
- Tivoli Storage Manager server
- Tivoli Storage Manager backup-archive client
- Tivoli Storage Manager application programming interface

It is also assumed that you have an understanding of the following operating systems:

- AIX®
- HP-UX
- Linux
- Solaris Operating Environment (referred to as Solaris throughout this document)

Publications

Publications for the IBM Tivoli Storage Manager family of products are available online. The IBM Tivoli Storage Manager product family includes IBM Tivoli Storage FlashCopy® Manager, IBM Tivoli Storage Manager for Space Management, IBM Tivoli Storage Manager for Databases, and several other storage management products from IBM Tivoli.

To search all publications, go to the Tivoli Storage Manager information center at http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3.

© Copyright IBM Corp. 1998, 2011

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

Go to Tivoli Documentation Central to find information centers that contain official product documentation for current and previous versions of Tivoli products, including the Tivoli Storage Manager product family. You can find Tivoli Documentation Central at https://www.ibm.com/developerworks/wikis/display/tivolidoccentral/Home.

You can also order some related publications from the IBM Publications Center website. The website provides information about ordering publications from countries other than the United States. In the United States, you can order publications by calling 1-800-879-2755.

Tivoli Storage Manager publications

The following tables list the publications that make up the Tivoli Storage Manager library.

Table 1. Tivoli Storage Manager server publications

Publication title	Order number
IBM Tivoli Storage Manager for AIX Installation Guide	GC23-9781
IBM Tivoli Storage Manager for AIX Administrator's Guide	SC23-9769
IBM Tivoli Storage Manager for AIX Administrator's Reference	SC23-9775
IBM Tivoli Storage Manager for HP-UX Installation Guide	GC23-9782
IBM Tivoli Storage Manager for HP-UX Administrator's Guide	SC23-9770
IBM Tivoli Storage Manager for HP-UX Administrator's Reference	SC23-9776
IBM Tivoli Storage Manager for Linux Installation Guide	GC23-9783
IBM Tivoli Storage Manager for Linux Administrator's Guide	SC23-9771
IBM Tivoli Storage Manager for Linux Administrator's Reference	SC23-9777
IBM Tivoli Storage Manager for Oracle Solaris Installation Guide	GC23-9784
IBM Tivoli Storage Manager for Oracle Solaris Administrator's Guide	SC23-9772
IBM Tivoli Storage Manager for Oracle Solaris Administrator's Reference	SC23-9778
IBM Tivoli Storage Manager for Windows Installation Guide	GC23-9785
IBM Tivoli Storage Manager for Windows Administrator's Guide	SC23-9773
IBM Tivoli Storage Manager for Windows Administrator's Reference	SC23-9779
IBM Tivoli Storage Manager for z/OS Media Installation and User's Guide	SC27-4018
IBM Tivoli Storage Manager Upgrade and Migration Guide for V5 Servers	GC27-4017
IBM Tivoli Storage Manager Integration Guide for Tivoli Storage Manager FastBack®	SC27-2828

Table 2. Tivoli Storage Manager storage agent publications

Publication title	Order number
IBM Tivoli Storage Manager for SAN for AIX Storage Agent User's Guide	SC23-9797

Table 2. Tivoli Storage Manager storage agent publications (continued)

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

Table 3. Tivoli Storage Manager client publications

Publication title	Order number
IBM Tivoli Storage Manager for UNIX and Linux: Backup-Archive Clients Installation and User's Guide	SC23-9791
IBM Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and User's Guide	SC23-9792
IBM Tivoli Storage Manager Using the Application Programming Interface	SC23-9793
IBM Tivoli Storage Manager for Space Management for UNIX and Linux: User's Guide	SC23-9794
IBM Tivoli Storage Manager HSM for Windows Administration Guide	SC23-9795

Table 4. Tivoli Storage Manager data protection publications

Publication title	Order number
IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Installation and User's Guide	GC27-4010
IBM Tivoli Storage Manager for Databases: Data Protection for Oracle for UNIX and Linux Installation and User's Guide	SC27-4019
IBM Tivoli Storage Manager for Databases: Data Protection for Oracle for Windows Installation and User's Guide	SC27-4020
IBM Tivoli Storage Manager for Mail: Data Protection for Microsoft Exchange Server Installation and User's Guide	GC27-4009
IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino® UNIX and Linux Installation and User's Guide	SC27-4021
IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino for Windows Installation and User's Guide	SC27-4022
IBM Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP Installation and User's Guide for DB2	SC33-6341
IBM Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP Installation and User's Guide for Oracle	SC33-6340
IBM Tivoli Storage Manager for Virtual Environments Installation and User's Guide	SC27-2898
IBM Tivoli Storage Manager for Microsoft SharePoint Guide	N/A

Table 5. IBM Tivoli Storage Manager troubleshooting and tuning publications

Publication title	Order number
IBM Tivoli Storage Manager Problem Determination Guide	GC23-9789

Table 5. IBM Tivoli Storage Manager troubleshooting and tuning publications (continued)

Publication title	Order number
IBM Tivoli Storage Manager Performance Tuning Guide	GC23-9788
IBM Tivoli Storage Manager Client Messages and Application Programming Interface Return Codes	SC27-2878
IBM Tivoli Storage Manager Server Messages and Error Codes	SC27-2877
IBM Tivoli Storage Manager for Mail: Data Protection for Microsoft Exchange Server Messages	GC27-4011
IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Messages	GC27-4012
IBM Tivoli Storage Manager for Databases: Data Protection for Oracle Messages	SC27-4014
IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino Messages	SC27-4015
IBM Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP Messages	SC27-4016

Note: You can find information about IBM System Storage® Archive Manager at http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3/c_complydataretention_ovr.html.

Tivoli Storage FlashCopy Manager publications

The following table lists the publications that make up the Tivoli Storage FlashCopy Manager library.

Table 6. Tivoli Storage FlashCopy Manager publications

Publication title	Order number
IBM Tivoli Storage FlashCopy Manager for UNIX and Linux Installation and User's Guide	SC27-4005
IBM Tivoli Storage FlashCopy Manager for Windows Installation and User's Guide	SC27-4006
IBM Tivoli Storage FlashCopy Manager for VMware Installation and User's Guide	SC27-4007
IBM Tivoli Storage FlashCopy Manager Messages	GC27-4008

Support information

You can find support information for IBM products from various sources.

Start at the IBM Support Portal: http://www.ibm.com/support/entry/portal/. You can select the products that you are interested in and search for a wide variety of relevant information.

Getting technical training

Information about Tivoli technical training courses is available online.

Go to the following websites to sign up for training, ask questions, and interact with others who use IBM storage products.

Tivoli software training and certification
Choose from instructor led, online classroom training, self-paced Web classes, Tivoli certification preparation, and other training options at http://www.ibm.com/software/tivoli/education/

Tivoli Support Technical Exchange
Technical experts share their knowledge and answer your questions in webcasts at http://www.ibm.com/software/sysmgmt/products/support/supp_tech_exch.html.

Storage Management community
Interact with others who use IBM storage management products at http://www.ibm.com/developerworks/servicemanagement/sm/index.html

Global Tivoli User Community
Share information and learn from other Tivoli users throughout the world at http://www.tivoli-ug.org/.

IBM Education Assistant
View short "how to" recordings designed to help you use IBM software products more effectively at http://publib.boulder.ibm.com/infocenter/ieduasst/tivv1r0/index.jsp

Searching knowledge bases

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

Begin by searching the Tivoli Storage Manager Information Center at http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3. From this website, you can search the current Tivoli Storage Manager documentation.

Searching the Internet

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

To search multiple Internet resources, go to the IBM support website at http://www.ibm.com/support/entry/portal/.

You can search for information without signing in. Sign in using your IBM ID and password if you want to customize the site based on your product usage and information needs. If you do not already have an IBM ID and password, click **Sign in** at the top of the page and follow the instructions to register.

From the support website, you can search various resources including:

- IBM technotes
- IBM downloads
- IBM Redbooks® publications
- IBM Authorized Program Analysis Reports (APARs)

Select the product and click **Downloads** to search the APAR list.

If you still cannot find a solution to the problem, you can search forums and newsgroups on the Internet for the latest information that might help you find problem resolution.

An independent user discussion list, ADSM-L, is hosted by Marist College. You can subscribe by sending an email to listserv@vm.marist.edu. The body of the message must contain the following text: `SUBSCRIBE ADSM-L` *your_first_name your_family_name*.

To share your experiences and learn from others in the Tivoli Storage Manager and Tivoli Storage FlashCopy Manager user communities, go to the following wikis:

Tivoli Storage Manager wiki
http://www.ibm.com/developerworks/wikis/display/tivolistoragemanager

Tivoli Storage FlashCopy Manager wiki
https://www.ibm.com/developerworks/mydeveloperworks/wikis/home/wiki/Tivoli Storage FlashCopy Manager

Using IBM Support Assistant

IBM Support Assistant is a complimentary software product that can help you with problem determination. It is available for some Tivoli Storage Manager and Tivoli Storage FlashCopy Manager products.

To learn about which products are supported, go to the IBM Support Assistant download web page at http://www.ibm.com/software/support/isa/download.html.

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

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

You can find more information at the IBM Support Assistant website:

http://www.ibm.com/software/support/isa/

You can also install the stand-alone IBM Support Assistant application on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products that you use. Find add-ons for specific products at http://www.ibm.com/support/docview.wss?uid=swg27012689.

Finding product fixes

A product fix to resolve your problem might be available from the IBM software support website.

You can determine what fixes are available by checking the IBM software support website at http://www.ibm.com/support/entry/portal/.

- If you previously customized the site based on your product usage:
  1. Click the link for your product, or a component for which you want to find a fix.
  2. Click **Downloads**, and then click **Fixes by version**.
- If you have not customized the site based on your product usage, click **Downloads** and search for your product.

Receiving notification of product fixes

You can receive notifications about fixes, flashes, upgrades, and other news about IBM products.

To sign up to receive notifications about IBM products, follow these steps:

1. From the support page at http://www.ibm.com/support/entry/portal/, click **Sign in to create, manage, or view your subscriptions** in the **Notifications** pane.
2. Sign in using your IBM ID and password. If you do not have an ID and password, click **register now** and complete the registration process.
3. Click **Manage all my subscriptions** in the **Notifications** pane.
4. Click the **Subscribe** tab and then click **Tivoli**.
5. Select the products for which you want to receive notifications and click **Continue**.
6. Specify your notification preferences and click **Submit**.

Contacting IBM Software Support

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

To obtain help from IBM Software Support, complete the following steps:

1. Ensure that you have completed the following prerequisites:
   a. Set up a subscription and support contract.
   b. Determine the business impact of your problem.
   c. Describe your problem and gather background information.
2. Follow the instructions in “Submitting the problem to IBM Software Support” on page xv.

Setting up a subscription and support contract

Set up a subscription and support contract. The type of contract that you need depends on the type of product you have.

For IBM distributed software products (including, but not limited to, IBM Tivoli, Lotus®, and Rational® products, as well as IBM DB2® and IBM WebSphere® products that run on Microsoft Windows or on operating systems such as AIX or Linux), enroll in IBM Passport Advantage® in one of the following ways:

- **Online:** Go to the Passport Advantage website at http://www.ibm.com/software/lotus/passportadvantage/, click **How to enroll**, and follow the instructions.
- **By telephone:** You can call 1-800-IBMSERV (1-800-426-7378) in the United States. For the telephone number to call in your country, go to the IBM Software Support Handbook web page at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html and click **Contacts**.

Determining the business impact

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

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

Describing the problem and gathering background information

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

To save time, know the answers to these questions:

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

Submitting the problem to IBM Software Support

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

Online

Go to the IBM Software Support website at http://www.ibm.com/support/entry/portal/Open_service_request/Software/Software_support_(general). Sign in to access IBM Service Requests and enter your information into the problem submission tool.

By telephone

For the telephone number to call in your country, go to the IBM Software Support Handbook at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html and click **Contacts**.

What to do when you encounter a problem

If you encounter a problem while using Data Protection for Oracle or if you cannot start Data Protection for Oracle, do the following:

1. Run the **tdpoconf showenvironment** command to collect information on your options file (*–TDPO_OPTFILE=*) and specified output files (*–outfile=*).
2. If the above command ran successfully, check its output to see if the setup worked as expected.
3. If the above command failed, check the tdpoerror.log and dsierror.log files. The tdpoerror.log is a log file created in the installation directory by default. The dsierror.log is generated by the Tivoli Storage Manager API when a problem occurs with the Tivoli Storage Manager API setup.
4. Fix the problem and run the **tdpoconf** utility again.
5. Verify that the Oracle target database instance is symbolically linked with :
   a. Log in as the Oracle user.
   b. Run the following command:

   ```
   $ ls -al $ORACLE_HOME/lib/libobk.a
   ```

   Look for the *libobk* link(s) in the system's respective 32-bit or 64-bit library directory.
   c. Verify that the link points to a file that exists. For example:

   ```
   $ORACLE_HOME/lib/libobk.a -> /opt/tivoli/tsm/client/oracle/bin64/libobk64.a
   ```

   or

   ```
   $ORACLE_HOME/lib/libobk.so -> /usr/lib/sparcV9/libobk.so
   /usr/lib/sparcV9/libobk.so -> /opt/tivoli/tsm/client/oracle/bin64/libobk64.so
   ```

   Make sure that the final link destination is the correct bit level and points to a file that exists.
6. If the problem persists, gather the following information:
   - A problem description file that includes the command you used and the session output you received when the problem occurred.
   - The tdpo.opt file specified by ***TDPO_OPTFILE*** variable in the RMAN script
   - The dsm.opt file specified by ***dsmi_orc_config*** in the tdpo.opt file
   - The dsm.sys file
   - The Data Protection for Oracle error log file (tdpoerror.log) in the following location (listed from highest to lowest precedence):

- The value of the Tivoli Storage Manager API ***errorlogname*** option specified in the dsm.sys file.
- The value of the DSMI_LOG environment variable.

  Make sure DSMI_LOG (specified in the tdpo.opt file) specifies a directory with Read/Write permissions for the Oracle user. By default, the DSMI_LOG environment variable specifies a directory owned by root.
- If a failure occurs during option processing for the initialization, the tdpoerror.log file may be located in $ORACLE_HOME/bin.

- The Tivoli Storage Manager API error log file (dsierror.log) in the following location (listed from highest to lowest precedence):
  - The value of the Tivoli Storage Manager API ***errorlogname*** option specified in the dsm.sys file. Make sure ***errorlogname*** specifies a directory and file name with Read/Write permissions for the Oracle user.
  - The value of the DSMI_LOG environment variable.
- The RMAN log file
- The Tivoli Storage Manager API trace file

  To generate the Tivoli Storage Manager API trace file, add the following lines in your dsm.opt file:

  ```
  tracefile /home/oracle/rman/tsmapi.out
  traceflag service
  ```
- The node information on the Tivoli Storage Manager server. To obtain this information, enter:

  ```
  query node <nodename> format=detail
  ```
- The Tivoli Storage Manager server activity log. To obtain this information, enter this Tivoli Storage Manager administrator command:

  ```
  query actlog
  ```

  Note that this command provides one previous hour of activity. Since the activity log should be obtained for the time period immediately prior to the failed operation until a few moments after the failed operation, you can specify the following settings to obtain activity for the exact time of failure:

  ```
  query actlog begindate=MM/DD/YYYY begintime=HH:MM:SS
  ```
- The Data Protection for Oracle trace file

  To generate the Data Protection for Oracle trace file, add the following lines in your tdpo.opt file:

  ```
  tdpo_trace_flags orclevel0 orclevel1 orclevel2
  tdpo_trace_file /home/oracle/rman/tdpo.out
  ```

  where:

  orclevel0
  Traces out function exit points when errors occur.

  orclevel1
  Traces out normal function entry and exit points.

  orclevel2
  Traces out more detailed information.

  Note: Any path and file name can be specified for the ***tdpo_trace_file*** and ***tracefile*** options. However, the directory must exist and have writable rights.

Conventions used in this book

This guide uses several conventions for special terms and actions, operating system-dependent commands and paths.

Typeface conventions

This guide uses the following typeface conventions:

bold

- Commands, keywords, authorization roles, or other information that you must use.
- Example: Use the **query** command to query the Tivoli Storage Manager server for information about objects that have been backed up.

italics

- Values or variables that you must provide.
- Emphasized words and phrases.
- Example: The node name of the *production node* and *backup node* must not be the same.

bold italics

- Options and parameters.
- Example: Specify the value for the ***compression*** option.

monospace

- Directories, parameters, URLs, and output examples.
- Example: The product is installed in the `/usr/tivoli/tsm/client/ba/bin` directory.

UPPERCASE

- Environment variables associated with Tivoli Storage Manager, operating systems, or Oracle Server.
- Example: Make sure the DSM_DIR environment variable is set correctly.

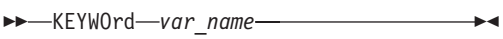
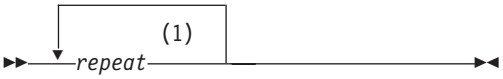
Reading syntax diagrams

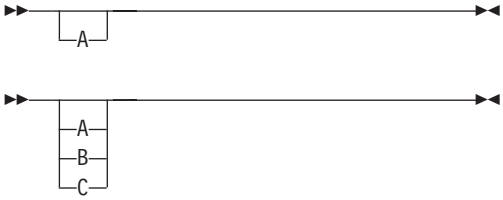
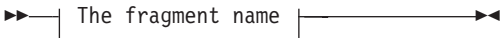
This section describes how to read the syntax diagrams used in this book. To read a syntax diagram, follow the path of the line. Read from left to right, and top to bottom.

- The ►►— symbol indicates the beginning of a syntax diagram.
- The —► symbol at the end of a line indicates the syntax diagram continues on the next line.
- The ►— symbol at the beginning of a line indicates a syntax diagram continues from the previous line.
- The —►◄ symbol indicates the end of a syntax diagram.

Syntax items, such as a keyword or variable, can be:

- On the line (required element)
- Above the line (default element)
- Below the line (optional element).

Syntax Diagram Description	Example
Abbreviations: Uppercase letters denote the shortest acceptable truncation. If an item appears entirely in uppercase letters, it cannot be truncated. You can type the item in any combination of uppercase or lowercase letters. In this example, you can enter KEYWO, KEYWORD, or KEYWOrd.	
Symbols: Enter these symbols exactly as they appear in the syntax diagram.	* Asterisk { } Braces : Colon , Comma = Equal Sign - Hyphen () Parentheses . Period Space
Variables: Italicized lowercase items (*var_name*) denote variables. In this example, you can specify a *var_name* when you enter the KEYWORD command.	
Repetition: An arrow returning to the left means you can repeat the item. A character or space within the arrow means you must separate repeated items with that character or space. A footnote by the arrow references the number of times you can repeat the item.	  **Notes:** 1 Specify *repeat* as many as 5 times.
Required Choices: When two or more items are in a stack and one of them is on the line, you *must* specify one item. In this example, you *must* choose A, B, or C.	

Syntax Diagram Description	Example
Optional Choice: When an item is below the line, that item is optional. In the first example, you can choose A or nothing at all. When two or more items are in a stack below the line, all of them are optional. In the second example, you can choose A, B, C, or nothing at all.	
Defaults: Defaults are above the line. The default is selected unless you override it. You can override the default by including an option from the stack below the line. In this example, A is the default. You can override A by choosing B or C. You can also specify the default explicitly.	
Repeatable Choices: A stack of items followed by an arrow returning to the left means you can select more than one item or, in some cases, repeat a single item. In this example, you can choose any combination of A, B, or C.	
Syntax Fragments: Some diagrams, because of their length, must fragment the syntax. The fragment name appears between vertical bars in the diagram. The expanded fragment appears between vertical bars in the diagram after a heading with the same fragment name.	 **The fragment name:**

New for Data Protection for Oracle Version 6.3

Read about the new features and other changes to IBM Tivoli Storage Manager for Databases: Data Protection for Oracle Version 6.3.

The following features are new for Data Protection for Oracle in Version 6.3:

A new `query` command is available to query information about backed up files
With the **`tdposync query`** command, you can query the Tivoli Storage Manager server for information about database objects that have been backed up. You can obtain statistics that indicate whether a backup object was encrypted, compressed, or deduplicated.

The `tdposync` utility can work with backup history information in the Oracle control file
The **`tdposync syncdb`** command can use the backup history information stored in the Oracle control file to synchronize the Tivoli Storage Manager database with the Oracle Recovery Manager (RMAN) backup history. Synchronization can be done with either a control file or the Oracle catalog.

Use the `send` command to send additional parameters to the Tivoli Storage Manager API
You can use the Oracle RMAN **`send`** command in an RMAN script to specify any supported Tivoli Storage Manager options, such as TCPport and TCPServeraddress, to the Tivoli Storage Manager API. Any option that is sent by using the **`send`** command takes precedence over the option specified in the options files for Data Protection for Oracle or Tivoli Storage Manager API.

UTF-8 is added for the language locales that are already supported by Data Protection for Oracle
The Data Protection for Oracle Version 6.3 message catalogs are encoded in UTF-8. If you are installing the Data Protection for Oracle message catalogs for languages other than English, you must also have the appropriate **`iconv`** UTF-8 converters installed on your system. If the appropriate **`iconv`** UTF-8 converters are not installed, all Data Protection for Oracle messages are displayed in English.

Related tasks

"Querying backup objects" on page 44

"Using the **`send`** command" on page 36

Related reference

"**`Query`** command" on page 57

"TDPOSYNC" on page 52

"**`Syncdb`** command" on page 54

© Copyright IBM Corp. 1998, 2011

Chapter 1. Data Protection for Oracle overview

A brief overview of IBM Tivoli Storage Manager and IBM IBM Tivoli Storage Manager for Databases: Data Protection for Oracle is provided.

Tivoli Storage Manager overview

Tivoli Storage Manager is a client/server program that provides storage management services in a multi-vendor, multi-platform computer environment.

Tivoli Storage Manager provides these functions:

- Reduces network complexity

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

  Tivoli Storage Manager can reduce the cost of network administration by allowing administrators to perform these actions:
  - Automate repetitive processes
  - Schedule unattended processes
  - Administer Tivoli Storage Manager from anywhere in the network
- Reduces the risk of data loss

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

  Tivoli Storage Manager allows users to move files from client file systems to Tivoli Storage Manager storage. This saves space on client file systems and can eliminate the expense of upgrading client storage hardware.

  Tivoli Storage Manager monitors client storage space and moves files from client file systems to Tivoli Storage Manager storage if an out-of-space condition threatens. This function can also eliminate the expense of client hardware upgrades.

Tivoli Storage Manager provides these services:

- Backup and restore services

  These services generate backup copies of data at specified intervals and restores the data from these copies when required. These services protect against workstation or file server media failure, accidental file deletion, data corruption, data vandalism, or site disasters.
- Archive and retrieve services

  These services provide backup-archive clients with point-in-time copies of data for long-term storage.
- Server hierarchical storage management services

© Copyright IBM Corp. 1998, 2011

These services migrate client files from expensive storage media to less expensive storage media (from disk to tape, for example). Administrator-defined thresholds determine file migration for each storage pool. Migration applies to all backup and archive client files.

- Automation services

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

- Administration services

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

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

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

- Security services

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

- Disaster recovery management

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

Overview of Data Protection for Oracle

Data Protection for Oracle interfaces with the Oracle Recovery Manager (RMAN) to send backup versions of Oracle databases to the Tivoli Storage Manager server.

Data Protection for Oracle currently supports Oracle 11g databases with the Oracle Recovery Manager. See Chapter 2, “Installing,” on page 5 for specific levels of supported Oracle databases.

RMAN and Data Protection for Oracle

Oracle Recovery Manager (RMAN) provides consistent and secure backup, restore, and recovery performance for Oracle databases. While the Oracle RMAN initiates a backup or restore, Data Protection for Oracle acts as the interface to the Tivoli Storage Manager server . The Tivoli Storage Manager server then applies administrator-defined storage management policies to the data. Data Protection for Oracle implements the Oracle defined Media Management application program interface (SBTAPI) 2.0. This SBTAPI interfaces with RMAN and translates Oracle commands into Tivoli Storage Manager API calls to the Tivoli Storage Manager server.

With the use of RMAN, Data Protection for Oracle allows you to perform the following functions:

- Full and incremental backup function for the following while online or offline:
  - Databases
  - Tablespaces
  - Datafiles
  - Archive log files
  - Control files
- Full database restores while offline
- Tablespace and datafile restore while online or offline

LAN-free data transfer

Data Protection for Oracle supports backup and restore operations in a LAN-free environment. This environment shifts the movement of data from the communications network to a storage area network (SAN). Data moves over the SAN to a SAN-attached storage device by the Tivoli Storage Manager Storage Agent. Running Data Protection for Oracle in a LAN-free environment avoids constraints of the network and decreases the load on the Tivoli Storage Manager server, allowing the server to support a greater number of simultaneous connections.

Before enabling LAN-free support, you must install the Tivoli Storage Manager Managed System for SAN Storage Agent on the same system as Data Protection for Oracle. See the *IBM Tivoli Storage Manager for SAN* for your operating environment for more information about LAN-free requirements.

Migration and coexistence

- Existing backups created using previous versions of Data Protection for Oracle are restorable using Data Protection for Oracle 6.3.
- Backups created with Data Protection for Oracle 6.3 cannot be restored using previous versions of Data Protection for Oracle.

Related tasks

Chapter 3, “Configuring Data Protection for Oracle,” on page 21

“Scripts” on page 36

Chapter 2. Installing

Install IBM Tivoli Storage Manager for Databases: Data Protection for Oracle to protect your Oracle server databases.

Installing Data Protection for Oracle

Verify installation prerequisites and follow the instructions to install Data Protection for Oracle for UNIX and Linux.

Hardware, software, and operating system requirements must be met before attempting to install Data Protection for Oracle.

Installation prerequisites

Before you install Data Protection for Oracle, ensure that your system meets the minimum hardware, software, and operating system requirements.

The following sections provide an overview of the minimum hardware and software requirements for the V6.3 release of Data Protection for Oracle. Additional details and functional requirements are available in the Hardware and Software Requirements technote that is associated with this release.

Details of the hardware and software requirements for Data Protection for Oracle can evolve over time due to maintenance updates and the addition of operating system, application, and other software currency support.

For the most current requirements, review the Hardware and Software Requirements technote that is associated with your level of your Data Protection for Oracle program. This technote is available in the All Requirement Documents website at http://www.ibm.com/support/docview.wss?uid=swg21218747. When you are at the website, follow the link to the requirements technote for your specific release or update level.

Minimum hardware requirements

You must meet the minimum hardware requirements for operating Data Protection for Oracle in a UNIX or Linux environment.

Hardware requirements for AIX

Use the following types of hardware for the AIX platform:

- IBM System p®
- IBM System i®
- Hardware that is compatible with the operating system and the application

Hardware requirements for HP-UX

Use HP Integrity Server (Itanium) or compatible hardware that is supported by the operating system and the application.

© Copyright IBM Corp. 1998, 2011

Hardware requirements for Linux on x86

Use a 32-bit x86-based PC architecture that is supported by the operating system and the application.

Hardware requirements for Linux on x86_64

Use the following types of hardware for the Linux x86_64 platforms:

- An X86 based PC architecture (such as Pentium) or later
- An AMD64/EM64T architecture that is compatible with the operating system and the application

Hardware requirements for Linux on System z®

Use Any System z system that is supported by the operating system and the application.

Hardware requirements for Solaris SPARC

Use Sun-4 SPARC or compatible hardware supported by the operating system and the application.

Minimum software and operating system requirements

You must meet the minimum software requirements for operating Data Protection for Oracle in a UNIX or Linux environment.

Operating system requirements for AIX

Use the following operating systems on the AIX platform:

- 64-bit AIX 6.1, and later mod levels and fix packs
- 64-bit AIX 7.1, and later mod levels and fix packs

Operating system requirements for HP-UX

Use the following operating system on the HP-UX platform:

64-bit HP 11iv3, and later mod levels and fix packs

Operating system requirements for Linux on x86

Use the following operating systems on Linux on x86 platform:

- 32-bit Red Hat Enterprise Linux (RHEL) 5.0, and later mod levels and fix packs
- 32-bit Red Hat Enterprise Linux (RHEL) 6.0, and later mod levels and fix packs
- 32-bit SUSE Enterprise Linux (SLES) 10.0, and later mod levels and fix packs
- 32-bit SUSE Enterprise Linux (SLES) 11.0, and later mod levels and fix packs
- 32-bit Asianux 3.0, and later mod levels and fix packs

Operating system requirements for Linux on x86_64

Use the following operating systems on the Linux on x86_64 platform:

- 64-bit Red Hat Enterprise Linux (RHEL) 5.0, and later mod levels and fix packs
- 64-bit Red Hat Enterprise Linux (RHEL) 6.0, and later mod levels and fix packs
- 64-bit SUSE Enterprise Linux (SLES) 10.0, and later mod levels and fix packs
- 64-bit SUSE Enterprise Linux (SLES) 11.0, and later mod levels and fix packs

- Asianux 3.0, and later mod levels and fix packs

Operating system requirements for Linux on System z

Use the following operating systems on the Linux on System z platform:
- 64-bit Red Hat Enterprise Linux (RHEL) 5.0, and later mod levels and fix packs
- 64-bit Red Hat Enterprise Linux (RHEL) 6.0, and later mod levels and fix packs
- 64-bit SUSE Enterprise Linux (SLES) 10.0, and later mod levels and fix packs
- 64-bit SUSE Enterprise Linux (SLES) 11.0, and later mod levels and fix packs

Operating system requirements for Solaris SPARC

Use the following operating system on the Solaris SPARC platform: 64-bit Solaris 10, and later mod levels and fix packs.

Oracle Database levels

The following Oracle Database levels are supported:
- 32-bit Oracle Database 11gR1: Standard or Enterprise editions
- 32-bit Oracle Database 11gR2: Standard or Enterprise editions
- 64-bit Oracle Database 11gR1: Standard or Enterprise editions
- 64-bit Oracle Database 11gR2: Standard or Enterprise editions

Oracle Database environments

The following Oracle Database environments are supported:
- 32-bit Oracle Real Application Clusters 11gR1
- 32-bit Oracle Real Application Clusters 11gR2
- 64-bit Oracle Real Application Clusters 11gR1
- 64-bit Oracle Real Application Clusters 11gR2

Java levels

Use the following Oracle Java™ levels on the HP-UX, Solaris, and Linux platforms:
- Java JRE 6, and later mod levels and fix packs
- Java JRE 7, and later mod levels and fix packs

Tivoli Storage Manager server and API requirements

The following Tivoli Storage Manager server and API versions are required for Data Protection for Oracle:
- Any Tivoli Storage Manager server in support that is compatible with the Tivoli Storage Manager API used in your environment
- One of the following Tivoli Storage Manager API versions:
  - For Linux x86, Tivoli Storage Manager API Version 6.2.2, and later mod levels and fix packs
  - For all other UNIX and Linux platforms, either of the following Tivoli Storage Manager API versions:
    - Tivoli Storage Manager API Version 6.2.2, and later mod levels and fix packs

- Tivoli Storage Manager API Version 6.3.0, and later mod levels and fix packs

Tivoli Storage Manager communication methods

Use the following communication methods for AIX, HP-UX Itanium, and Solaris SPARC:

- TCP/IP
- Shared memory

  Data Protection for Oracle and the Tivoli Storage Manager server must be installed on the same machine in order for shared memory to work.

Use TCP/IP as the following communication method for Linux on x86, Linux x86_64 and Linux on System z:

Virtualization support

Information regarding the virtualization environments that are compatible with Data Protection for Oracle is available at: http://www.ibm.com/support/docview.wss?uid=swg21239546.

Installing Data Protection for Oracle on AIX 64-bit

Use these instructions to install Data Protection for Oracle on an AIX 64-bit operating system.

Before you begin, you must uninstall any previous version of Data Protection for Oracle, or the Tivoli Storage Manager API, before installing a new or updated version. If you are installing a fix pack or interim fix version of Data Protection for Oracle, do not remove the license enablement file from the previous version. The fix pack and interim fix drivers do not contain a license enablement file.

All installable files on the CD reside under the `/usr/sys/inst.images` directory.

Table 7. AIX 64-bit Default Installation Directories

AIX	Default Installation Directories
Data Protection for Oracle 64-bit	/usr/tivoli/tsm/client/oracle/bin64
Data Protection for Oracle Utilities	/usr/tivoli/tsm/client/oracle/bin64
Tivoli Storage Manager API 64-bit	/usr/tivoli/tsm/client/api/bin64

Table 8. Data Protection for Oracle AIX 64-bit, Utilities, Languages, and Tivoli Storage Manager API Package Names

Package	Package Name
Data Protection for Oracle 64-bit	tivoli.tsm.client.oracle.aix.64bit
Data Protection for Oracle Utilities	tivoli.tsm.client.oracle.tools.aix.64bit
Electronic License Agreement	tivoli.tsm.loc.client.oracle.aix.64bit.ela
Data Protection for Oracle Languages	tivoli.tsm.client.oracle.msg.aix.64bit.*xx_XX*

Table 8. Data Protection for Oracle AIX 64-bit, Utilities, Languages, and Tivoli Storage Manager API Package Names (continued)

Package	Package Name
Tivoli Storage Manager API 64-bit	tivoli.tsm.client.api.aix.64bit
Tivoli Storage Manager API Languages	tivoli.tsm.client.msg.*XX_XX*

Follow these instructions to install Data Protection for Oracle. This example assumes that your CD drive is `/dev/cd0`.

1. Insert the CD containing the client package into the CD drive.
2. Log in as the *root* user.
3. Enter `smitty install` at the command prompt.
4. Select **Install and Update Software**. Press **Enter**.
5. Select **Install and Update from ALL Available Software**. Press **Enter**.
6. Enter `/dev/cd0` in the entry field for **INPUT device / directory for software**. Press **Enter**.
7. Highlight the **SOFTWARE to install** option. Press **F4** to list available software.
8. Select the installable packages by performing the following:
   a. Highlight the Data Protection for Oracle package (`tivoli.tsm.client.oracle.aix.64bit`) and press **F7**.
   b. Highlight the Data Protection for Oracle utilities package (`tivoli.tsm.client.oracle.tools.aix.64bit`) and press **F7**.
   c. Highlight the Tivoli Storage Manager API package (`tivoli.tsm.client.api.aix.64bit`) and press **F7**.
   d. If you want to install Data Protection for Oracle in a language other than English, highlight the desired language package (`tivoli.tsm.client.oracle.msg.aix.64bit.`*`xx_XX`*) and press **F7**. Make sure the Tivoli Storage Manager API language package for the desired language (`tivoli.tsm.client.msg.`*`XX_XX`*) is also installed.
   e. Highlight the Electronic License Agreement (`tivoli.tsm.loc.client.oracle.aix.64bit.ela`) and press **F7**.
      1) Make sure you set **ACCEPT new license agreements?** to **Yes**. (The default is **No**). You can also specify the *-Y* option with the **installp** command.
      2) Set **Preview new license agreements?** to **No** (the default value) for the installation to proceed.
      3) If **Preview new license agreements?** is set to **Yes**, the installation will enter preview mode but Data Protection for Oracle does not install. **Preview new license agreements?** must be set to **No** for Data Protection for Oracle to install.

   After all five packages are selected, press **Enter**.
9. When the **Install and Update from LATEST Available Software** window displays, press **Enter**.
10. A window displays and prompts you with this message:

```
ARE YOU SURE?
```

    Press **Enter** to continue the installation procedure.

11. After successfully installing Data Protection for Oracle, press **F10** to exit the **smitty install** environment. You can view the **Summary** for more information regarding the installation.

Installing Data Protection for Oracle on 64-bit HP-UX Itanium

Use these instructions to install Data Protection for Oracle on the 64-bit version of HP-UX Itanium.

Before you begin, you must uninstall any previous version of Data Protection for Oracle, or the Tivoli Storage Manager API, before installing a new or updated version. If you are installing a fix pack or interim fix version of Data Protection for Oracle, do not remove the license enablement file from the previous version. The fix pack and interim fix drivers do not contain a license enablement file.

All installable files reside under the `/cdrom/oracle/hpuxia/` directory.

Table 9. HP-UX Itanium 64-bit Default Installation Directories

HP-UX	Default Installation Directories
Data Protection for Oracle 64-bit	/opt/tivoli/tsm/client/oracle/bin64
Data Protection for Oracle Utilities	/opt/tivoli/tsm/client/oracle/bin64
Data Protection for Oracle Messages	/opt/tivoli/tsm/client/oracle/bin64
Tivoli Storage Manager API	/opt/tivoli/tsm/client/api/bin64

Table 10. Data Protection for Oracle 64-bit and Tivoli Storage Manager installable files and packages

Component	Installable file or package
Data Protection for Oracle 64-bit base code, license, utilities	TDPOracle64.bin
Data Protection for Oracle Languages	TDPOracle64.msg.*xx_XX*.bin
Tivoli Storage Manager API	TIVsmCapi64
Tivoli Storage Manager API Languages	TIVsmC.msg.*xx_XX*

To install Data Protection for Oracle:

1. Log in as the *root* user:

```
# su
Password:
```

   Enter your password.

2. Create a directory for mounting the CD. Set the appropriate permission to the directory:

```
# mkdir /cdrom
# chmod 755 /cdrom
```

3. Insert the CD into the drive and mount the CD:

```
# mount -r -F hsfs <device_name> /cdrom
```

Enter the device name for the CD in this command. An example of `device_name` is `/dev/dsk/c1t2d0`.

4. Issue this command to install the Tivoli Storage Manager API:

```
$ swinstall -v -s /cdrom/oracle/hpuxia/api/TIVsmCapi64
```

he Tivoli Storage Manager API default language is English. To install additional languages (optional), issue this command for the desired language:

```
$ swinstall -v -s /cdrom/oracle/hpuxia/api/TIVsmC.msg.xx_XX
```

Note: `xx_XX` represents the country code for the language contents of the package.

5. Change to the `/cdrom/oracle/hpuxia` directory where the Data Protection for Oracle installable file resides on the CD:

```
$ cd /cdrom/oracle/hpuxia
```

6. Enter the name of the installable file (`TDPOracle64.bin`) on the command line and press **Enter** to install the Data Protection for Oracle product, utilities, and license:

```
$ TDPOracle64.bin
```

To install in console mode, enter the following command and press **Enter**:

```
$ TDPOracle64.bin -i console
```

To install in silent mode, enter the following command and press **Enter**:

```
$ TDPOracle64.bin -i silent
```

To install in GUI mode, enter the following command and press **Enter**:

```
$ TDPOracle64.bin -i gui
```

If the installable file was downloaded from the FTP site, the filename might be different than `TDPOracle64.bin`.

7. If you want to install Data Protection for Oracle in a language other than English, enter the name of the Data Protection for Oracle installable file for the desired language (`TDPOracle.msg.xx_XX.bin`) on the command line and press **Enter**:

```
$ TDPOracle.msg.xx_XX.bin
```

Make sure the Tivoli Storage Manager API language package for the desired language (`TIVsmC.msg.xx_XX`) is also installed.

Installing Data Protection for Oracle on Linux x86

Use these instructions to install Data Protection for Oracle on a Linux x86 operating system.

Before you begin, you must uninstall any previous version of Data Protection for Oracle, or the Tivoli Storage Manager API, before installing a new or updated version. If you are installing a fix pack or interim fix version of Data Protection for Oracle, do not remove the license enablement file from the previous version. The fix pack and interim fix drivers do not contain a license enablement file.

All installable files reside under the `/cdrom/oracle/linux86/` directory.

Table 11. Linux x86 Default Installation Directories

Linux	Default Installation Directories
Data Protection for Oracle 32-bit	/opt/tivoli/tsm/client/oracle/bin
Data Protection for Oracle Utilities	/opt/tivoli/tsm/client/oracle/bin
Data Protection for Oracle Messages	/opt/tivoli/tsm/client/oracle/bin
Tivoli Storage Manager API 32-bit	/opt/tivoli/tsm/client/api/bin

Table 12. Data Protection for Oracle Linux x86 and Tivoli Storage Manager installable files and packages

Component	Installable file or package
Data Protection for Oracle 32-bit base code, license, and utilities	TDP-Oracle.i386.bin
Data Protection for Oracle Languages	TDPOracle.msg.*xx_XX*.bin
Tivoli Storage Manager API 32-bit	TIVsm-API.i386.rpm
Tivoli Storage Manager API Languages	TIVsm-.msg.*xx_XX*.i386.rpm

The following installation procedure is designed to install directly from the Data Protection for Oracle CD:

1. Log in as the *root* user.
2. Mount the Data Protection for Oracle CD to `/cdrom`:

```
$ mount <device name> /cdrom
```

3. Change to the `<cdrom>/oracle/linux86/api` directory where the Tivoli Storage Manager API installation package resides on the CD:

```
$ cd <cdrom>/oracle/linux86/api
```

4. Issue the following command to install the Tivoli Storage Manager API:

```
$ rpm -i TIVsm-API.i386.rpm
```

   The Tivoli Storage Manager API default language is English. To install additional languages (optional), issue this command for the desired language:

```
$ rpm -i TIVsm-.msg.xx_XX.i386.rpm
```

Note: xx_XX represents the country code for the language contents of the package.

5. Change to the <*cdrom*>/oracle/linux86 directory where the Data Protection for Oracle installable file resides on the CD:

```
$ cd <cdrom>/oracle/linux86
```

6. Enter the name of the installable file (TDP-Oracle.i386.bin) on the command line and press **Enter** to install Data Protection for Oracle:

```
$ TDP-Oracle.i386.bin
```

   To install in console mode, enter the following command and press **Enter**:

```
$ TDP-Oracle.i386.bin -i console
```

   To install in silent mode, enter the following command and press **Enter**:

```
$ TDP-Oracle.i386.bin -i silent
```

   To install in GUI mode, enter the following command and press **Enter**:

```
$ TDP-Oracle.i386.bin -i gui
```

   If the installable file was downloaded from the FTP site, the filename might be different than TDP-Oracle.i386.bin.

7. If you want to install Data Protection for Oracle in a language other than English, enter the name of the Data Protection for Oracle installable file for the desired language (TDPOracle.msg.*xx_XX*.bin) on the command line and press **Enter**:

```
$ TDPOracle.msg.xx_XX.bin
```

   Make sure the Tivoli Storage Manager API language package for the desired language (TIVsm-.msg.*xx_XX*.i386.rpm) is also installed. Note that the libobk.so library file is located automatically based on the link that the installation program places in the /usr/lib directory.

Installing Data Protection for Oracle on Linux x86_64

Use these instructions to install Data Protection for Oracle on Linux x86_64 operating systems.

Before you begin, you must uninstall any previous version of Data Protection for Oracle, or the Tivoli Storage Manager API, before installing a new or updated version. If you are installing a fix pack or interim fix version of Data Protection for Oracle, do not remove the license enablement file from the previous version. The fix pack and interim fix drivers do not contain a license enablement file.

All installable files reside under the /cdrom/oracle/linux86_64 directory.

Table 13. Linux x86_64 Default Installation Directories

Linux	Default Installation Directories
Data Protection for Oracle Linux x86_64	/opt/tivoli/tsm/client/oracle/bin64

Table 13. Linux x86_64 Default Installation Directories (continued)

Linux	Default Installation Directories
Data Protection for Oracle Utilities	/opt/tivoli/tsm/client/oracle/bin64
Data Protection for Oracle Messages	/opt/tivoli/tsm/client/oracle/bin64
Tivoli Storage Manager API	/opt/tivoli/tsm/client/api/bin64

Table 14. Data Protection for Oracle Linux x86_64 and Tivoli Storage Manager installable files and packages

Component	Installable file or package
Data Protection for Oracle Linux x86_64 base code, license, utilities	TDP-Oracle.x86_64.bin
Data Protection for Oracle Languages	TDPOracle.msg.*xx_XX*.x86_64.bin
Tivoli Storage Manager API Linux x86_64	TIVsm-API64.i386.rpm
Tivoli Storage Manager API Languages	TIVsm-msg.*xx_XX*.i386.rpm

The following installation procedure is designed to install directly from the Data Protection for Oracle CD:

1. Log in as the *root* user on the machine with the accessible CD device.
2. Mount the Data Protection for Oracle CD to `/cdrom`:

   ```
   $ mount <device name> /cdrom
   ```

3. Mount `/cdrom` to the `/cdrom` directory on the Linux zSeries® machine. The `/cdrom` directory must already exist on the Linux zSeries machine:

   ```
   $ mount -o soft hostname:/cdrom /cdrom
   ```

   Note: *hostname* is the machine with the accessible CD device identified in Step 1.
4. Change to the `<cdrom>/oracle/linux86_64/api` directory where the installation package resides on the CD:

   ```
   $ cd <cdrom>/oracle/linux86_64/api
   ```

5. Issue the following command to install the Tivoli Storage Manager API:

   ```
   $ rpm -i TIVsm-API64.x86_64.rpm
   ```

   The Tivoli Storage Manager API default language is English. To install additional languages (optional), issue this command for the desired language:

   ```
   $ rpm -i TIVsm-msg.xx_XX.i386.rpm
   ```

   Note: `xx_XX` represents the country code for the language contents of the package.
6. Change to the `<cdrom>/oracle/linux86_64` directory where the Data Protection for Oracle installable file resides on the CD:

```
$ cd <cdrom>/oracle/linux86_64
```

Note: *<cdrom>* is the drive where the CD is mounted.

7. Enter the name of the installable file (`TDP-Oracle.x86_64.bin`) on the command line and press **Enter** to install Data Protection for Oracle:

   ```
   $ TDP-Oracle.x86_64.bin
   ```

   To install in console mode, enter the following command and press **Enter**:

   ```
   $ TDP-Oracle.x86_64.bin -i console
   ```

   To install in silent mode, enter the following command and press **Enter**:

   ```
   $ TDP-Oracle.x86_64.bin -i silent
   ```

   To install in GUI mode, enter the following command and press **Enter**:

   ```
   $ TDP-Oracle.x86_64.bin -i gui
   ```

   If the installable file was downloaded from the FTP site, the filename might be different from `TDP-Oracle.x86_64.bin`.

8. If you want to install Data Protection for Oracle in a language other than English, enter the name of the Data Protection for Oracle installable file for the desired language (`TDPOracle.msg.xx_XX.bin`) on the command line and press **Enter**:

   ```
   $ TDPOracle.msg.xx_XX.x86_64.bin
   ```

   Make sure the Tivoli Storage Manager API language package for the desired language (`TIVsm-msg.xx_XX.x86_64.rpm`) is also installed.

Note: The libobk.so library file is located automatically based on the link that the installation program places in the `/usr/lib64` directory.

Installing Data Protection for Oracle on Linux zSeries 64-bit

Use these instructions to install Data Protection for Oracle on Linux z-Series 64-bit operating systems.

Before you begin, you must uninstall any previous version of Data Protection for Oracle, or the Tivoli Storage Manager API, before installing a new or updated version. If you are installing a fix pack or interim fix version of Data Protection for Oracle, do not remove the license enablement file from the previous version. The fix pack and interim fix drivers do not contain a license enablement file.

All installable files reside under the `/cdrom/oracle/linuxz64` directory.

Table 15. Linux zSeries (64-bit environment) Default Installation Directories

Linux	Default Installation Directories
Data Protection for Oracle Linux zSeries	/opt/tivoli/tsm/client/oracle/bin64
Data Protection for Oracle Utilities	/opt/tivoli/tsm/client/oracle/bin64

Table 15. Linux zSeries (64-bit environment) Default Installation Directories (continued)

Linux	Default Installation Directories
Data Protection for Oracle Messages	/opt/tivoli/tsm/client/oracle/bin64
Tivoli Storage Manager API	/opt/tivoli/tsm/client/api/bin64

Table 16. Data Protection for Oracle Linux zSeries (64-bit environment) and Tivoli Storage Manager installable files and packages

Component	Installable file or package
Data Protection for Oracle Linux zSeries base code, license, utilities	TDP-Oracle.s390x.bin
Data Protection for Oracle Languages	TDP-Oracle.msg.*xx_XX*.s390x.bin
Tivoli Storage Manager API Linux zSeries	TIVsm-API64.s390.rpm, or TIVsm-API64.s390x.rpm (for V6.3 API)
Tivoli Storage Manager Languages	TIVsm-msg.*xx_XX*.s390x.rpm

This installation procedure is designed to install directly from the Data Protection for Oracle CD:

1. Log in as the *root* user on the machine with the accessible CD device.
2. Mount the Data Protection for Oracle CD to `/cdrom`:

   ```
   $ mount <device name> /cdrom
   ```

3. Mount `/cdrom` to the `/cdrom` directory on the Linux machine. The `/cdrom` directory must already exist on the Linux machine:

   ```
   $ mount -o soft hostname:/cdrom /cdrom
   ```

   Note: *hostname* is the machine with the accessible CD device identified in Step 1.
4. Change to the `<cdrom>/oracle/linuxz64/api` directory where the Tivoli Storage Manager API installation package resides on the CD:

   ```
   $ cd <cdrom>/oracle/linuxz64/api
   ```

5. Issue the following command to install the Tivoli Storage Manager API:

   ```
   $ rpm -i TIVsm-API.s390x.rpm
   ```

   The Tivoli Storage Manager API default language is English. To install additional languages (optional), issue this command for the language that you want:

   ```
   $ rpm -i TIVsm-msg.xx_XX.s390x.rpm
   ```

   Note: `xx_XX` represents the country code for the language contents of the package.
6. Change to the `<cdrom>/oracle/linuxz64` directory where the Data Protection for Oracle installable file resides on the CD:

```
$ cd <cdrom>/oracle/linuxz64
```

Note *<cdrom>* is the drive where the CD is mounted.

7. Enter the name of the installable file (`TDP-Oracle.s390x.bin`) on the command line and press **Enter** to install Data Protection for Oracle:

```
$ TDP-Oracle.s390x.bin
```

To install in console mode, enter the following command and press **Enter**:

```
$ TDP-Oracle.s390x.bin -i console
```

To install in silent mode, enter the following command and press **Enter**:

```
$ TDP-Oracle.s390x.bin -i silent
```

To install in GUI mode, enter the following command and press **Enter**:

```
$ TDP-Oracle.s390x.bin -i gui
```

If the installable file was downloaded from the FTP site, the filename might be different than `TDP-Oracle.s390x.bin`.

8. If you want to install Data Protection for Oracle in a language other than English, enter the name of the Data Protection for Oracle installable file for the language that you want (`TDP-Oracle.msg.xx_XX.s390x.bin`) on the command line and press **Enter**:

```
$ TDP-Oracle.msg.xx_XX.s390x.bin
```

Make sure the Tivoli Storage Manager API language package for the language that you want (`TIVsm-msg.xx_XX.s390x.rpm`) is also installed.

Note: The libobk.so library file is located automatically based on the link that the installation program places in the `/usr/lib64` directory. This is the default link:
`/usr/lib64/libobk.so /opt/tivoli/tsm/client/oracle/bin64/libobk.so`

Installing Data Protection for Oracle on 64-bit Solaris SPARC

Use these instructions to install Data Protection for Oracle on 64-bit Solaris SPARC.

Before you begin, you must uninstall any previous version of Data Protection for Oracle, or the Tivoli Storage Manager API, before installing a new or updated version. If you are installing a fix pack or interim fix version of Data Protection for Oracle, do not remove the license enablement file from the previous version. The fix pack and interim fix drivers do not contain a license enablement file.

All installable files reside under the `/cdrom/oracle/solaris` directory.

Table 17. Solaris SPARC 64-bit Default Installation Directories

Solaris	Default Installation Directories
Data Protection for Oracle 64-bit	/opt/tivoli/tsm/client/oracle/bin64

Table 17. Solaris SPARC 64-bit Default Installation Directories (continued)

Solaris	Default Installation Directories
Data Protection for Oracle Utilities	/opt/tivoli/tsm/client/oracle/bin64
Data Protection for Oracle Messages	/opt/tivoli/tsm/client/oracle/bin64
Tivoli Storage Manager API 64-bit	/opt/tivoli/tsm/client/api/bin64

Table 18. Data Protection for Oracle 64-bit and Tivoli Storage Manager installable files and packages

Component	Installable file or package
Data Protection for Oracle 64-bit base code, license, utilities	TDPoracle64.bin
Data Protection for Oracle Languages	TDPoracle64*xx*_*XX*.bin
Tivoli Storage Manager API 64-bit	TIVsmCapi.pkg
Tivoli Storage Manager API Languages	TIVsmCl*Xx*.pkg

Perform these instructions to install the Tivoli Storage Manager API, Data Protection for Oracle, and the Data Protection for Oracle license package. This example assumes that your CD drive is **/cdrom** and that you are installing the Data Protection for Oracle 64-bit product.

1. Insert the CD containing the client package into the CD drive.
2. Log in as the *root* user.
3. Issue this command to install the Tivoli Storage Manager API:

   ```
   $ pkgadd -d /cdrom/oracle/solaris/api/TIVsmCapi.pkg
   ```

   The Tivoli Storage Manager API default language is English. To install additional languages (optional), issue this command for the desired language:

   ```
   $ pkgadd -d /cdrom/oracle/solaris/api/TIVsmCl Xx.pkg
   ```

   Note: `Xx` represents the country code for the language contents of the package.
4. Change to the `/cdrom/oracle/solaris` directory where the Data Protection for Oracle installable file resides on the CD:

   ```
   $ cd /cdrom/oracle/solaris
   ```

5. Enter the name of the installable file (`TDPoracle64.bin`) on the command line and press **Enter** to install Data Protection for Oracle:

   ```
   $ TDPoracle64.bin
   ```

   To install in console mode, enter the following command and press **Enter**:

   ```
   $ TDPoracle64.bin -i console
   ```

   To install in silent mode, enter the following command and press **Enter**:

```
$ TDPoracle64.bin -i silent
```

To install in GUI mode, enter the following command and press **Enter**:

```
$ TDPoracle64.bin -i gui
```

If the installable file was downloaded from the FTP site, the filename might be different from `TDPoracle64.bin`.

6. If you want to install Data Protection for Oracle in a language other than English, enter the name of the Data Protection for Oracle installable file for the desired language (`TDPoracle64xx_XX.bin`) on the command line and press **Enter**:

```
$ TDPoracle64xx_XX.bin
```

Make sure the Tivoli Storage Manager API language package for the desired language (`TIVsmClXx.pkg`) is also installed.

7. Link the Oracle target database instance with Data Protection for Oracle by performing the following steps:
   a. Set the Oracle LD_LIBRARY_PATH option to specify `$ORACLE_HOME/lib` as the first entry:

```
LD_LIBRARY_PATH=$ORACLE_HOME/lib
```

   b. Shut down all Oracle instances that use `$ORACLE_HOME`.
   c. Go to the `$ORACLE_HOME/lib` directory.
   d. Symbolically link the library file to *libobk.so*:

```
$ ln -s /usr/lib/sparcv9/libobk.so $ORACLE_HOME/lib/libobk.so
```

   e. Start the Oracle instances.

Chapter 3. Configuring Data Protection for Oracle

Use these instructions to configure Data Protection for Oracle for backup and restore operations.

Data Protection for Oracle must be installed on your system and a Tivoli Storage Manager server must be available to communicate with Data Protection for Oracle.

Review all configuration information before performing any configuration tasks.

Quick configuration with default settings

You can quickly configured Data Protection for Oracle using default settings and minimal configuration tasks. The quick configuration minimizes setup time and helps you to proceed quickly to a state where you can begin backing up your Oracle databases.

Use the instructions in this topic to configure Data Protection for Oracle. These instructions use AIX 64-bit as the example operating system. If you are using an operating system other than AIX, you must change the installation paths and library extensions documented in this procedure as applicable to the operating system in use.

See "Configuring Data Protection for Oracle" on page 23 for detailed instructions on how to customize Data Protection for Oracle for your environment and processing needs.

1. Install Data Protection for Oracle. For detailed installation instructions, see Chapter 2, "Installing," on page 5.
2. Make sure the following link exists:

   ```
   $ORACLE_HOME/lib/libobk.a -> /usr/lib/libobk64.a
   ```

3. Change to the `/usr/tivoli/tsm/client/oracle/bin64` directory and copy the `tdpo.opt.smp` file to `tdpo.opt`. Edit the `tdpo.opt` file to include these options:

   ```
   dsmi_orc_config /usr/tivoli/tsm/client/oracle/bin64/dsm.opt
   dsmi_log <directory with write permissions>
   ```

   For more information about these options, see "Available Data Protection for Oracle options" on page 24.
4. In this same directory, create a `dsm.opt` file. Edit the `dsm.opt` file to include the following server stanza:

   ```
   SErvername tdpo
   ```

   For more information about this option and the `dsm.opt` file, see "3. Define Tivoli Storage Manager options in the client options file" on page 27.
5. Change to the `/usr/tivoli/tsm/client/api/bin64` directory and create a symbolic link to `/usr/tivoli/tsm/client/ba/bin/dsm.sys`. Edit the `dsm.sys` file to include another server stanza with the following options:

© Copyright IBM Corp. 1998, 2011

```
SErvername tdpo
COMMMethod TCPip
TCPServeraddress x.x.x.x
PASSWORDAccess generate
passworddir /home/<oracle user>
nodename TDPONodeName
```

Replace *x.x.x.x* with the IP address of the Tivoli Storage Manager server to which Data Protection for Oracle will back up data. Replace *<oracle user>* with the Oracle User ID of the target Oracle database instance.

For more information about the `dsm.sys` file, these options, and their relationship with Data Protection for Oracle, see "3. Define Tivoli Storage Manager options in the client options file" on page 27.

6. Register the node to the Tivoli Storage Manager server with the following command:

   `REG NODE` *`hostname`*`_oracle` *`password`* `maxnummp=`*`n`*

   where *hostname* is the name of the machine where Data Protection for Oracle is installed, *password* is the password for this node, and *n* is equal to the number of channels that you are planning to use.

7. Make sure the Oracle user has the following permissions:
   - Read (r) permission to the `/usr/tivoli/tsm/client/oracle/bin64` and `/usr/tivoli/tsm/client/api/bin64` directories.
   - Read permission (r-) to the tdpo.opt, dsm.opt, and dsm.sys files located in the `/usr/tivoli/tsm/client/oracle/bin` and `/usr/tivoli/tsm/client/api/bin` directories.

8. Change to the `/usr/tivoli/tsm/client/oracle/bin64` directory and run the **tdpoconf password** command as *Oracle* user to generate the password file.

   For more information about this command, see "Password command" on page 50.

9. Run the **tdpoconf showenvironment** command to confirm proper configuration.

   For more information about this command, see "Showenvironment command" on page 51.

10. As Oracle user, run your RMAN backup script with the ENV=(***TDPO_OPTFILE***=/usr/tivoli/tsm/client/oracle/bin64/tdpo.opt) parameter specified.

    For example:

```
run
{
   allocate channel t1 type 'sbt_tape' parms
            'ENV=(TDPO_OPTFILE=/usr/tivoli/tsm/client/oracle/bin64/tdpo.opt)';

   backup
      filesperset 5
      format 'df_%t_%s_%p'
      (database);

   }
```

    Note that the `allocate channel` entry is divided on two lines after the `parms` option to accommodate page formatting.

    For more information about RMAN backup scripts, see "Using RMAN and Data Protection for Oracle" on page 35.

Configuring Data Protection for Oracle

After Data Protection for Oracle is successfully installed, you must complete the several configuration tasks.

1. Define Data Protection for Oracle options in the tdpo.opt file.
2. Register the Data Protection for Oracle node to a Tivoli Storage Manager server.
3. Define Tivoli Storage Manager options in the dsm.opt and dsm.sys files.
4. Define Tivoli Storage Manager policy requirements.
5. Initialize the password with a Tivoli Storage Manager server.

If you would like to configure Data Protection for Oracle using default settings, see "Quick configuration with default settings" on page 21 for instructions.

1. Define Data Protection for Oracle options in the tdpo.opt file

You must define options to control the way Data Protection for Oracle backs up and restores data.

The Data Protection for Oracle options file, tdpo.opt, contains options that determine the behavior and performance of Data Protection for Oracle. The *only* environment variable Data Protection for Oracle Version 6.3 recognizes within an RMAN script is the fully qualified path name to the tdpo.opt file. Therefore, some RMAN scripts may need to be edited to use ***TDPO_OPTFILE****=fully qualified path and file name of options file* variable in place of other environment variables. For example:

```
allocate channel t1 type 'sbt_tape' parms
       'ENV=(TDPO_OPTFILE=/home/rman/scripts/tdpo.opt)'
```

See "Scripts" on page 36 for further information. Note that the `allocate channel` entry is divided on two lines after the `parms` option to accommodate page formatting.

The ***TDPO_OPTFILE*** variable *must* be specified in upper case characters only.

If a fully qualified path name is not provided, Data Protection for Oracle uses the tdpo.opt file located in the Data Protection for Oracle default installation directory. If this file does not exist, Data Protection for Oracle fails.

Note:

- For best results, use the tdpo.opt file exclusively instead of default parameters.
- RMAN and the **tdpoconf** and **tdposync** utilities use the options defined in the tdpo.opt file.
- By default, the tdpo.opt file is located in the directory where Data Protection for Oracle is installed.
- You can specify options in the tdpo.opt file in both upper case or lower case type. However, the ***TDPO_OPTFILE*** variable *must* be specified in upper case characters only.

Available Data Protection for Oracle options

The following options can be set in the tdpo.opt file:

dsmi_log
Specify the directory that contains the Data Protection for Oracle error log file (tdpoerror.log).

Note that if the Tivoli Storage Manager ***errorlogname*** option is specified in the dsm.sys file (for the stanza used by Data Protection for Oracle), the ***errorlogname*** option will override the value specified by ***dsmi_log***. If the ***errorlogname*** option is being used, make sure that it specifies a file in a path that has write permissions.

For error log files, create a directory for the error logs and have the ***dsmi_log*** option point to that directory. The user performing backups must have writable rights to this directory.

dsmi_orc_config
Specify the complete path to the Tivoli Storage Manager client user options file (dsm.opt) used during the Data Protection for Oracle session. If you do not specify this option, Data Protection for Oracle looks for this options file in the Data Protection for Oracle installation directory. You must specify this option if your Tivoli Storage Manager client user options file is located in a directory other than the Data Protection for Oracle installation directory.

tdpo_fs
Specify a file space name on the Tivoli Storage Manager server for Data Protection for Oracle backup, delete, and restore operations. The file space name can contain a string of *1* to *1024* characters.

- The default file space name is *adsmorc*.
- When you have more than one Oracle database, use this option to back up each Oracle target database to its own file space on the Tivoli Storage Manager server.
- The file space name in the include/exclude statement must match the file space name specified in the ***tdpo_fs*** option for include/exclude processing to function correctly.
- If this option was set during Data Protection for Oracle backup operations, this option *must* be set during restore and delete operations.

tdpo_owner
This option specifies a session-owner name and object owner name. The value can contain a string of 1 to 64 characters. This value is case sensitive. For restore and delete operations, this option *must* specify the same value that was used during the Data Protection for Oracle backup. Do not set this option when ***passwordaccess*** *generate* is specified.

tdpo_pswdpath
This option specifies the directory where the TDPO.nodename password file is located. The default value is the directory where Data Protection for Oracle is installed. Note that when ***passwordaccess*** *generate* is specified, Data Protection for Oracle uses the value of the ***passworddir*** option specified in the dsm.sys file and does NOT use the ***tdpo_pswdpath*** option. However, the directory specified by the ***passworddir*** option must be a directory that is writeable by the Oracle user. The Oracle user is the User ID of the target Oracle database instance.

tdpo_node

Specify the Data Protection for Oracle node name used during operations with the Tivoli Storage Manager server. The node name can contain a string of *1* to *64* characters. It is recommended that you use a node name that is different from the backup-archive client node name.

Be aware that it is the Tivoli Storage Manager API (and not Data Protection for Oracle) that negotiates which login credentials (nodename, password) to use with the Tivoli Storage Manager server. As a result, certain option settings affect password management. For example, when the ***tdpo_node*** option is specified (in the tdpo.opt file) and ***passwordaccess*** *prompt* is specified (in the dsm.sys file), the Tivoli Storage Manager API uses the value of the ***tdpo_node*** option and ignores the value of the ***nodename*** option (specified in the dsm.sys file). If you do not specify a value for the **passwordaccess** option, the default value is `prompt`. Make sure you follow these recommendations:

- When ***passwordaccess*** *prompt* is specified in the dsm.sys file, you can specify the ***tdpo_node*** option in the tdpo.opt file.
- When ***passwordaccess*** *generate* is specified in the dsm.sys file, do NOT specify the ***tdpo_node*** option in the tdpo.opt file.

To restore data from one Oracle server to another Oracle server using Data Protection for Oracle, be aware of the following ***tdpo_node*** considerations:

- The value of the ***tdpo_node*** option in the tdpo.opt file on the target Oracle server must equal the value of the ***tdpo_node*** option in the tdpo.opt file on the source Oracle server.
- If ***passwordaccess*** *prompt* is specified for the backup, then ***passwordaccess*** *prompt* must be specified for the restore. For example, if ***passwordaccess*** *prompt* is specified in the dsm.sys file on the target Oracle server, run the **tdpoconf password** command to create the password locally on the source Oracle server.
- If ***passwordaccess*** *generate* is specified for the backup, then ***passwordaccess*** *generate* must be specified for the restore. Be aware that if the password for the Data Protection for Oracle node is unknown (due to the ***passwordaccess*** *generate* setting), you can reset the password for the production node on the Tivoli Storage Manager server. Then, after the password is reset, use the new password to run the **tdpoconf password** command on both the production machine (to set the password for the next backup) and the alternate machine (to set the password for the restore).
- Data Protection for Oracle and the Tivoli Storage Manager API must be at the same levels on both the source Oracle server and the target Oracle server.

tdpo_date_fmt

This option specifies the format you want to use to display dates.

You can specify a number between *0* and *5* inclusively. The default value is *1*.

0 Use the locale-specified date format.

1 MM/DD/YYYY (Default)

2 DD-MM-YYYY

3 YYYY-MM-DD

4 DD.MM.YYYY

5 YYYY.MM.DD

tdpo_num_fmt
This option specifies the format you want to use to display numbers. You can specify a number between *1* and *6* inclusively. The default value is *1*.

1 1,000.00 (Default)

2 1,000,00

3 1 000,00

4 1 000.00

5 1.000,00

6 1'000,00

tdpo_time_fmt
This option specifies the format you want to use to display time.

You can specify a number between *0* and *4* inclusively. The default value is *1*.

0 Use the locale-specified time format.

1 23:00:00 (Default)

2 23,00,00

3 23.00.00

4 12:00:00 A/P

tdpo_mgmt_class_2
This option specifies the second management class used for copy 2 in the RMAN duplex copy command.

tdpo_mgmt_class_3
This option specifies the third management class used for copy 3 in the RMAN duplex copy command.

tdpo_mgmt_class_4
This option specifies the fourth management class used for copy 4 in the RMAN duplex copy command. Four copies is the maximum allowed by RMAN.

Note: See "Using the Duplex Copy function" on page 38 for specific details on using management class options.

2. Register the Data Protection for Oracle node to a Tivoli Storage Manager server

The Data Protection for Oracle node name and password (if required) must be registered to the Tivoli Storage Manager server before you can begin requesting backup and restore services. The process of setting up a node name and password with the Tivoli Storage Manager server is called *registration*.

The following information is needed to register Data Protection for Oracle with the Tivoli Storage Manager server:

- The Data Protection for Oracle node name

  This is the node name that identifies the instance on which Data Protection for Oracle is installed. It is recommended that you use a separate and unique node name for Data Protection for Oracle. This prevents any confusion with an existing Tivoli Storage Manager backup-archive client on the same workstation.
- The initial password

  This is the password you want to use, if a password is required.

The following information is defined by the Tivoli Storage Manager administrator:

- The policy domain to which your client node belongs.

  A policy domain contains policy sets and management classes that control how Tivoli Storage Manager manages the objects you back up. Rather than binding Data Protection for Oracle backups to a different management class, it is recommended that a unique policy domain be defined for Data Protection for Oracle node names. These backups can be bound to the default management class within this unique policy domain. Rather than binding a different management class for Oracle backups, it is also recommended that you specify a different domain for Oracle backups with a separate management class.

- The authority to enable compression.

  The Tivoli Storage Manager administrator can specify the server to compress files. If the Tivoli Storage Manager administrator specifies that the compression decision belongs to the client (***compression*** *client*), you must specify ***compression*** *yes* in the client system options file (dsm.sys) in order for the Data Protection for Oracle node to be able to compress objects before sending them to the Tivoli Storage Manager server.

- The authority to delete backup data from Tivoli Storage Manager storage.

  The Data Protection for Oracle node can only delete backed up data from Tivoli Storage Manager storage if the Tivoli Storage Manager administrator registers the node with ***backdelete*** authority. Specify the following option to allow ***backdelete*** authority:

  backdelete *yes*

  Note that when ***backdelete*** *no* is specified and a deletion request is made, the request fails and an error message displays. Therefore, specify ***backdelete*** *yes* for the object to be immediately removed from the Tivoli Storage Manager server when the next inventory expiration occurs. This expiration also makes the previously used storage space available for new use.

3. Define Tivoli Storage Manager options in the client options file

You must define some Tivoli Storage Manager options after the Data Protection for Oracle node is registered to the Tivoli Storage Manager server:

- These options are defined in the Tivoli Storage Manager client system options file (dsm.sys by default) and client user options file (dsm.opt by default).
- Note that the Tivoli Storage Manager client user options file (dsm.opt by default) that you must edit for Data Protection for Oracle is located in the directory specified by the ***dsmi_orc_config*** option. If this option is not specified, Data Protection for Oracle looks for this options file in the Data Protection for Oracle installation directory.
- The Tivoli Storage Manager client system options file (dsm.sys by default) must be located in the directory where the Tivoli Storage Manager API is installed.
- Data Protection for Oracle provides sample Tivoli Storage Manager options files that you can modify for this purpose. These sample files are located in the Data Protection for Oracle installation directory.
- The Tivoli Storage Manager administrator can provide you with the TCP server address (***tcpserveraddress***) and communication method (***commmethod***) for connecting Data Protection for Oracle to the Tivoli Storage Manager server.

Required options

You must set required Tivoli Storage Manager client options in order to operate Data Protection for Oracle.

Specify the required options in the Tivoli Storage Manager client system options file (dsm.sys by default) located in the directory where the Tivoli Storage Manager API is installed.

passwordaccess

Specify whether you want Data Protection for Oracle or the Tivoli Storage Manager API to manage the password. You can specify one of the following values:

prompt Data Protection for Oracle manages the password. This is the default. When specifying ***passwordaccess*** *prompt* in the dsm.sys file, you can optionally set the following values in the tdpo.opt file:

```
tdpo_node <node name>
tdpo_owner <tdpo owner name>
tdpo_pswdpath (optional) <path to password file>
```

After specifying these values, use the **tdpoconf password** command (as root user) to create the password and password file (TDPO.*nodename*) on the local machine. Be aware that when ***passwordaccess*** *prompt* is specified, the user must be aware of the password expiration date. A backup failure may occur if the password is allowed to expire. To allow the Tivoli Storage Manager API to manage the password, specify ***passwordaccess*** *generate*.

generate

The Tivoli Storage Manager API manages all password actions after the password is created using the **tdpoconf password** command. The Tivoli Storage Manager API stores and manages the password and automatically *generates* a new password when the current password expires. This method of password management is useful when running unattended scheduled backups because it ensures that the backup never fails due to an expired password. When specifying ***passwordaccess*** *generate*, set the following values in the dsm.sys file:

```
passwordaccess generate
passworddir <directory owned and writable by Oracle owner>
nodename <node name>
```

However, do *not* specify the following options in the tdpo.opt file when specifying ***passwordaccess*** *generate*:

- ***tdpo_node***
- ***tdpo_owner***
- ***tdpo_pswdpath***

After specifying ***passwordaccess*** *generate* and the other appropriate values in the dsm.sys file, run the **tdpoconf password** command (as the Oracle user) to create the encrypted password in the TSM.PWD file.

servername

Specify the name you want to use to identify a stanza that contains the

options used for connecting to the Tivoli Storage Manager server. Although the name does not have to be the actual name of a Tivoli Storage Manager server, the name must match the name specified by the ***servername*** option in the dsm.opt file.

tcpserveraddress

Specify the TCP/IP address in the stanza for the Tivoli Storage Manager server to be used for Oracle backups. When the Tivoli Storage Manager server that is specified with the ***tcpserveraddress*** option uses a non-default port for communication, specify the correct port in the stanza with the ***tcpport*** option.

commmethod

Specify the communication method for Data Protection for Oracle to communicate with the Tivoli Storage Manager server. Note that this option requires other Tivoli Storage Manager options, depending on the communication method you specify.

Required option in the `dsm.opt` file

Specify this option in the Tivoli Storage Manager client user options file (dsm.opt by default) located in the directory specified by the ***dsmi_orc_config*** option:

servername

Specify a Tivoli Storage Manager server stanza name that matches the name specified by the ***servername*** option in your client system options file (dsm.sys by default) that is used to contact Data Protection for Oracle for backup services.

Other options to consider

There are other Tivoli Storage Manager client options that you can use when configuring Data Protection for Oracle.

You can specify these options in the Tivoli Storage Manager client system options file (dsm.sys).

compression

Specify whether the Tivoli Storage Manager API compresses data before sending it to the Tivoli Storage Manager server. You can specify `yes` or `no`. The default value is `No`. The value of the compression option for Data Protection for Oracle is honored only if the Tivoli Storage Manager administrator leaves the compression decision to the node. Enabling compression affects performance in three ways:

- CPU utilization is higher on the machine on which Data Protection for Oracle is running.
- Network bandwidth utilization is lower because fewer bytes are transmitted.
- Storage usage on the Tivoli Storage Manager server is reduced.

It is recommended that you specify *yes* when any of the following conditions exist:

- The network adapter has a data overload.
- Communications between Data Protection for Oracle and the Tivoli Storage Manager server are over a low bandwidth connection.
- There is heavy network traffic.

It is recommended that you specify *no* when any of the following conditions exist:

- The machine running Data Protection for Oracle has a CPU overload. The added CPU usage as a result of enabling compression can impact other applications, including the Oracle server.
- You are not constrained by network bandwidth. In this case, you can achieve the best performance by specifying ***compression*** *no* and enabling hardware compaction on the tape drive, which also reduces storage requirements.
- Hardware compression is in use for the media where Data Protection for Oracle data resides.

After a completed backup operation, view the throughput rate and the compression status for a backup object in the Tivoli Storage Manager server activity log file. Run the Tivoli Storage Manager server QUERY ACTLOG command in the Tivoli Storage Manager server administrative client window. Be aware that the throughput rate and the compression status are not written to the activity log when activity logging is disabled on the Tivoli Storage Manager server. See the SET ACTLOGRETENTION command in the *Tivoli Storage Manager Administrator's Reference* for complete activity logging information.

You can also determine whether objects were compressed by running the **tdposync query** command.

deduplication

Specify whether the Tivoli Storage Manager API deduplicates data before sending it to the Tivoli Storage Manager server. You can specify `Yes` or `No`. The default value is `No`. The value of the deduplication option for Data Protection for Oracle applies only if the Tivoli Storage Manager administrator allows client-side data deduplication.

You can determine whether objects have been deduplicated by running the **tdposync query** command or by examining the Tivoli Storage Manager server activity log file.

The ***deduplication*** and ***enablelanfree*** options are mutually exclusive. Therefore, you can only use either one option or the other, but not both options together.

The ***deduplication*** and ***enableclientencryptkey*** options are also mutually exclusive. Therefore, you can only use either one option or the other, but not both options together.

enablelanfree

Specify whether you run backup or restore operations in a LAN-free environment if you are equipped to do so. You can specify *yes* or *no*. The default value is *no*. You can avoid network constraints by shifting the movement of data to a storage area network (SAN). After a completed backup operation, view the LAN-free status for a backup object in the Tivoli Storage Manager server activity log file. For more information, see the appropriate Storage Agent User's Guide.

The ***enablelanfree*** and ***deduplication*** options are mutually exclusive. Therefore, you can only use either one option or the other, but not both options together.

include

When a management class other than the default management class is

defined within an existing policy domain, add an include statement to the client options file that is used by the Oracle node.

You must add an include statement to the dsm.sys file.

This include statement binds the Oracle backup objects to the management class that is defined for managing these objects. The include statement uses the following naming convention:

```
/FilespaceName//ObjectName
```

The FORMAT parameter in the RMAN script can also be used to assist with object naming. For example, if the FORMAT parameters (in the RMAN script) specified the following values for databases and logs:

```
format 'DB_%u_%p_%c'
format 'LOG_%u_%p_%c'
```

The include statement in the dsm.sys file (used by the Oracle node) would be as follows:

```
INCLUDE /adsmorc/.../DB* mgmtclassnameforDBs
INCLUDE /adsmorc/.../LOG* mgmtclassnameforLogs
```

Make sure the FORMAT parameter specifies a unique name for the backup. If the object name already exists on the Tivoli Storage Manager server, the backup might fail with a RC=8 error recorded in the sbtio.log file.

enableclientencryptkey

When ***enableclientencryptkey*** is set to *yes*, Data Protection for Oracle provides 128-bit transparent encryption of Oracle databases during backup and restore processing. One random encryption key is generated per session and is stored on the Tivoli Storage Manager server with the object in the server database. Although Tivoli Storage Manager manages the key, a valid database must be available in order to restore an encrypted object.

Important: The ***enableclientencryptkey*** and ***deduplication*** options are mutually exclusive because encrypted files cannot be deduplicated. Therefore, you can only use either one or the other option, but not both options together.

You can specify the databases you want encrypted by adding an include statement with the ***include.encrypt*** option in the dsm.sys file.

For example, to enable transparent encryption, do the following steps:

1. Edit the client system options file, dsm.sys.
2. Specify ***enableclientencryptkey*** *yes*.
3. Specify ***encryptiontype*** *AES128* (recommended) or *DES56*.
4. Specify the objects to encrypt. This example encrypts all data:

   ```
   include.encrypt        /adsmorc/.../*
   ```

Thus, the encryption options would be as follows in this client system options file, dsm.sys:

```
enableclientencryptkey yes
encryptiontype aes128
include.encrypt        /adsmorc/.../*
```

See *IBM Tivoli Storage Manager Using the Application Programming Interface* for more details regarding the ***enableclientencryptkey*** option.

You can determine whether objects were encrypted by running the **tdposync query** command.

4. Define Tivoli Storage Manager policy requirements

Data Protection for Oracle requires special Tivoli Storage Manager policy domain settings.

RMAN uses the ***format*** parameter (in the RMAN script) to generate unique backup file names. Because all backup objects inserted into the Tivoli Storage Manager backup storage pool have unique file names, they never expire on the Tivoli Storage Manager server. As a result, Data Protection for Oracle requires the following special Tivoli Storage Manager policy domain settings:

Backup copy group values

Data Protection for Oracle provides the **tdposync** utility to remove unwanted backup objects from the Tivoli Storage Manager server. It is recommended that the following Tivoli Storage Manager backup copy group options be set:

- ***verdeleted*** *0*
- ***retonly*** *0*

Then, when Data Protection for Oracle marks a backup object inactive, that object is deleted from the Tivoli Storage Manager server the next time expiration processing occurs. A backup object is marked for immediate expiration when you delete it through RMAN using the Data Protection for Oracle interface or with the **tdposync** utility. Note that an inactive backup object cannot be restored through RMAN using the Data Protection for Oracle interface.

Note:

1. The Tivoli Storage Manager administrator must also register your node by specifying ***backdelete*** *yes* in order for backup objects to be deleted. However, be aware that a backup object is marked for immediate expiration when ***backdelete*** *yes* and you delete it through RMAN using the Data Protection for Oracle interface or with the **tdposync** utility. Also note that when ***backdelete*** *no* is specified and a deletion request is made, the request fails and an error message displays.
2. The following backup copy group options are not applicable to Data Protection for Oracle:
   - ***frequency***
   - ***verexists***
   - ***retextra***
   - ***mode***
   - ***serialization***

   Data Protection for Oracle accepts default values for these options.

Management class

Tivoli Storage Manager uses management classes to manage backups on the Tivoli Storage Manager server. When you back up a database, the default management class for your node is used. Because the policy requirements for Data Protection for Oracle may be different from the desired settings for the regular Tivoli Storage Manager backup-archive clients, you must have a different management class defined for Data Protection for Oracle. It is recommended that you define a separate policy

domain where the default management class has the required settings and then register all Data Protection for Oracle nodes to that domain.

If you choose to define a new management class within an existing policy domain (not the default management class for that domain), then you must add an ***include*** statement to the Data Protection for Oracle options file to bind all objects to that management class.

The following steps assign a management class name *orcbackup* to all Oracle backups with a default file space name *adsmorc*:

1. Add this ***inclexcl*** entry under the server stanza you use in the dsm.sys file:

   ```
   inclexcl /u01/oracle/include.def
   ```

2. Add the following ***include*** entry to the `/u01/oracle/include.def` file:

   ```
   include /adsmorc/.../* orcbackup
   ```

   Note: The file space name in the include/exclude statement must match the file space name defined with the ***tdpo_fs*** option. If a file space name other than the default value (*adsmorc*) is used:

   a. You must specify the file space name with the ***tdpo_fs*** option.

   b. You must specify the file space name defined in the ***tdpo_fs*** option in the include/exclude statement.

All the files backed up with a default file space name of *adsmorc* are assigned to management class *orcbackup*.

Note: Data Protection for Oracle stores all objects as backup objects on Tivoli Storage Manager storage, so an archive copy group is not required, although it can exist.

See your Tivoli Storage Manager administrator or see the *Tivoli Storage Manager Administrator's Guide* for more information on defining or updating Tivoli Storage Manager policy domains and copy groups.

5. Initialize the password with a Tivoli Storage Manager server

The administrator must run the **tdpoconf** utility program to set the password before using Data Protection for Oracle.

Related reference

"TDPOCONF" on page 50

Chapter 4. Protecting Oracle Server data

Use Data Protection for Oracle to back up and restore Oracle Server data.

Data Protection for Oracle must be installed and configured on your system and an Oracle Server must be available.

Using RMAN and Data Protection for Oracle

You can perform full or partial, offline or online backups with Oracle. Once you identify which database to back up, Oracle locates all necessary files and sends them to the Tivoli Storage Manager server through Data Protection for Oracle.

As a result, Data Protection for Oracle provides an interface between Oracle Media Management API calls and Tivoli Storage Manager API routines.

Invoking RMAN

Invoke RMAN to back up and restore an Oracle database.

In this example, the catalog database contains a registered target database. Invoke RMAN with this command:

```
$>  rman target xxx/yyy@target rcvcat aaa/bbb@catalog
  cmdfile bkdb.scr msglog bkdb.log
```

This starts RMAN in the sequence shown.

```
target xxx/yyy@target: connect to target database
using user xxx and password yyy with connect string target
rcvcat aaa/bbb@catalog: connect to catalog database
using user aaa and password bbb with connect string catalog
cmdfile bkdb.scr:  run bkdb.scr script
msglog bkdb.log:  log the output messages in bkdb.log
```

Tip: In the above example, RMAN creates a log file (bkdb.log) in the current working directory. If an error occurs, you will see the error stack in the log file.

Attention: For backup and restore operations in a Linux environment, Oracle recommends that the Oracle LD_ASSUME_KERNEL variable be set for the Oracle user. For example:

```
LD_ASSUME_KERNEL=2.4.21; export LD_ASSUME_KERNEL
```

After a completed backup or restore operation, view the throughput rate and encryption status for a backup object in the Tivoli Storage Manager server activity log file. Run the Tivoli Storage Manager server **QUERY ACTLOG** command in the Tivoli Storage Manager server administrative client window. A message similar to the following will be available:

© Copyright IBM Corp. 1998, 2011

```
08/03/11
12:41:27
ANE4991I (Session: 67, Node: MACHINE_ORC) DP Oracle AIX ANU0599 TDP for Oracle:
(5508): =>()
ANU2526I Backup details for backup piece /adsmorc//df_727444762_116_1 (database "orcl").
Total bytes processed: 9961472. Deduplicated: Yes. Bytes after deduplication: 2272805.
Deduplication reduction: 77.18%. Compressed: Yes. Bytes after compression: 52253.
Compressed by: 97.70%. Encryption: None. LAN-Free: No. Total bytes sent: 52253.
Total data reduction: 99.48%. Total processing time: 00:00:01.
Throughput rate: 9728.00Kb/Sec. (SESSION: 67)
```

Scripts

Data Protection for Oracle does not recognize environment variables specified in an RMAN script. The *only* environment variable Data Protection for Oracle recognizes within an RMAN script is the fully qualified path name to the `tdpo.opt` file. Therefore, existing RMAN scripts may need to be edited to use ***TDPO_OPTFILE****=fully qualified path and file name of options file* variable in place of other environment variables.

The *TDPO_OPTFILE* variable can be specified in either lower or uppercase in an RMAN script. Data Protection for Oracle uses the default `tdpo.opt` file in the installation directory if no path is specified.

Using the `send` command

Use the Oracle RMAN **`send`** command in an RMAN script to pass Tivoli Storage Manager options to the Tivoli Storage Manager API.

When you use this technique to send Tivoli Storage Manager options such as TCPServeradddress and TCPport to the Tivoli Storage Manager API, you can customize the actions that the script takes without updating the existing Data Protection for Oracle or Tivoli Storage Manager API options files. Therefore, any option that is sent through the send command overrides the option that is specified in the Data Protection for Oracle or Tivoli Storage Manager API options files.

You must specify the **`send`** command in an RMAN script. You can specify one or more Tivoli Storage Manager options in a **`send`** command string. The **`send`** command string can contain up to 512 bytes in length.

For example, to back up an Oracle database to the Tivoli Storage Manager server named "`halley`" at TCP/IP port 1601, and to enable the cache for client-side data deduplication for only channel t1, specify the following statements in an RMAN script:

```
allocate channel t1 type 'SBT_TAPE';
SEND channel 't1' '-TCPSERVER=halley -TCPPORT=1601 -ENABLEDEDUPCACHE=YES';
```

Data Protection for Oracle passes the command string to the Tivoli Storage Manager API. The Tivoli Storage Manager API validates the contents of the string. If an invalid entry is detected, the API issues an ANS****E message to Data Protection for Oracle, which returns this error condition to Oracle RMAN and stops processing.

You can specify any Tivoli Storage Manager API option that typically goes into the `dsm.opt` file and the following client system options (`dsm.sys`):

- ENABLECLIENTENCRYPTKEY
- ENABLELANFREE

- TCPSERVERADDRESS
- TCPPORT
- ASNODENAME
- FROMNODE
- FROMOWNER
- DEDUPCACHEPATH
- ENABLEARCHIVERETENTIONPROTECTION

You can specify multiple Tivoli Storage Manager API options in the same **send** command.

The ENABLELANFREE and DEDUPLICATION options are mutually exclusive. If both options are defined, client-side data deduplication will not occur.

The ENABLECLIENTENCRYPTKEY and DEDUPLICATION options are also mutually exclusive. If both options are defined, client-side data deduplication will not occur.

Related tasks

"Script examples"

Script examples

Sample RMAN scripts illustrate how to create parallel backup streams to Tivoli Storage Manager server storage.

In these examples, to back up to Tivoli Storage Manager by using Data Protection for Oracle, you must specify `type 'sbt_tape'` in the RMAN script or within the global RMAN configuration settings.

Example 1:

When the Tivoli Storage Manager server and Oracle machines have multiple network cards, you can back up your data using multiple network paths to improve network throughput. Your environment is set up as follows:

- The Oracle machine has two network cards with two addresses (A and B).
- The Tivoli Storage Manager server also has two network cards with two addresses (C and D).
- Paths exist between A and C, B and D, but not between A and D or B and C.

Create two backup streams (Oracle channels) without using two separate options files to point to different two different addresses. Channel t1 goes to address C, channel t2 goes to address D. Be careful not to send parts of your backup to two different Tivoli Storage Manager server because you will not be able to restore it.

You can maintain one Data Protection for Oracle options file and change the Tivoli Storage Manager server specification in an RMAN script in the following manner:

```
run
{
   allocate channel t1 type 'sbt_tape';
      SEND channel t1 '-TCPSERVER=<C>';
   allocate channel t2 type 'sbt_tape';
      SEND channel t2 '-TCPSERVER=<D>';

   backup
      filesperset 5
      format 'df_%t_%s_%p'
```

```
      (database);
   release channel t2;
   release channel t1;
}
```

Example 2:

This backup script allocates two parallel connections to the Tivoli Storage Manager server. The Tivoli Storage Manager server views these connections as two separate sessions:

```
run
{
   allocate channel t1 type 'sbt_tape' parms
            'ENV=(TDPO_OPTFILE=/home/oracle/tdpo.opt)';
   allocate channel t2 type 'sbt_tape' parms
            'ENV=(TDPO_OPTFILE=/home/oracle/tdpo.opt)';

   backup
      filesperset 5
      format 'df_%t_%s_%p'
      (database);

  }
```

Tip: On AIX operating systems, do not use `/home/oracle11gr2/scripts/tdpo.opt` in your path. "oracle11gr2 " exceeds the 8-character string limit for users on AIX.

Example 3:

This restore script allocates one parallel connection to the Tivoli Storage Manager server:

```
run
{
allocate channel t1 type 'sbt_tape' parms
'ENV=(TDPO_OPTFILE=/home/oracle/tdpo.opt)';
restore database;
recover database;
alter database open;
}
```

Note:

1. The `allocate channel` entry is divided on two lines after the `parms` option to accommodate page formatting.
2. The Oracle database must be in mount mode for the restore to succeed.

Using the Duplex Copy function

With Data Protection for Oracle, you can use the Oracle Server Duplex backup feature to make up to four exact duplicate copies of a backup that can be stored on different backup media.

A different management class is required for each backup copy. By default, the primary management class is the default management class on the policy domain defined for the Data Protection for Oracle node.

Note: It might be necessary to define the Oracle parameter value (BACKUP_TAPE_IO_SLAVES=TRUE) in the `init.ora` file of the target database for Data Protection for Oracle to use the duplex copy feature. Refer to your Oracle documentation regarding the use of this Oracle parameter.

For example, to create four backup copies:

1. Specify the following option in the RMAN backup script:

   ```
   set duplex=4
   ```

2. Define the following options in the tdpo.opt file:
   - ***tdpo_mgmt_class_2***
   - ***tdpo_mgmt_class_3***
   - ***tdpo_mgmt_class_4***
3. Run the RMAN backup script.

The following backup behavior occurs:

- The first backup copy is bound to the default management class to which the node is registered.
- The second backup copy is bound to the management class defined by the ***tdpo_mgmt_class_2*** option.
- The third backup copy is bound to the management class defined by the ***tdpo_mgmt_class_3*** option.
- The fourth backup copy is bound to the management class defined by the ***tdpo_mgmt_class_4*** option.

Considerations

- The duplex copy feature does not use ***include*** statements. It only uses the management classes specified in the tdpo.opt file.
- You will receive an error message if you specify ***set duplex***=*4* in the RMAN backup script and do not define a sufficient number of ***tdpo_mgmt_class*** options in the tdpo.opt file.
- In order to place duplicate copies on different media:
  - Make sure the storage pool information for each backup copy group within the management classes is not the same.
  - Make sure backups from these different storage pools are not migrated to the same storage pool at a later time.
- Be aware that duplicate data will be sent across the network.
- Be aware that if you specify ***set duplex***=*4* and allocate *one* channel in the RMAN backup script, RMAN will start *four* sessions to the Tivoli Storage Manager server. Likewise, if you specify ***set duplex***=*4* and allocate *two* channels in the RMAN backup script, RMAN will start *eight* sessions to the Tivoli Storage Manager server.
- The duplex copy feature sends the backup copies simultaneously. If the backup destination is tape, the number of sessions will be multiples of the duplex value. As a result, make sure RMAN does not start more sessions than the maximum mount points allowed by the Tivoli Storage Manager server. The node definition option on the Tivoli Storage Manager server (***maxnummp***) determines the maximum number of mount points a client node is allowed to use on the Tivoli Storage Manager server during a backup operation. You can view the maximum mount points allowed by the Tivoli Storage Manager server for a particular node by entering the **query node** command from a Tivoli Storage Manager Administrative Client prompt:

  ```
  q node f=d
  ```

  See the appropriate *Tivoli Storage Manager Administrator's Reference* for more information regarding this option.

It is highly recommended that you review your current Oracle documentation regarding the duplex backup function.

Removing old backups

Data Protection for Oracle uses the Tivoli Storage Manager backup repository. Each database backup creates a new object with a unique name. Since these objects have unique names, they always remain active and never expire. This allows the Database Administrator (DBA) to control and coordinate copies removed from the Tivoli Storage Manager server with RMAN.

The Tivoli Storage Manager administrator must specify ***backdelete***=*yes* when registering your node in order for you to be able to delete backup objects.

Note: Make sure to use the same tdpo.opt file that was used for the original backup. This enables the backup objects to be found on the Tivoli Storage Manager server.

Example

A sample script for removing an old backup is provided.

To remove an old backup, issue this command from the RMAN prompt:

```
run
{
   allocate channel for delete type 'sbt_tape' parms
            'ENV=(TDPO_OPTFILE=/home/oracle/tdpo.opt)';

   change backupset backupset number delete;

}
```

See the Oracle RMAN manual for more information on the **change** command and its options.

Using the Tivoli Storage Manager scheduler with Data Protection for Oracle

You can use the Tivoli Storage Manager scheduler with Data Protection for Oracle to automate online backups of Oracle server databases. An example illustrates the use of the Tivoli Storage Manager Version 6.3 backup-archive client scheduler.

For the Tivoli Storage Manager scheduler to function correctly, the Tivoli Storage Manager backup–archive client must reside on the same machine as Data Protection for Oracle.

After Data Protection for Oracle has been registered to a Tivoli Storage Manager server and installed on the Oracle server, perform these steps:

1. On the Tivoli Storage Manager server:
   a. Define a schedule to run an AIX, HP-UX, Linux, or Solaris scheduler backup script (schedbkdb.scr) in the policy domain to which Data Protection for Oracle is registered.
   b. Associate the Data Protection for Oracle node to the defined schedule.
2. On the machine where Data Protection for Oracle is installed:
   a. Create a single `dsm.sys` file from which to associate nodes for your client, Data Protection for Oracle, and scheduled backups.

b. Create the scheduler backup script (schedbkdb.scr). This is the script that the Tivoli Storage Manager scheduler invokes directly.
c. Create a command script (mysched.scr). This is the script that contains the Oracle environment information and invokes the RMAN backup script.
d. Create the RMAN backup script (bkdb.scr). This is the script that actually performs the Oracle RMAN backup.
e. Start the scheduler.

Example: setting up a schedule

This example illustrates how to set up a schedule to automatically back up Oracle server databases.

For consistency, this procedure uses specific information. However, you can define a command file with any set of commands you choose. This allows you to use the same command file to define schedules on other Tivoli Storage Manager servers. All command information is presented as command-line interface entries.

This schedule in this procedure contains the following settings:

- The Data Protection for Oracle node name is *NodeA1*.
- The password for node name *NodeA1* is *PasswordA1*.
- The policy domain to which node name *NodeA1* is registered is *PolicyA1*.
- The schedule is a daily backup of an online Oracle database.
- The scheduled backup begins between 9:00 and 9:15 PM.

Part I: Setting up a schedule on the Tivoli Storage Manager server

Define a schedule on the Tivoli Storage Manager server to automatically run online backups of Oracle server databases.

To set up a schedule on the Tivoli Storage Manager server:

1. Define the following schedule on the Tivoli Storage Manager server. You can enter the command on the Tivoli Storage Manager server console or on an administrative client. The administrative client does not have to be running on the same system as the Tivoli Storage Manager server.

   ```
   define schedule PolicyA1 daily_orcbkup description="08Daily Online DB Backup"
   action=command objects="/usr/tivoli/tsm/client/oracle/sched/schedbkdb.scr"
   starttime=21:00 duration=15 durunits=minutes period=1 perunits=day
   dayofweek=any
   ```

   The following message must display before proceeding to the next step:

   ```
   ANR2500I Schedule daily_orcbkup defined in policy domain PolicyA1.
   ```

2. Issue the following command to associate the Data Protection for Oracle node to the backup schedule defined in step 1:

   ```
   define association PolicyA1 daily_orcbkup NodeA1
   ```

   The following message must display before proceeding to Part II:

   ```
   ANR2510I Node NodeA1 associated with schedule orc_dailybkup
            in policy domain PolicyA1.
   ```

   Summary:

   - A backup schedule is now defined on the Tivoli Storage Manager server.

- The backup schedule will run the scheduler backup script (`schedbkdb.scr`), which will run the command script (`mysched.scr`), which will run the RMAN backup script (`bkdb.scr`) located in the `/home/oracle/sched` directory.
- The backup is performed once a day around 9:00 PM.
- The backup schedule can start on any day of the week.
- You can run the Tivoli Storage Manager **query schedule** and **query association** commands to confirm that the schedule and node association are set correctly.

Part II: Setting up a schedule on the client machine (*NodeA1*)

Use this procedure to define a schedule on the client machine with the client node *NodeA1*.

This example assumes the following setup:

- The Tivoli Storage Manager backup-archive client is installed on *NodeA1* in the `/usr/tivoli/tsm/client/ba/bin` directory.
- Data Protection for Oracle is installed on *NodeA1* in the `/usr/tivoli/tsm/client/oracle/bin64` directory.
- An AIX operating system is used.

For best results, set the password expiration for the Data Protection for Oracle node (*NodeA1*) to *not* expire. Otherwise the password will become out of sync between Data Protection for Oracle and the scheduler. You can do this by specifying ***passwordaccess*** *generate*. However, if ***passwordaccess*** *prompt* is already specified, you can prevent password expiration by issuing the following command:

```
update node NodeA1 passexp=0
```

Scheduling Data Protection for Oracle backups with the Tivoli Storage Manager scheduler requires special configuration issues to be addressed. This procedure addresses this issue by creating a dsm.sys file from which to associate nodes for your client, Data Protection for Oracle, and scheduled backups:

To set up a schedule on the client machine with client node *NodeA1*:

1. Create a dsm.sys file in the `/usr/tivoli/tsm/client/ba/bin` directory (if one does not already exist) and add the following ***servername*** stanzas:
   a. Add a ***servername*** stanza for the file system backups associated with your Tivoli Storage Manager backup-archive client.

      For example:

      ```
      servername   TSMbackup
         commmethod   tcpip
         tcpserveraddress    site.xyzinc.com
         tcpport    1500
         nodename   client
         passwordaccess    generate
      ```

      The ***servername*** *TSMbackup* setting must be specified in the dsm.opt file associated with the Tivoli Storage Manager backup-archive client. The default directory location is `/usr/tivoli/tsm/client/ba/bin`.

   b. Add a ***servername*** stanza for the backups associated with Data Protection for Oracle.

      For example:

      ```
      servername   TSMOracle
         commmethod   tcpip
         tcpserveraddress     site.xyzinc.com
         tcpport    1500
      ```

```
   nodename   NodeA1
   passwordaccess    generate
   passworddir       /home/<oracle user>
```

Replace *<oracle user>* with the Oracle User ID of the target Oracle database instance.

The ***servername*** *TSMOracle* setting must be specified in the dsm.opt file associated with Data Protection for Oracle. The default directory location is `/usr/tivoli/tsm/client/oracle/bin64`. This dsm.opt file can have a unique name, such as dsmoracle.opt. Make sure the ***dsmi_orc_config*** option specifies the user options file (dsmoracle.opt in Step 1b) associated with Data Protection for Oracle. For example:

```
dsmi_orc_config /usr/tivoli/tsm/client/oracle/bin64/dsmoracle.opt
```

c. Add a ***servername*** stanza for the *scheduled* backups associated with Data Protection for Oracle.

For example:

```
servername   DPSched
   commmethod   tcpip
   tcpserveraddress    site.xyzinc.com
   tcpport    1500
   nodename   NodeA1
   passwordaccess    generate
   passworddir       /home/<oracle user>
```

Replace *<oracle user>* with the Oracle User ID of the target Oracle database instance.

2. Make sure there is a symbolic link to this dsm.sys file so that the file is available to the Tivoli Storage Manager API directory (`/usr/tivoli/tsm/client/api/bin64`).
3. Create the scheduler backup script (schedbkdb.scr) in the `/usr/tivoli/tsm/client/oracle/sched/` directory. This is the scheduler backup script that was defined for the scheduler in Step 1 in "Part I: Setting up a schedule on the Tivoli Storage Manager server" on page 41. This scheduler backup script will run the command script (mysched.scr), which will run the RMAN backup script (bkdb.scr). This is an example of the scheduler backup script (schedbkdb.scr):

```
#!/bin/ksh
su - OracleUser -c /home/oracle/sched/mysched.scr
```

4. Create the command script (`mysched.scr`) in the `/home/oracle/sched/` directory. A sample of the command script (`mysched.scr`) is provided: in the following example:

```
#!/bin/ksh
export ORACLE_HOME=/orc11g/app/oracle/product/11.2.0
export PATH=$ORACLE_HOME/bin:$PATH
rman target agnttest/agnttest@target rcvcat rman/rman@rman
cmdfile /home/oracle/sched/bkdb.scr msglog /home/oracle/sched/bkdb.log
```

You must place the command text, `rman target agnttest/agnttest@target rcvcat rman/rman@rman` and `cmdfile /home/oracle/sched/bkdb.scr msglog /home/oracle/sched/bkdb.log`, on the same line in this command script. The command text is placed on two lines in this example to accommodate page formatting.

5. Create the RMAN backup script (bkdb.scr) in the `/home/oracle/sched/` directory. This is an example of the RMAN backup script (bkdb.scr):

```
run {
allocate channel t1 type 'sbt_tape' parms
'ENV=(TDPO_OPTFILE=/home/oracle/sched/tdpo.opt)';
```

```
allocate channel t2 type 'sbt_tape' parms
'ENV=(TDPO_OPTFILE=/home/oracle/sched/tdpo.opt)';

backup
format 'df_%t_%s_%p_%u_%c'
(database); }
```

6. Login as the *root* user to the machine where Data Protection for Oracle is installed as node name *NodeA1*.
7. Start the scheduler in the **inittab**. Use the ***servername*** parameter to specify the correct stanza to use in the dsm.sys file:

   ```
   dsmc sched -servername=DPSched
   ```

   Data Protection for Oracle is now enabled for scheduled backups.

Querying backup objects

Use the **tdposync query** command to query the Tivoli Storage Manager server for information about objects that have been backed up.

When you issue the **tdposync query** command, information about a backup object is displayed, such as the size, date of backup, and whether the object has been compressed, encrypted, or deduplicated by the Tivoli Storage Manager client during the backup.

Related tasks

"Using data deduplication with Data Protection for Oracle"

Related reference

"**Query** command" on page 57

Using data deduplication with Data Protection for Oracle

You can use data deduplication with Data Protection for Oracle to reduce the amount of redundant data that is backed up to the Tivoli Storage Manager server.

Overview of data deduplication

Data deduplication is a method of reducing storage needs by eliminating redundant data

Two types of data deduplication are available with Tivoli Storage Manager: client-side data deduplication and server-side data deduplication.

Client-side data deduplication is a data deduplication technique that is used on the Tivoli Storage Manager API to remove redundant data during backup processing before the data is transferred to the Tivoli Storage Manager server. Using client-side data deduplication can reduce the amount of data that is sent over a local area network.

Server-side data deduplication is a data deduplication technique that is done by the server. The Tivoli Storage Manager server administrator can specify the data deduplication location (client or server) to use with the **DEDUP** parameter on the **REGISTER NODE** or **UPDATE NODE** server command.

Setting up Data Protection for Oracle for client-side data deduplication

You must edit the client options file before Data Protection for Oracle can use client-side data deduplication through the Tivoli Storage Manager API.

You can turn on client-side data deduplication by adding `DEDUPLICATION YES` to the `dsm.sys` file and by making sure that the deduplication prerequisites are met.

The Tivoli Storage Manager server administrator must enable data deduplication for the Data Protection for Oracle with the appropriate server command. For example:

```
UPDATE NODE ORACLE_NODE DEDUPLICATION=CLIENTORSERVER
```

The Tivoli Storage Manager server administrator must enable data deduplication on the storage pool where the Oracle data is stored with the following server command:

```
UPDATE STGPOOL BACKUP_POOL DEDUPLICATION=YES
```

For more information, see the Tivoli Storage Manager information center at http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3, and search on *API deduplication*.

After you have created backups with client-side data deduplication enabled, you can use the **tdposync query** command to verify that client deduplication occurred during the backup operation. For detailed statistics, you can also query the Tivoli Storage Manager server activity log for the total data reduction.

You can also use the performance monitor feature in the Tivoli Storage Manager Version 6.3 server to verify the percentage of data that has been deduplicated. The performance monitor feature is part of the Tivoli Storage Manager Administration Center. The data deduplication statistics are displayed graphically in the Performance GUI in the Administration Center.

The following example illustrates how you can set up the `dsm.sys` file on AIX to enable the performance monitor feature:

```
servername fvtseries2
tcps fvtseries11esx2.storage.usca.ibm.com
tcpp 1500
nodename apitest
*errorlogname /home/api/logs/tdperrs.log
errorlogname  /home/orc11r2/tdperrs.log
PERFMONTCPSERVERADDRESS jumboesx1.storage.usca.ibm.com
PERFMONTCPPORT 5129
```

Considerations:

- The **deduplication** and **enablelanfree** options are mutually exclusive. Therefore, you can only use either one option or the other, but not both options together.
- The **deduplication** and **enableclientencryptkey** options are also mutually exclusive. Therefore, you can only use either one option or the other, but not both options together.
- A local deduplication cache is an optimization that can reduce network traffic between the Tivoli Storage Manager server and the client. Client-side data deduplication can occur with or without it. Do not use the deduplication cache with Data Protection for Oracle for the following reasons:

  - The cache cannot be used when multiple processes, such as concurrent backups or Tivoli Storage Manager API applications, transfer content concurrently. Data Protection for Oracle backup operations that use multiple channels use multiple processes.
  - It is possible that the client deduplication cache can become out of sync with the server-deduplicated disk storage pool. This state can be the result of object expiration, file space deletion, and overflow to an associated tape storage pool. When the client cache contains entries that are no longer in the Tivoli Storage Manager server deduplicated pool, the cache is reset and the backup operations fails. The Tivoli Storage Manager API does not attempt the backup again.
- When Tivoli Storage Manager server expiration or a similar process that removes deduplicated data extents runs concurrently with a deduplicated backup, the backup might fail. Backup operations with client-side deduplication enabled fails with the following messages:
  - Return code=254
  - Error message: `ANS7899E The client referenced a deduplicated extent that does not exist on the TSM server.`

Related tasks

"Determining total data reduction"

Related reference

"**Query** command" on page 57

Determining total data reduction

You can determine the percentage of total data reduction by querying the Tivoli Storage Manager server activity log.

Look for message number ANU2526I, which displays the data deduplication statistics, as shown in the following example:

```
ANE4991I (Session: 67, Node: MACHINE_ORC) DP Oracle AIX ANU0599 TDP for Oracle: (5508): =>()
ANU2526I Backup details for backup piece /adsmorc//df_727444762_116_1 (database "orcl").
 Total bytes processed: 9961472. Deduplicated: Yes. Bytes after deduplication: 2272805.
 Deduplication reduction: 77.18%. Compressed: Yes. Bytes after compression: 52253. Compressed by: 97.70%.
 Encryption: None. LAN-Free: No. Total bytes sent: 52253. Total data reduction: 99.48%.
 Total processing time: 00:00:01. Throughput rate: 9728.00Kb/Sec. (SESSION: 67)
```

In the following example, the Oracle database backup piece size is 9,961,472 bytes. Then it was deduplicated and the number of bytes after deduplication is 2,272,805.

The total data reduction is calculated as follows:

- The percentage of data that is deduplicated is as follows:

  ```
  Deduplication reduction = (1 - 2272805 / 9961472 ) = 0.7718
  ```

- After data deduplication, the object was compressed. The number of bytes before compression is the number of bytes after deduplication. The data was compressed to 52,253 bytes. Therefore,

  ```
  Compressed by  = (1 - 52253 / 2272805) = 0.9770
  ```

- The total bytes sent to the server equals the number of bytes after compression. The formula for total data reduction is as follows:

  ```
  Total data reduction = (1 - bytes after compression / bytes processed)
  = (1 - 52253 / 9961472) = 0.9948
  ```

If there is no deduplication, the number of bytes after deduplication equals the number of bytes processed . If there is no compression, the number of bytes after compression equals the number of bytes after deduplication.

If you want to find out data reduction across multiple backup pieces, you can add up the numbers and calculate the ratios.

You can also use the performance monitor feature in the Tivoli Storage Manager Version 6.3 server to verify the percentage of data that has been deduplicated. The performance monitor feature is part of the Tivoli Storage Manager Administration Center. The data deduplication statistics are displayed graphically in the Performance GUI in the Administration Center.

The following example illustrates how you can set up the `dsm.sys` file on AIX to enable the performance monitor feature:

```
servername fvtseries2
tcps fvtseries11esx2.storage.usca.ibm.com
tcpp 1500
nodename apitest
*errorlogname /home/api/logs/tdperrs.log
errorlogname  /home/orc11r2/tdperrs.log
PERFMONTCPSERVERADDRESS jumboesx1.storage.usca.ibm.com
PERFMONTCPPORT 5129
```

For more information about deduplication statistics, see the topic "Querying a storage pool for statistics about data deduplication" in the Tivoli Storage Manager Information Center at http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3.

Chapter 5. Data Protection for Oracle reference

Use Data Protection for Oracle commands and utilities to protect Oracle Server data.

Data Protection for Oracle utilities

Use the **tdpoconf** and **tdposync** utilities to set up and maintain Data Protection for Oracle. These utilities are located in the directory where Data Protection for Oracle is installed.

The Data Protection for Oracle utilities help you do the following tasks:

- Use the **tdpoconf** utility for password maintenance and general Data Protection for Oracle setup and maintenance.
- Use the **tdposync** utility to delete the Oracle backups on the Tivoli Storage Manager server, which are not in the RMAN catalog or Oracle control file. This situation occurs when backups have inadvertently not been deleted from the Tivoli Storage Manager server.
- Use the **tdposync** utility to query backed up objects on the Tivoli Storage Manager server.

Command line syntax and characteristics

The command line syntax for the Data Protection for Oracle utilities is provided.

The Data Protection for Oracle utilities use the following command line syntax:

```
tdpoconf <command> <0 or more optional parameters>
tdposync <command> <0 or more optional parameters>
```

The command line parameters have the following characteristics:

- Minimum abbreviations for keywords are indicated in upper case.
- Optional parameters begin with a dash (-).
- Optional parameters can appear in any order.
- Some keyword parameters require a value separated by the equal sign (=).
- If a parameter requires more than one value, the values are separated with commas.
- A space separates the invocation from the command and the command from any optional parameters.
- Each parameter is separated from others by a space.
- If a parameter value includes spaces, the entire parameter must be enclosed in double quotes.

© Copyright IBM Corp. 1998, 2011

TDPOCONF

This utility provides setup tasks to ease the configuration of Data Protection for Oracle. The utility uses the `tdpo.opt` file in the installation directory to centralize information for setup purposes.

Two commands are available using the **tdpoconf** utility:

- **PASSWord**
- **SHOWENVironment**

A description of these two commands and their parameters follows.

Password command

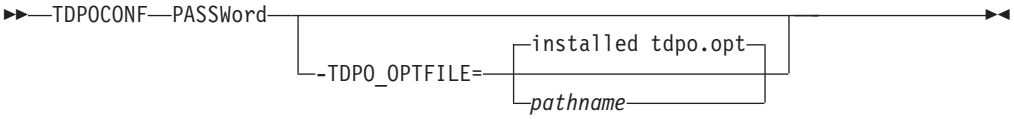
Use the **password** command to create a new password or change an existing password on the Tivoli Storage Manager server. You are prompted to enter both the old and new passwords when you invoke this utility.

Be aware of the following requirements based on the value of the ***passwordaccess*** setting in the dsm.sys file:

passwordaccess *prompt*
: Run the **tdpoconf password** command as the *root* user. This command creates an encrypted password file, *TDPO.Nodename*. The *Nodename* value will be the value specified by the ***tdpo_node*** option in the Data Protection for Oracle options file specified with the ***TDPO_OPTFILE*** variable. This file is located in the directory specified by the ***tdpo_pswdpath*** option. If the ***tdpo_pswdpath*** option is not specified, the *TDPO.Nodename* file is placed in the Data Protection for Oracle installation directory. Make sure that the *TDPO.Nodename* file can be read by the Oracle user that performs the backup.

passwordaccess *generate*
: Run the **tdpoconf password** command as the Oracle user. The password is placed in the file, *TSM.PWD*, and is owned by the Oracle user. This *TSM.PWD* file is created in the directory specified by the ***passworddir*** option defined in the dsm.sys file. Do not specify the ***tdpo_node*** option in the tdpo.opt file. Data Protection for Oracle uses the value of the ***nodename*** option specified in the dsm.sys file. If the ***tdpo_pswdpath*** option is specified in the tdpo.opt file, it is ignored. See the description of the ***tdpo_pswdpath*** option in "Available Data Protection for Oracle options" on page 24 for more information.

Syntax



Optional parameters

-TDPO_OPTFILE=*pathname*
: This parameter specifies the fully qualified path name to the tdpo.opt file. If you choose not to specify this option, the default path is used.

Example

This is an output example of the **tdpoconf password** command:

```
************************************************************
*  IBM Tivoli Storage Manager for Databases Utility        *
*  Password file initialization/update program             *
*                                                          *
************************************************************

Please enter current password:

Please enter new password:

Please reenter new password for verification:

ANU0260I Password successfully changed.
```

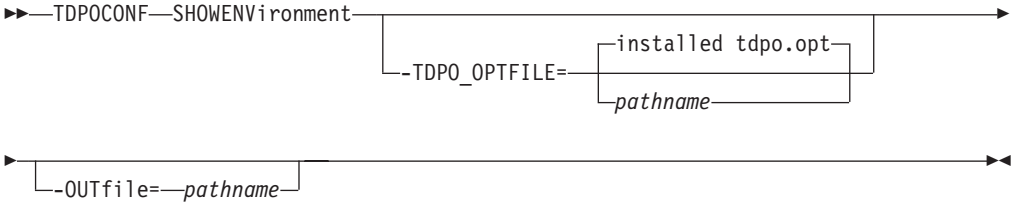
Showenvironment command

Use the **showenvironment** command to query the Tivoli Storage Manager server using the options set in *–TDPO_OPTFILE*, the tdpo.opt file in the default installation directory, or the default values set by Data Protection for Oracle.

The screen output displays information about the Tivoli Storage Manager API and Tivoli Storage Manager server. This command is useful when troubleshooting Data Protection for Oracle setup. If, for example, the password file is not initialized properly, **tdpoconf showenvironment** reports this error immediately and prevents complications that can arise if this error were to go undetected.

Note: For initial setup, it is recommended that you direct the output to a file with the *–outfile* option to ensure that the desired environment is set correctly before using RMAN.

Syntax



Optional parameters

-TDPO_OPTFILE=*pathname*
This parameter specifies the fully qualified path name to the tdpo.opt file. This is the options file that is used by the utilities and the Data Protection for Oracle library.

-OUTfile=*pathname*
This parameter specifies the fully qualified path name to the output file. The formatted text of this file is the same content that appears as output to the screen.

Example

Below is an output example of the **tdpoconf showenvironment** command:

```
Data Protection for Oracle Information
 Version:             6
 Release:             3
 Level:               0
```

```
 Sublevel:             0
 Platform:             64bit TDPO Linux86-64

Tivoli Storage Manager Server Information
 Server Name:          TSMSERVER_ORC
 Server Address:       TSMSERVER
 Server Type:          Linux/x86_64
 Server Port:          1500
 Communication Method: TCP/IP

Session Information
 Owner Name:
 Node Name:            NODE_ORC
 Node Type:            TDPO Linux86-64
 DSMI_DIR:             /opt/tivoli/tsm/client/api/bin64
 DSMI_ORC_CONFIG:      /opt/tivoli/tsm/client/oracle/bin64/dsm.opt
 TDPO_OPTFILE:         /opt/tivoli/tsm/client/oracle/bin64/tdpo.opt
 Compression:          FALSE
 License Information:  License file exists and contains valid license data.
```

Note: The `Server Name` value above identifies the Tivoli Storage Manager server *stanza* in the dsm.sys file, not the actual name of the Tivoli Storage Manager server.

TDPOSYNC

The **tdposync** utility checks for items on the Tivoli Storage Manager server that are not in the RMAN catalog or Oracle control file. With this utility, you can repair these discrepancies between the Tivoli Storage Manager server and the RMAN catalog or Oracle control file. By removing unwanted objects in Tivoli Storage Manager storage, you can reclaim space on the server.

Attention: Deleted files and inactive files cannot be restored! When using this utility to delete files, ensure that you do not log on under the wrong node name, query a different database than intended, and delete files in error. Double-check the node name listed at the top of the PICK window. See "Optional parameters" on page 54 and "PICK Window" on page 56 for further details.

When you run an RMAN deletion script, entries are deleted in the RMAN recovery catalog or Oracle control file before confirmation from the Tivoli Storage Manager server. In cases where objects are not found on the Tivoli Storage Manager server, RMAN tries to delete backup sets from the Tivoli Storage Manager server and fails. However, the entries in the RMAN catalog or control file for these objects are still removed. When this removal occurs, RMAN can no longer identify these backups through the catalog even or control file even though the file still exists on the Tivoli Storage Manager server. This utility therefore synchronizes the contents of the servers.

When the RMAN catalog or control file contains backups marked as expired, RMAN still considers these objects as existing. If you run the **tdposync** untility against these objects, it recognizes these objects in the RMAN catalog or control file and on the Tivoli Storage Manager server and considers them to be in sync. Therefore, you must delete these objects from the RMAN catalog or control file for them to be deleted from the Tivoli Storage Manager server. Use the Oracle **crosscheck** command to verify whether the backups exist. Then, use the Oracle **delete expired** command to remove their record from the RMAN catalog or control file.

When you start **tdposync**, the following processing takes place:

1. Prompts you for the RMAN catalog owner ID or Oracle database user name, password, and connect string
2. Gathers information for the Oracle servers
3. Queries the Oracle backup catalog and the Tivoli Storage Manager server
4. Displays formatted output to the screen (files that exist on Tivoli Storage Manager but not in the RMAN catalog or Oracle control file)
5. Prompts you to take one of the following actions:
   - Delete any files found causing the discrepancy
   - Delete all files
   - Exit the program without deleting files from the Tivoli Storage Manager server

TDPOSYNC considerations

The following information must be considered before using the **tdposync** command:

- Resynchronize Oracle catalogs with the target databases before running the **tdposync syncdb** command. First, connect to the target database and the catalog database. The following is an example:

  ```
  $ rman target xxx/yyy@targetdb  rcvcat xxx/yyy@catalogdb
  ```

  When you are connected to both databases, type `resync catalog` at the RMAN prompt.

- If the information for **sqlplus** that you provide to **tdposync** is incorrect (such as logon, password, or connect string information), **sqlplus** stops at its logon screen. You must log on again at the prompt by using the RMAN catalog owner ID, password, and connect string. For example:

  ```
  login/password@connectstring
  ```

  where `connectstring` represents the Oracle database in which to connect. The `connectstring` is also sometimes referred to as the Transparent Network Substrate (TNS) alias. When the correct input is entered, **tdposync** proceeds.

- By default, Data Protection for Oracle prompts you to synchronize with one Oracle catalog at a time. However, if you use multiple Oracle catalogs to back up multiple target databases to the same file space, the same node name, and the same owner name on the same Tivoli Storage Manager server, you must use **–numcatalogs**=*number*. This action is necessary so that **tdposync** has all the information to correctly query both Oracle and Tivoli Storage Manager.

  Similarly, if you use Oracle control files to back up multiple target databases to the same file space, the same node name, and the same owner name on the same Tivoli Storage Manager server, you must use **-numorinstances**=*number*.

  If, for example, you back up only *one* target database by using two catalogs, *do not* specify this option. However, if you back up *two* target databases by using two catalogs (one catalog for each) to the same Tivoli Storage Manager server under the same file space, node name, and owner name, you must specify **numcatalogs**. If you fail to provide information for the second target database (by not specifying two catalogs), that database is displayed as eligible for deletion.For more information , see “Optional parameters” on page 54.

  Attention: Failure to provide all pertinent and correct information can result in erroneous output. To prevent the erroneous output, see the next consideration.

- If you have more than one Oracle database, back up each Oracle target database to its own file space on the Tivoli Storage Manager server. To back up each Oracle target database to its own file space, use the `tdpo_fs` option in the

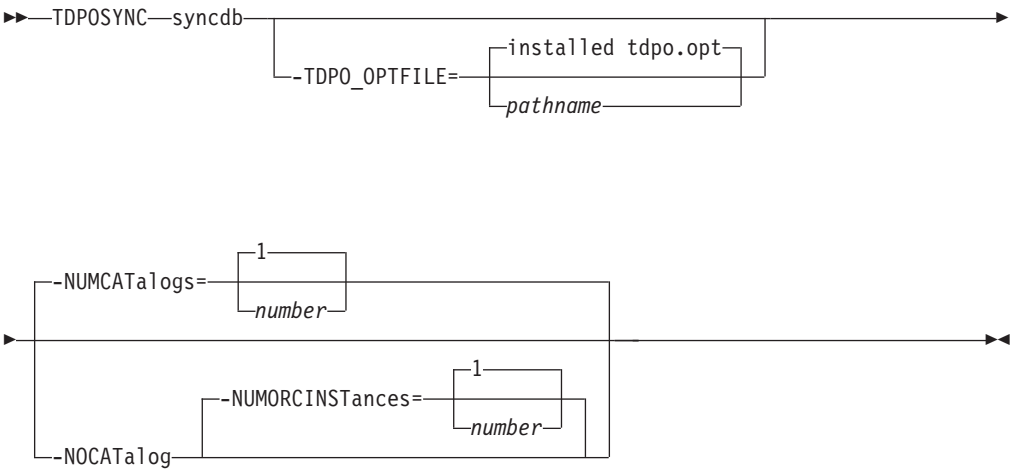
tdpo.opt file. For best results, use a separate Data Protection for Oracle options file for *each* database that you back up to Tivoli Storage Manager. In this way, it is only necessary to synchronize one catalog at a time (once for each target database), thus minimizing the display of wrong information in the PICK window.

- Make sure to use the same tdpo.opt file that was used for the original backup.

Syncdb command

This command synchronizes Oracle catalog databases or the Oracle control file with the Tivoli Storage Manager server. This command is the only command that is available to the **tdposync** utility.

Syntax



Optional parameters

-TDPO_OPTFILE=*pathname*

This parameter specifies the fully qualified path name to the tdpo.opt file. This file is the options file that is used by the utilities and the Data Protection for Oracle library. This file contains the information for the Tivoli Storage Manager server name and address that **tdposync** needs for synchronizing.

Note: For **syncdb TDPO_OPTFILE**, you must specify the same options file values that were used to perform the original backup operations.

-NUMCATalogs=*number*

This parameter specifies the number of Oracle catalog databases that you want to synchronize and prompts you for information for each catalog that exists on your node.

Specify this option only when you use *multiple* Oracle catalogs to back up multiple target databases to the same Tivoli Storage Manager server under the same file space, node name, and owner name.

According to the number you specify for **-numcatalogs**, you are prompted for the user name, password, and connect string for each. If you do not specify **-numcatalogs**, the default is 1, and you are prompted only once.

For each catalog, you are prompted for the following information:

- Catalog # User Name:

- Catalog # Password:
- Catalog # Connect String:

You are also prompted for the following date information to narrow your search:

- From Date: (MM/DD/YYYY)
- To Date: (MM/DD/YYYY)

If no dates are specified, Data Protection for Oracle displays all objects that are not in sync.

-NOCATalog
This parameter specifies that the **tdposync** utility uses the backup history information that is stored in the Oracle control file rather than a catalog database to reconcile the Tivoli Storage Manager database with the RMAN backup history.

-NUMORCINSTances=*number*

This parameter specifies the number of Oracle instances that you want to synchronize, and prompts you for information for each instance that exists on your node.

Specify this option only when you use multiple Oracle instances to back up multiple target databases to the same Tivoli Storage Manager server under the same file space, node name, and owner name.

According to the number you specify for **-numorcinstances**, you are prompted for the user name, password, and connect string for each instance. If you do not specify a value for **-numorcinstances**, the default is 1, and you are prompted only once.

For each Oracle instance, you are prompted for the following information:

- Oracle Database # User Name
- Oracle Database # Password
- Oracle Database # Connect String

You are also prompted for the following date information to narrow your search:

- From Date: (MM/DD/YYYY)
- To Date: (MM/DD/YYYY)

If no dates are specified, Data Protection for Oracle displays all objects that are not in sync.

Example

This sample output is an example of the **tdposync syncdb** command for using the RMAN catalog to synchronize the Tivoli Storage Manager database with the RMAN backup history:

```
Command: TDPOSYNC syncdb

Catalog 1 User Name: rman

Catalog 1 Password: rman

Catalog 1 Connect String: rman
```

```
From Date (MM/DD/YYYY): 01/01/2007

To Date (MM/DD/YYYY): 01/11/2007
```

This sample output is an example of the **tdposync syncdb** command for using the Oracle control file to synchronize the Tivoli Storage Manager database with the RMAN backup history.

```
Command: TDPOSYNC syncdb -nocatalog -numorcinstances=2

Output:
Oracle Database 1 User Name: OrcUser1

Oracle Database 1 Password: OrcUser1pw

Oracle Database 1 Connect String: Oracle_DB_A


Oracle Database 2 User Name: OrcUser2

Oracle Database 2 Password: OrcUser2pw

Oracle Database 2 Connect String: Oracle_DB_B

From Date (01/01/1990):

To Date (07/07/2010):
```

PICK Window:

The PICK window provides information to help you decide if the files that are displayed are out of synchronization with the Oracle catalog or control file.

The following information is provided:

- The node with which you are querying the Tivoli Storage Manager server
- The date of the file backup
- The size of the backup
- The backup name (`/fs//backup file name`)

Attention: Use caution when selecting files for deletion. If you are unsure that the files in question are really out of synchronization, do further research before deleting them. Once you delete files, they *cannot* be restored.

Example

This is an example output of the PICK window:

```
Node Name: AGENT_NODE
  Owner Name: oracle10g

               Backup Date            Size        Backup Name
        ---------------------------------------------------------------
     1. | 01/09/2007  09:19:59       108.01MB    /adsmorc//1kc2cnfv_1_1
     2. | 01/02/2007  11:36:20       56.25MB     /adsmorc//4kc3cnfv_1_1
     3. | 01/02/2007  07:14:30       102.00MB    /adsmorc//4qcgdhfr_1_1
     4. | 01/02/2007  07:21:38       78.10MB     /adsmorc//4ocf8999_1_1
     5. | 01/09/2007  11:00:11       10.99MB     /adsmorc//4ocf8999_1_2
     6. | 01/09/2007  11:00:12       32.07MB     /adsmorc//4ocf8999_1_3
     7. | 01/09/2007  11:00:13       623.90MB    /adsmorc//4rch25jk_1_1
     8. | 01/09/2007  11:00:14       441.61MB    /adsmorc//4rch25jk_1_2
     9. | 01/09/2007  11:00:15       10.18MB     /adsmorc//4rch25jk_1_3
        |
        |
        |
        0--------10-------20-------30-------40-------50-------60-------70
<U>=Up  =Down  <T>=Top  <B>=Bottom  <R>=Right  <L#>=Left
<G#>=Goto Line #  <#>=Toggle Entry  <+>=Select All  <->=Deselect All
<#:#+>=Select A Range <#:#->=Deselect A Range  <O>=Ok  <C>=Cancel
pick>
```

Files selected for deletion are marked by a plus (+). To delete selected files:

1. Enter **OK** at the PICK prompt.

   A warning message appears to confirm deletion of the selected files.
2. Enter **Yes** to delete the selected files from the Tivoli Storage Manager server.

Attention: The deletion process is irreversible. Use caution when selecting files for deletion.

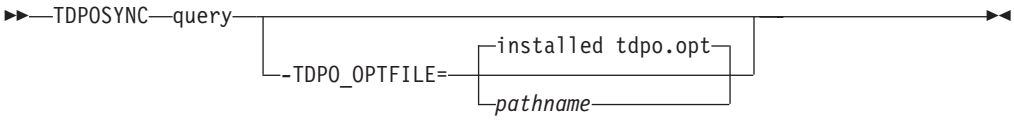
Query command

Use this command to query the Tivoli Storage Manager server for information about objects that have been backed up. You can obtain information such as whether an object has been compressed, encrypted, or deduplicated by the client during a backup operation.

The **query** command uses the options set in the **-TDPO_OPTFILE** parameter, the `tdpo.opt` file in the default installation directory, or the default values set by Data Protection for Oracle to query the Tivoli Storage Manager server.

When you issue the **tdposync query** command, you are prompted to enter date range for the query. The screen output displays information about the objects that were backed up to the Tivoli Storage Manager server between the start and end dates that you specified.

Syntax



Optional parameters

-TDPO_OPTFILE *=pathname*

This parameter specifies the fully qualified path name to the `tdpo.opt` file. This file is the options file that is used by the utilities and the Data Protection for

Oracle library. The file contains the information for the Tivoli Storage Manager server and the server address that **tdposync** command must use for synchronizing.

When you specify the **query TDPO_OPTFILE** command, you must specify the same options file values that were used for the original backup operations. If you do not specify the **TDPO_OPTFILE** path, the default value in the default Oracle installation path (`/usr/tivoli/tsm/client/oracle/bin64/tdpo.opt`) is used.

Description of the output fields

Name Object name on the Tivoli Storage Manager server; for instance, `/fs/hl/ll`.

Owner
The name of the user who backed up the object.

This field is empty if the user is root.

Size The size of the object size on the Tivoli Storage Manager server.

Creation Date / Time
The date and time the object was backed up.

Compressed
Displays whether an object was compressed during the backup operation.

Encryption Type
Displays the type of encryption that was used during the backup operation. The possible values are as follows:

None The object was not encrypted.

AES-128
The object was encrypted by using AES-128 encryption.

DES-56
The object was encrypted by using DES-56 encryption.

Client-deduplicated
Displays whether an object underwent client-side data deduplication.

Examples

Example 1
Query the Tivoli Storage Manager server for information about objects that have been backed up.

Command: `tdposync query`

Output:

```
IBM Tivoli Storage Manager for Databases:
Data Protection for Oracle
Version 6, Release 3, Level 0.0
(C) Copyright IBM Corporation 1997, 2011. All rights reserved.

From Date (01/01/1990):

To Date (07/08/2010):

Backup Object Information
-------------------------

Name ............................... /adsmorc//df_722435657_35_1
Owner...............................
Size ............................... 2,010 KB
Creation Date / Time ............... 07/08/2010 10:08:20
Compressed ......................... Yes
Encryption Type .................... None
Client-deduplicated ................ No

Backup Object Information
-------------------------

...
```

Example 2

When you issue the **tdposync query** command, the entire list of backup object information is printed to the command prompt window without page separators, scrolling, or canceling capability. Redirect the output of the query to a file and find out the encryption type that was used for the backups from the previous week.

Command: `echo -e "<from date>\n<to date>\n" | tdposync query > out.txt` where the "from" and "to" dates specify last week's date range.

Open the file `out.txt` with a text editor and search for *Encryption Type* to determine the type of encryption that was used.

Example 3

Determine the data deduplication reduction for a particular node by querying the Tivoli Storage Manager server activity log for the ANU2526I message.

Related tasks

"Using data deduplication with Data Protection for Oracle" on page 44

Appendix. Accessibility features for the Tivoli Storage Manager product family

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in the Tivoli Storage Manager family of products:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The Tivoli Storage Manager Information Center, and its related publications, are accessibility-enabled. The accessibility features of the information center are described at http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3/topic/com.ibm.help.ic.doc/iehs36_accessibility.html.

Keyboard navigation

On Windows, the Tivoli Storage Manager product family follows Microsoft conventions for all keyboard navigation and access. Drag and Drop support is managed using the Microsoft Windows Accessibility option known as MouseKeys. For more information about MouseKeys and other Windows accessibility options, please refer to the Windows online help (keyword: MouseKeys).

On other operating systems, these products follow the operating-system conventions for keyboard navigation and access.

Vendor software

The Tivoli Storage Manager product family includes certain vendor software that is not covered under the IBM license agreement. IBM makes no representation about the accessibility features of these products. Contact the vendor for the accessibility information about its products.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

© Copyright IBM Corp. 1998, 2011

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

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

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

© Copyright IBM Corp. 1998, 2011

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

Licensees of this program who want to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information 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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample

programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Intel, Itanium, and Pentium are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

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

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

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

Glossary

This glossary includes terms and definitions for IBM Tivoli Storage Manager and IBM Tivoli Storage FlashCopy Manager products.

To view glossaries for other IBM products, go to http://www.ibm.com/software/globalization/terminology/.

The following cross-references are used in this glossary:

- *See* refers the reader from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- *See also* refers the reader to a related or contrasting term.

A

absolute mode
In storage management, a backup copy-group mode that specifies that a file is considered for incremental backup even if the file has not changed since the last backup. See also *modified mode*.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights. For example, an access control list is associated with a file that identifies the users who can access that file and their access rights.

access mode
An attribute of a storage pool or a storage volume that specifies whether the server can write to or read from the storage pool or storage volume. The access mode can be read/write, read-only, or unavailable. Volumes in primary storage pools can also have an access mode of destroyed. Volumes in copy storage pools can also have an access mode of offsite.

acknowledgment
The transmission of acknowledgment characters as a positive response to a data transmission.

ACL See *access control list*.

activate
To validate the contents of a policy set and then make it the active policy set.

active-data pool
A named set of storage pool volumes that contain only active versions of client backup data.

active file system
A file system to which space management has been added. With space management, tasks for an active file system include automatic migration, reconciliation, selective migration, and recall. Contrast with *inactive file system*.

active policy set
The activated policy set that contains the policy rules in use by all client nodes that are assigned to the policy domain. See also *policy domain* and *policy set*.

active version
The most recent backup copy of a file stored. The active version of a file cannot be deleted until a backup process detects that the user has either replaced the file with a newer version or has deleted the file from the file server or workstation. Contrast with *inactive version*.

activity log
A log that records normal activity messages that are generated by the server. These messages include information about server and client operations, such as the start time of sessions or device I/O errors.

adaptive subfile backup
A type of backup that sends only changed portions of a file to the server, instead of sending the entire file. Adaptive subfile backup reduces network traffic and increases the speed of the backup.

administrative client
A program that runs on a file server, workstation, or mainframe that administrators use to control and monitor the Tivoli Storage Manager server. Contrast with *backup-archive client*.

administrative command schedule
A database record that describes the

© Copyright IBM Corp. 1998, 2011

planned processing of an administrative command during a specific time period. See also *client schedule*.

administrative privilege class
See *privilege class*.

administrative session
A period of time during which an administrator user ID communicates with a server to perform administrative tasks. Contrast with *client node session*.

administrator
A user who is registered to the server as an administrator, and who is authorized to perform tasks and issue commands through the assignment of an administrative privilege class.

Advanced Program-to-Program Communication (APPC)
An implementation of the SNA LU 6.2 protocol that allows interconnected systems to communicate and share the processing of programs.

agent node
A client node that has been granted proxy authority to perform operations on behalf of another client node, which is the target node.

aggregate
An object, stored in one or more storage pools, consisting of a group of logical files that are packaged together. See also *logical file* and *physical file*.

aggregate data transfer rate
A performance statistic that indicates the average number of bytes that were transferred per second while processing a given operation.

APPC See *Advanced Program-to-Program Communication*.

application client
A program that is installed on a system to protect an application. The Tivoli Storage Manager server provides backup services to an application client.

archive
To copy programs, data, or files to other storage media, usually for long-term storage or security. Contrast with *retrieve*.

archive copy
A file or group of files that was archived to server storage.

archive copy group
A policy object containing attributes that control the generation, destination, and expiration of archived files.

archive-retention grace period
The number of days that the storage manager retains an archived file when the server is unable to rebind the file to an appropriate management class. See also *bind*.

association
(1) The defined relationship between a client node and a client schedule. An association identifies the name of a schedule, the name of the policy domain to which the schedule belongs, and the name of a client node that performs scheduled operations.

(2) On a configuration manager, the defined relationship between a profile and an object such as a policy domain. Profile associations define the configuration information that is distributed to a managed server when it subscribes to the profile.

audit To check for logical inconsistencies between information that the server has and the actual condition of the system. The storage manager can audit information about items such as volumes, libraries, and licenses. For example, when a storage manager audits a volume, the server checks for inconsistencies between information about backed-up or archived files that are stored in the database and the actual data that are associated with each backup version or archive copy in server storage.

authentication
The process of checking a user's password before permitting user access to the Tivoli Storage Manager server. Authentication can be turned on or off by an administrator with system privilege.

authentication rule
A specification that another user can use to either restore or retrieve files from storage.

authority
The right to access objects, resources, or functions. See also *privilege class*.

authorization rule
A specification that permits another user to either restore or retrieve a user's files from storage.

authorized user
A user who has administrative authority for the Tivoli Storage Manager client on a workstation. This user changes passwords, performs open registrations, and deletes file spaces.

AutoFS
See *automounted file system*.

automatic detection
A feature that detects, reports, and updates the serial number of a drive or library in the database when the path from the local server is defined.

automatic migration
The process that is used to automatically move files from a local file system to storage, based on options and settings that are chosen by a root user on a workstation. See also *threshold migration* and *demand migration*.

automatic reconciliation
The process that is used to reconcile file systems at regular intervals. The intervals are set by a user with root user authority. See also *reconciliation*.

automounted file system (AutoFS)
A file system that is managed by an automounter daemon. The automounter daemon monitors a specified directory path, and automatically mounts the file system to access data.

B

backup-archive client
A program that runs on a workstation or file server and provides a means for users to back up, archive, restore, and retrieve files. Contrast with *administrative client*.

backup copy group
A policy object containing attributes that control the generation, destination, and expiration of backup versions of files. A backup copy group belongs to a management class.

backup-retention grace period
The number of days the storage manager retains a backup version after the server is unable to rebind the file to an appropriate management class.

backup set
A portable, consolidated group of active versions of backup files that are generated for a backup-archive client.

backup set collection
A group of backup sets that are created at the same time and which have the same backup set name, volume names, description, and device classes. The server identifies each backup set in the collection by its node name, backup set name, and file type.

backup version
A file or directory that a client node backed up to server storage. More than one backup version can exist in server storage, but only one backup version is the active version. See also *active version* and *inactive version*.

bind To associate all versions of a file with a management class name. See *rebind*.

bindery
A database that consists of three system files for a NetWare server. The files contain user IDs and user restrictions.

C

cache To place a duplicate copy of a file on random access media when the server migrates a file to another storage pool in the hierarchy.

cache file
A snapshot of a logical volume created by Logical Volume Snapshot Agent. Blocks are saved immediately before they are modified during the image backup and their logical extents are saved in the cache files.

CAD See *client acceptor*.

central scheduler
A function that permits an administrator to schedule client operations and administrative commands. The operations can be scheduled to occur periodically or on a specific date. See *client schedule* and *administrative command schedule*.

client A software program or computer that requests services from a server.

client acceptor
An HTTP service that serves the applet for the web client to web browsers. On Windows systems, the client acceptor is installed and run as a service. On AIX, UNIX, and Linux systems, the client acceptor is run as a daemon, and is also called the *client acceptor daemon* (CAD).

client acceptor daemon (CAD)
See *client acceptor*.

client domain
The set of drives, file systems, or volumes that the user selects to back up or archive data, using the backup-archive client.

client node
A file server or workstation on which the backup-archive client program has been installed, and which has been registered to the server.

client node session
A session in which a client node communicates with a server to perform backup, restore, archive, retrieve, migrate, or recall requests. Contrast with *administrative session*.

client options file
An editable file that identifies the server and communication method, and provides the configuration for backup, archive, hierarchical storage management, and scheduling.

client option set
A group of options that are defined on the server and used on client nodes in conjunction with client options files.

client-polling scheduling mode
A method of operation in which the client queries the server for work. Contrast with *server-prompted scheduling mode*.

client schedule
A database record that describes the planned processing of a client operation during a specific time period. The client operation can be a backup, archive, restore, or retrieve operation, a client operating system command, or a macro. See also *administrative command schedule*.

client/server
Pertaining to the model of interaction in distributed data processing in which a program on one computer sends a request to a program on another computer and awaits a response. The requesting program is called a client; the answering program is called a server.

client system-options file
A file, used on AIX, UNIX, or Linux system clients, containing a set of processing options that identify the servers to be contacted for services. This file also specifies communication methods and options for backup, archive, hierarchical storage management, and scheduling. This file is also called the dsm.sys file. See also *client user-options file*.

client user-options file
A file that contains the set of processing options that the clients on the system use. The set can include options that determine the server that the client contacts, and options that affect backup operations, archive operations, hierarchical storage management operations, and scheduled operations. This file is also called the dsm.opt file. For AIX, UNIX, or Linux systems, see also *client system-options file*.

closed registration
A registration process in which only an administrator can register workstations as client nodes with the server. Contrast with *open registration*.

collocation
The process of keeping all data belonging to a single-client file space, a single client node, or a group of client nodes on a minimal number of sequential-access volumes within a storage pool. Collocation can reduce the number of volumes that must be accessed when a large amount of data must be restored.

collocation group
A user-defined group of client nodes whose data is stored on a minimal number of volumes through the process of collocation.

commit point
A point in time when data is considered consistent.

Common Programming Interface for Communications (CPI-C)
A call-level interface that provides a consistent application programming interface (API) for applications that use program-to-program communications. CPI-C uses LU 6.2 architecture to create a set of interprogram services that can establish and end a conversation, send and receive data, exchange control information, and notify a partner program of errors.

communication method
The method by which a client and server exchange information. See also *Transmission Control Protocol/Internet Protocol*.

communication protocol
A set of defined interfaces that permit computers to communicate with each other.

compression
A function that removes repetitive characters, spaces, or strings of characters from the data being processed and replaces the repetitive characters with control characters. Compression reduces the amount of storage space that is required for the data.

configuration manager
A server that distributes configuration information, such as policies and schedules, to managed servers according to their profiles. Configuration information can include policy and schedules. See also *managed server* and *profile*.

conversation
A connection between two programs over a session that allows them to communicate with each other while processing a transaction.

copy backup
A full backup in which the transaction log files are not deleted so that backup procedures that use incremental or differential backups are not disrupted

copy group
A policy object containing attributes that control how backup versions or archive copies are generated, where backup versions or archive copies are initially located, and when backup versions or archive copies expire. A copy group belongs to a management class. See also *archive copy group*, *backup copy group*, *backup version*, and *management class*.

copy storage pool
A named set of volumes that contain copies of files that reside in primary storage pools. Copy storage pools are used only to back up the data that is stored in primary storage pools. A copy storage pool cannot be a destination for a backup copy group, an archive copy group, or a management class (for space-managed files). See also *primary storage pool* and *destination*.

CPI-C See *Common Programming Interface for Communications*.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

damaged file
A physical file in which Tivoli Storage Manager has detected read errors.

data access control mode
A mode that controls whether a command can access a migrated file, see a migrated file as zero-length, or receive an input/output error if it attempts to access a migrated file. See also *execution mode*.

database backup series
One full backup of the database, plus up to 32 incremental backups made since that full backup. Each full backup that is run starts a new database backup series. A number identifies each backup series.

database snapshot
A complete backup of the entire database to media that can be taken off-site. When a database snapshot is created, the current database backup series is not interrupted. A database snapshot cannot have incremental database backups associated with it. See also *database backup series*. Contrast with *full backup*.

data deduplication
A method of reducing storage needs by eliminating redundant data. Only one instance of the data is retained on storage

media. Other instances of the same data are replaced with a pointer to the retained instance.

data manager server
A server that collects metadata information for client inventory and manages transactions for the storage agent over the local area network. The data manager server informs the storage agent with applicable library attributes and the target volume identifier.

data mover
A device that moves data on behalf of the server. A network-attached storage (NAS) file server is a data mover.

data storage-management application-programming interface (DSMAPI)
A set of functions and semantics that can monitor events on files, and manage and maintain the data in a file. In an HSM environment, a DSMAPI uses events to notify data management applications about operations on files, stores arbitrary attribute information with a file, supports managed regions in a file, and uses DSMAPI access rights to control access to a file object.

default management class
A management class that is assigned to a policy set. This class is used to govern backed up or archived files when a file is not explicitly associated with a specific management class through the include-exclude list.

deduplication
See *data deduplication.*

demand migration
The process that is used to respond to an out-of-space condition on a file system for which hierarchical storage management (HSM) is active. Files are migrated to server storage until space usage drops to the low threshold that was set for the file system. If the high threshold and low threshold are the same, one file is migrated.

desktop client
The group of backup-archive clients that includes clients on Microsoft Windows, Apple, and Novell NetWare operating systems.

destination
A copy group or management class attribute that specifies the primary storage pool to which a client file will be backed up, archived, or migrated.

device class
A named set of characteristics that are applied to a group of storage devices. Each device class has a unique name and represents a device type of disk, file, optical disk, or tape.

device configuration file
(1) For a server, a file that contains information about defined device classes, and, on some servers, defined libraries and drives. The information is a copy of the device configuration information in the database.

(2) For a storage agent, a file that contains the name and password of the storage agent, and information about the server that is managing the SAN-attached libraries and drives that the storage agent uses.

device driver
A program that provides an interface between a specific device and the application program that uses the device.

disaster recovery manager (DRM)
A function that assists in preparing and using a disaster recovery plan file for the server.

disaster recovery plan
A file that is created by the disaster recovery manager (DRM) that contains information about how to recover computer systems if a disaster occurs and scripts that can be run to perform some recovery tasks. The file includes information about the software and hardware that is used by the server, and the location of recovery media.

domain
A grouping of client nodes with one or more policy sets, which manage data or storage resources for the client nodes. See *policy domain* or *client domain*.

DRM See *disaster recovery manager*.

DSMAPI
See *data storage-management application-programming interface*.

dynamic serialization
A type of copy serialization in which a file or folder is backed up or archived on the first attempt regardless of whether it changes during a backup or archive.

E

EA See *extended attribute*.

EB See *exabyte*.

EFS See *Encrypted File System*.

Encrypted File System (EFS)
A file system that uses file system-level encryption.

enterprise configuration
A method of setting up servers so that the administrator can distribute the configuration of one of the servers to the other servers, using server-to-server communication. See also *configuration manager*, *managed server*, *profile*, and *subscription*.

enterprise logging
The process of sending events from a Tivoli Storage Manager server to a designated event server. The event server routes the events to designated receivers, such as to a user exit. See also *event*.

error log
A data set or file that is used to record error information about a product or system.

estimated capacity
The available space, in megabytes, of a storage pool.

event (1) An administrative command or a client operation that is scheduled to be run using Tivoli Storage Manager scheduling.

(2) A message that an Tivoli Storage Manager server or client issues. Messages can be logged using Tivoli Storage Manager event logging.

event record
A database record that describes actual status and results for events.

event server
A server to which other servers can send events for logging. The event server routes the events to any receivers that are enabled for the sending server's events.

exabyte (EB)
For processor storage, real and virtual storage, and channel volume, 1 152 921 504 606 846 976 bytes. For disk storage capacity and communications volume, 1 000 000 000 000 000 000 bytes.

exclude
The process of identifying files in an include-exclude list. This process prevents the files from being backed up or migrated whenever a user or schedule enters an incremental or selective backup operation. A file can be excluded from backup and space management, backup only, or space management only.

exclude-include list
See *include-exclude list*.

execution mode
A mode that controls the space-management related behavior of commands that run under the **dsmmode** command.

expiration
The process by which files, data sets, or objects are identified for deletion because their expiration date or retention period has passed.

expiring file
A migrated or premigrated file that has been marked for expiration and removal from storage. If a stub file or an original copy of a premigrated file is deleted from a local file system, or if the original copy of a premigrated file is updated, the corresponding migrated or premigrated file is marked for expiration the next time reconciliation is run.

extend
To increase the portion of available space that can be used to store database or recovery log information.

extended attribute (EA)
Names or value pairs that are associated with files or directories. There are three classes of extended attributes: user attributes, system attributes, and trusted attributes.

extent The part of a file that is created during the data-deduplication process. Extents are compared with other file extents to identify duplicates.

external library
A type of library that is provided by Tivoli Storage Manager that permits LAN-free data movement for StorageTek libraries that are managed by Automated Cartridge System Library Software (ACSLS). To activate this function, the Tivoli Storage Manager library type must be EXTERNAL.

F

file access time
On AIX, UNIX, or Linux systems, the time when the file was last accessed.

file age
For migration prioritization purposes, the number of days since a file was last accessed.

file device type
A device type that specifies the use of sequential access files on disk storage as volumes.

file server
A dedicated computer and its peripheral storage devices that are connected to a local area network that stores programs and files that are shared by users on the network.

file space
A logical space in server storage that contains a group of files that have been backed up or archived by a client node, from a single logical partition, file system, or virtual mount point. Client nodes can restore, retrieve, or delete their file spaces from server storage. In server storage, files belonging to a single file space are not necessarily stored together.

file space ID (FSID)
A unique numeric identifier that the server assigns to a file space when it is stored in server storage.

file state
The space management mode of a file that resides in a file system to which space management has been added. A file can be in one of three states: resident, premigrated, or migrated. See also *resident file*, *premigrated file*, and *migrated file*.

file system migrator (FSM)
A kernel extension that intercepts all file system operations and provides any space management support that is required. If no space management support is required, the operation is passed to the operating system, which performs its normal functions. The file system migrator is mounted over a file system when space management is added to the file system.

file system state
The storage management mode of a file system that resides on a workstation on which the hierarchical storage management (HSM) client is installed. A file system can be in one of these states: native, active, inactive, or global inactive.

frequency
A copy group attribute that specifies the minimum interval, in days, between incremental backups.

FSID See *file space ID*.

FSM See *file system migrator*.

full backup
The process of backing up the entire server database. A full backup begins a new database backup series. See also *database backup series* and *incremental backup*. Contrast with *database snapshot*.

fuzzy backup
A backup version of a file that might not accurately reflect what is currently in the file because the file was backed up at the same time as it was being modified.

fuzzy copy
A backup version or archive copy of a file that might not accurately reflect the original contents of the file because it was backed up or archived the file while the file was being modified. See also *backup version* and *archive copy*.

G

General Parallel File System
A high-performance shared-disk file system that can provide data access from nodes in a cluster environment.

gigabyte (GB)
In decimal notation, 1 073 741 824 when referring to memory capacity; in all other cases, it is defined as 1 000 000 000.

global inactive state
The state of all file systems to which

space management has been added when space management is globally deactivated for a client node. When space management is globally deactivated, hierarchical storage management (HSM) cannot perform migration, recall, or reconciliation. However, a root user can update space management settings and add space management to additional file systems. Users can access resident and premigrated files.

Globally Unique Identifier (GUID)
An algorithmically determined number that uniquely identifies an entity within a system.

GPFS™
See *General Parallel File System*.

GPFS node set
A mounted, defined group of GPFS file systems.

group backup
The backup of a group containing a list of files from one or more file space origins.

GUID See *Globally Unique Identifier*.

H

hierarchical storage management (HSM)
A function that automatically distributes and manages data on disk, tape, or both by regarding devices of these types and potentially others as levels in a storage hierarchy that range from fast, expensive devices to slower, cheaper, and possibly removable devices. The objectives are to minimize access time to data and maximize available media capacity.

hierarchical storage management (HSM) client
A client program that works with the Tivoli Storage Manager server to provide hierarchical storage management (HSM) for a system. See also *hierarchical storage management* and *space manager client*.

HSM See *hierarchical storage management*.

HSM client
See *hierarchical storage management client*.

I

ILM See *information lifecycle management*.

image A file system or raw logical volume that is backed up as a single object.

image backup
A backup of a full file system or raw logical volume as a single object.

inactive file system
A file system for which space management has been deactivated. Contrast with *active file system*.

inactive version
A backup version of a file that is either not the most recent backup version, or that is a backup version of a file that no longer exists on the client system. Inactive backup versions are eligible for expiration processing according to the management class assigned to the file. Contrast with *active version*.

include-exclude file
A file containing statements to determine the files to back up and the associated management classes to use for backup or archive. See also *include-exclude list*.

include-exclude list
A list of options that include or exclude selected files for backup. An exclude option identifies files that should not be backed up. An include option identifies files that are exempt from the exclusion rules or assigns a management class to a file or a group of files for backup or archive services.

incremental backup
(1) A copy of all database data that has changed since the most recent successful full backup operation. An incremental backup is also known as a *cumulative backup image* because each incremental backup includes the contents of the previous incremental backup.

(2) The process of backing up information in the database that is new or changed since the last full backup. Contrast with *full backup*. See also *database backup series*.

(3) For Data Protection for Microsoft Exchange Server, a backup in which the transaction logs are backed up and then cleared.

individual mailbox restore
See *mailbox restore*.

information lifecycle management (ILM)
GPFS policy-based file management for storage pools and file sets.

inode The internal structure that describes the individual files on AIX, UNIX, or Linux systems. An inode contains the node, type, owner, and location of a file.

inode number
A number specifying a particular inode file in the file system.

IP address
A unique address for a device or logical unit on a network that uses the IP standard.

J

job file
A generated file that contains configuration information for a migration job. The file is XML format and can be created and edited in the hierarchical storage management (HSM) client for Windows client graphical user interface.

journal-based backup
A method for backing up Windows clients and AIX clients that exploits the change notification mechanism in a file to improve incremental backup performance by reducing the need to fully scan the file system.

journal daemon
On AIX, UNIX, or Linux systems, a program that tracks change activity for files residing in file systems.

journal service
In Microsoft Windows, a program that tracks change activity for files residing in file systems.

K

kilobyte (KB)
For processor storage, real and virtual storage, and channel volume, 210 or 1 024 bytes. For disk storage capacity and communications volume, 1 000 bytes.

L

LAN See *local area network*.

LAN-free data movement
The movement of client data between a client system and a storage device on a storage area network (SAN), bypassing the local area network. This process is also referred to as *LAN-free data transfer*.

LAN-free data transfer
See *LAN-free data movement*.

leader data
Bytes of data, from the beginning of a migrated file, that are stored in the file's corresponding stub file on the local file system. The amount of leader data that is stored in a stub file depends on the stub size that is specified.

library
(1) A repository for demountable recorded media, such as magnetic disks and magnetic tapes.

(2) A collection of one or more drives, and possibly robotic devices (depending on the library type), which can be used to access storage volumes.

library client
A server that uses server-to-server communication to access a library that is managed by another storage management server. See also *library manager*.

library manager
A server that controls device operations when multiple storage management servers share a storage device. See also *library client*.

local (1) Pertaining to a device, file, or system that is accessed directly from a user system, without the use of a communication line.

(2) For HSM products, pertaining to the destination of migrated files that are being moved.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

local shadow volumes
Data that is stored on shadow volumes localized to a disk storage subsystem.

LOFS See *loopback virtual file system.*

logical file
A file that is stored in one or more server storage pools, either by itself or as part of an aggregate. See also *aggregate* and *physical file*.

logical occupancy
The space that is used by logical files in a

storage pool. This space does not include the unused space created when logical files are deleted from aggregate files, so it might be less than the physical occupancy.

logical unit (LU)
An access point through which a user or application program accesses the Systems Network Architecture (SNA) network to communicate with another user or application program.

logical unit number (LUN)
In the Small Computer System Interface (SCSI) standard, a unique identifier that is used to differentiate devices, each of which is a logical unit (LU).

logical volume
A portion of a physical volume that contains a file system.

logical volume backup
A backup of a file system or logical volume as a single object.

Logical Volume Snapshot Agent (LVSA)
Software that can act as the snapshot provider for creating a snapshot of a logical volume during an online image backup.

loopback virtual file system (LOFS)
A file system that is created by mounting a directory over another local directory, also known as mount-over-mount. A LOFS can also be generated using an automounter.

LU See *logical unit*.

LUN See *logical unit number*.

LVSA See *Logical Volume Snapshot Agent*.

M

macro file
A file that contains one or more storage manager administrative commands, which can be run only from an administrative client using the MACRO command. Contrast with *Tivoli Storage Manager command script*.

mailbox restore
A function that restores Microsoft Exchange Server data (from IBM Data Protection for Microsoft Exchange backups) at the mailbox level or mailbox-item level.

managed object
In Tivoli Storage Manager, a definition in the database of a managed server that was distributed to the managed server by a configuration manager. When a managed server subscribes to a profile, all objects that are associated with that profile become managed objects in the database of the managed server. In general, a managed object cannot be modified locally on the managed server. Objects can include policy, schedules, client option sets, server scripts, administrator registrations, server definitions, and server group definitions.

managed server
A Tivoli Storage Manager server that receives configuration information from a configuration manager using a subscription to one or more profiles. Configuration information can include definitions of objects such as policy and schedules. See also *configuration manager*, *subscription*, and *profile*.

management class
A policy object that users can bind to each file to specify how the server manages the file. The management class can contain a backup copy group, an archive copy group, and space management attributes. See also *copy group*, *space manager client*, *bind*, and *rebind*.

maximum transmission unit
The largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the maximum transmission unit for Ethernet is 1500 bytes.

MB See *megabyte*.

media server
In a z/OS® environment, a program that provides access to z/OS disk and tape storage for Tivoli Storage Manager servers that run on operating systems other than z/OS.

megabyte (MB)
(1) 1 048 576 bytes (2 to the 20th power) when used in this publication.

(2) For processor storage, real and virtual storage, and channel volume, 2 to the power of 20 or 1 048 576 bits. For disk

storage capacity and communications volume, 1 000 000 bits.

metadata
Data that describes the characteristics of data; descriptive data.

migrate
To move data from one storage location to another. In Tivoli Storage Manager products, migrating can mean moving data from a client node to server storage, or moving data from one storage pool to the next storage pool defined in the server storage hierarchy. In both cases the movement is controlled by policy, such as thresholds that are set. See also *migration threshold*.

migrated file
A file that has been copied from a local file system to Tivoli Storage Manager storage. For HSM clients on UNIX or Linux systems, the file is replaced with a stub file on the local file system. On Windows systems, creation of the stub file is optional. See also *stub file* and *resident file*. For HSM clients on UNIX or Linux systems, contrast with *premigrated file*.

migrate-on-close recall mode
A mode that causes a migrated file to be recalled back to its originating file system temporarily. Contrast with *normal recall mode* and *read-without-recall recall mode*.

migration job
A specification of files to migrate, and actions to perform on the original files after migration. See also *job file*.

migration threshold
High and low capacities for storage pools or file systems, expressed as percentages, at which migration is set to start and stop.

mirroring
The process of writing the same data to multiple locations at the same time. Mirroring data protects against data loss within the recovery log.

mode A copy group attribute that specifies whether to back up a file that has not been modified since the last time the file was backed up. See *modified mode* and *absolute mode*.

modified mode
In storage management, a backup copy-group mode that specifies that a file is considered for incremental backup only if it has changed since the last backup. A file is considered a changed file if the date, size, owner, or permissions of the file have changed. See also *absolute mode*.

mount limit
The maximum number of volumes that can be simultaneously accessed from the same device class. The mount limit determines the maximum number of mount points. See also *mount point*.

mount point
On the Tivoli Storage Manager server, a logical drive through which volumes in a sequential access device class are accessed. For removable-media device types, such as tape, a mount point is a logical drive that is associated with a physical drive. For the file device type, a mount point is a logical drive that is associated with an I/O stream. The number of mount points for a device class is defined by the value of the mount limit attribute for that device class. See also *mount limit*.

mount retention period
The maximum number of minutes that the server retains a mounted sequential-access media volume that is not being used before it dismounts the sequential-access media volume.

mount wait period
The maximum number of minutes that the server waits for a sequential-access volume mount request to be satisfied before canceling the request.

MTU See *maximum transmission unit*.

N

Nagle algorithm
An algorithm that reduces congestion of TCP/IP networks by combining smaller packets and sending them together.

named pipe
A type of interprocess communication that permits message data streams to pass between peer processes, such as between a client and a server.

NAS See *network-attached storage*.

NAS node
A client node that is a network-attached storage (NAS) file server. Data for the NAS node is transferred by a NAS file server that is controlled by the network data management protocol (NDMP). A NAS node is also called a NAS file server node.

native file system
A file system that is locally added to the file server and is not added for space management. The hierarchical storage manager (HSM) client does not provide space management services to the file system.

native format
A format of data that is written to a storage pool directly by the Tivoli Storage Manager server. Contrast with *non-native data format*.

NDMP
See *Network Data Management Protocol*.

NetBIOS
See *Network Basic Input/Output System*.

network-attached storage (NAS) file server
A dedicated storage device with an operating system that is optimized for file-serving functions. A NAS file server can have the characteristics of both a node and a data mover.

Network Basic Input/Output System (NetBIOS)
A standard interface to networks and personal computers that is used on local area networks to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not have to handle the details of LAN data link control (DLC) protocols.

Network Data Management Protocol (NDMP)
A protocol that allows a network storage-management application to control the backup and recovery of an NDMP-compliant file server, without installing vendor-acquired software on that file server.

network data-transfer rate
A rate that is calculated by dividing the total number of bytes that are transferred by the data transfer time. For example, this rate can be the time that is spent transferring data over a network.

node A file server or workstation on which the backup-archive client program has been installed, and which has been registered to the server.

node name
A unique name that is used to identify a workstation, file server, or PC to the server.

node privilege class
A privilege class that gives an administrator the authority to remotely access backup-archive clients for a specific client node or for all clients in a policy domain. See also *privilege class*.

non-native data format
A format of data that is written to a storage pool that differs from the format that the server uses for operations.

normal recall mode
A mode that causes a migrated file to be copied back to its originating file system when it is accessed.

O

offline volume backup
A backup in which the volume is locked so that no other system applications can access it during the backup operation.

online volume backup
A backup in which the volume is available to other system applications during the backup operation.

open registration
A registration process in which users can register their workstations as client nodes with the server. Contrast with *closed registration*.

operator privilege class
A privilege class that gives an administrator the authority to disable or halt the server, enable the server, cancel server processes, and manage removable media. See also *privilege class*.

options file
A file that contains processing options. On Windows and NetWare systems, the file is called dsm.opt. On AIX, UNIX, Linux, and Mac OS X systems, the file is called dsm.sys.

originating file system
The file system from which a file was

migrated. When a file is recalled using normal or migrate-on-close recall mode, it is always returned to its originating file system.

orphaned stub file
A file for which no migrated file can be found on the Tivoli Storage Manager server that the client node is contacting for space management services. For example, a stub file can be orphaned when the client system-options file is modified to contact a server that is different than the one to which the file was migrated.

out-of-space protection mode
A mode that controls whether the program intercepts out-of-space conditions. See also *execution mode*.

P

pacing
In SNA, a technique by which the receiving system controls the rate of transmission of the sending system to prevent overrun.

packet In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole.

page A defined unit of space on a storage medium or within a database volume.

partial-file recall mode
A recall mode that causes the hierarchical storage management (HSM) function to read just a portion of a migrated file from storage, as requested by the application accessing the file.

password generation
A process that creates and stores a new password in an encrypted password file when the old password expires. Automatic generation of a password prevents password prompting. Password generation can be set in the options file (`passwordaccess` option). See also *options file*.

path An object that defines a one-to-one relationship between a source and a destination. Using the path, the source accesses the destination. Data can flow from the source to the destination, and back. An example of a source is a data mover (such as a network-attached storage [NAS] file server), and an example of a destination is a tape drive.

pattern-matching character
See *wildcard character*.

physical file
A file that is stored in one or more storage pools, consisting of either a single logical file, or a group of logical files that are packaged together as an aggregate. See also *aggregate* and *logical file*.

physical occupancy
The amount of space that is used by physical files in a storage pool. This space includes the unused space that is created when logical files are deleted from aggregates. See also *physical file*, *logical file*, and *logical occupancy*.

plug-in
A self-contained software component that modifies (adds, or changes) the function in a particular system. When a plug-in is added to a system, the foundation of the original system remains intact.

policy domain
A grouping of policy users with one or more policy sets, which manage data or storage resources for the users. The users are client nodes that are associated with the policy domain.

policy privilege class
A privilege class that gives an administrator the authority to manage policy objects, register client nodes, and schedule client operations for client nodes. Authority can be restricted to certain policy domains. See also *privilege class*.

policy set
A group of rules in a policy domain. The rules specify how data or storage resources are automatically managed for client nodes in the policy domain. Rules can be contained in management classes. See also *active policy set* and *management class*.

premigrated file
A file that has been copied to Tivoli Storage Manager storage, but has not been replaced with a stub file on the local file system. An identical copy of the file resides both on the local file system and

in Tivoli Storage Manager storage. Premigrated files occur on UNIX and Linux file systems to which space management has been added. Contrast with *migrated file* and *resident file*.

premigrated files database
A database that contains information about each file that has been premigrated to Tivoli Storage Manager storage. The database is stored in a hidden directory named `.SpaceMan` in each file system to which space management has been added.

premigration
The process of copying files that are eligible for migration to Tivoli Storage Manager storage, but leaving the original file intact on the local file system.

premigration percentage
A space management setting that controls whether the next eligible candidates in a file system are premigrated following threshold or demand migration.

primary storage pool
A named set of volumes that the server uses to store backup versions of files, archive copies of files, and files migrated from client nodes. See also *destination* and *copy storage pool*.

privilege class
A level of authority that is granted to an administrator. The privilege class determines which administrative tasks the administrator can perform. See also *node privilege class*, *operator privilege class*, *policy privilege class*, *storage privilege class*, and *system privilege class*.

profile
A named group of configuration information that can be distributed from a configuration manager when a managed server subscribes. Configuration information can include registered administrator IDs, policies, client schedules, client option sets, administrative schedules, storage manager command scripts, server definitions, and server group definitions. See also *configuration manager* and *managed server*.

Q

quota (1) For HSM on AIX, UNIX, or Linux systems, the limit (in megabytes) on the amount of data that can be migrated and premigrated from a file system to server storage.

(2) For HSM on Windows systems, a user-defined limit to the space that is occupied by recalled files.

R

randomization
The process of distributing schedule start times for different clients within a specified percentage of the schedule's startup window.

raw logical volume
A portion of a physical volume that is comprised of unallocated blocks and has no journaled file system (JFS) definition. A logical volume is read/write accessible only through low-level I/O functions.

read-without-recall recall mode
A mode that causes hierarchical storage management (HSM) to read a migrated file from storage without storing it back on the local file system. The last piece of information read from the file is stored in a buffer in memory on the local file system. Contrast with *normal recall mode* and *migrate-on-close recall mode*.

rebind
To associate all backed-up versions of a file with a new management class name. For example, a file that has an active backup version is rebound when a later version of the file is backed up with a different management class association. See also *bind*.

recall In Tivoli Storage Manager, to copy a migrated file from server storage back to its originating file system using the space management client. See also *transparent recall*, *selective recall*, and *recall mode*.

recall mode
A mode that is assigned to a migrated file with the **dsmattr** command that determines how the file is processed when it is recalled. It determines whether the file is stored on the local file system, is migrated back to Tivoli Storage Manager storage when it is closed, or is read from Tivoli Storage Manager storage without storing it on the local file system.

receiver
A server repository that contains a log of server and client messages as events. For example, a receiver can be a file exit, a user exit, or the Tivoli Storage Manager server console and activity log. See also *event*.

reclamation
The process of consolidating the remaining data from many sequential-access volumes onto fewer, new sequential-access volumes.

reclamation threshold
The percentage of space that a sequential-access media volume must have before the server can reclaim the volume. Space becomes reclaimable when files are expired or are deleted.

reconciliation
The process of synchronizing a file system with the Tivoli Storage Manager server, and then removing old and obsolete objects from the Tivoli Storage Manager server.

recovery log
A log of updates that are about to be written to the database. The log can be used to recover from system and media failures. The recovery log consists of the active log (including the log mirror) and archive logs.

register
To define a client node or administrator ID that can access the server.

registry
A repository that contains access and configuration information for users, systems, and software.

remote
(1) Pertaining to a system, program, or device that is accessed through a communication line.

(2) For HSM products, pertaining to the origin of migrated files that are being moved.

resident file
On a Windows system, a complete file on a local file system that might also be a migrated file because a migrated copy can exist in Tivoli Storage Manager storage. On a UNIX or Linux system, a complete file on a local file system that has not been migrated or premigrated, or that has been recalled from Tivoli Storage Manager storage and modified. Contrast with *stub file* and *premigrated file*. See *migrated file*.

restore
To copy information from its backup location to the active storage location for use. For example, to copy information from server storage to a client workstation.

retention
The amount of time, in days, that inactive backed-up or archived files are kept in the storage pool before they are deleted. Copy group attributes and default retention grace periods for the domain define retention.

retrieve
To copy archived information from the storage pool to the workstation for use. The retrieve operation does not affect the archive version in the storage pool.

roll back
To remove changes that were made to database files since the last commit point.

root user
A system user who operates without restrictions. A root user has the special rights and privileges needed to perform administrative tasks.

S

SAN See *storage area network*.

schedule
A database record that describes client operations or administrative commands to be processed. See *administrative command schedule* and *client schedule*.

scheduling mode
The type of scheduling operation for the server and client node that supports two scheduling modes: client-polling and server-prompted.

scratch volume
A labeled volume that is either blank or contains no valid data, that is not defined, and that is available for use.

script A series of commands, combined in a file, that carry out a particular function when the file is run. Scripts are interpreted as

they are run. Contrast with *Tivoli Storage Manager command script*.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

selective backup
The process of backing up certain files or directories from a client domain. The files that are backed up are those that are not excluded in the include-exclude list. The files must meet the requirement for serialization in the backup copy group of the management class that is assigned to each file. Contrast with *incremental backup*.

selective migration
The process of copying user-selected files from a local file system to Tivoli Storage Manager storage and replacing the files with stub files on the local file system. Contrast with *threshold migration* and *demand migration*.

selective recall
The process of copying user-selected files from Tivoli Storage Manager storage to a local file system. Contrast with *transparent recall*.

serialization
The process of handling files that are modified during backup or archive processing. See *dynamic serialization*, *static serialization*, *shared static serialization*, and *shared dynamic serialization*.

server A software program or a computer that provides services to other software programs or other computers.

server options file
A file that contains settings that control various server operations. These settings affect such things as communications, devices, and performance.

server-prompted scheduling mode
A client/server communication technique where the server contacts the client node when tasks must be done. Contrast with *client-polling scheduling mode*.

server storage
The primary, copy, and active-data storage pools that are used by the server to store user files such as backup versions, archive copies, and files migrated from space manager client nodes (space-managed files). See also *active-data pool*, *primary storage pool*, *copy storage pool*, *storage pool volume*, and *volume*.

session
A logical or virtual connection between two stations, software programs, or devices on a network that allows the two elements to communicate and exchange data.

session resource usage
The amount of wait time, processor time, and space that is used or retrieved during a client session.

shared dynamic serialization
A value for serialization that specifies that a file must not be backed up or archived if it is being modified during the operation. Tivoli Storage Manager retries the backup or archive operation a number of times; if the file is being modified during each attempt, Tivoli Storage Manager will back up or archive the file on its last try. See also *serialization*. Contrast with *dynamic serialization*, *shared static serialization*, and *static serialization*.

shared library
A library device that is used by multiple storage manager servers.

shared static serialization
A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. Tivoli Storage Manager attempts to retry the operation a number of times. If the file is in use during each attempt, the file is not backed up or archived. See also *serialization*. Contrast with *dynamic serialization*, *shared dynamic serialization*, and *static serialization*.

snapshot
An image backup type that consists of a point-in-time view of a volume.

space-managed file
A file that is migrated from a client node by the space manager client. The space manager client recalls the file to the client node on demand.

space management
The process of keeping sufficient free storage space available on a local file system for new data by migrating files to server storage. Synonymous with *hierarchical storage management*.

space manager client
A program that runs on a UNIX or Linux system to manage free space on the local file system by migrating files to server storage. The program can recall the files either automatically or selectively. Also called *hierarchical storage management (HSM) client*.

space monitor daemon
A daemon that checks space usage on all file systems for which space management is active, and automatically starts threshold migration when space usage on a file system equals or exceeds its high threshold.

sparse file
A file that is created with a length greater than the data it contains, leaving empty spaces for the future addition of data.

special file
On AIX, UNIX, or Linux systems, a file that defines devices for the system, or temporary files that are created by processes. There are three basic types of special files: first-in, first-out (FIFO); block; and character.

SSL See *Secure Sockets Layer*.

stabilized file space
A file space that exists on the server but not on the client.

stanza A group of lines in a file that together have a common function or define a part of the system. Each stanza is identified by a name that occurs in the first line of the stanza. Depending on the type of file, a stanza is ended by the next occurrence of a stanza name in the file, or by an explicit end-of-stanza marker. A stanza can also be ended by the end of the file.

startup window
A time period during which a schedule must be initiated.

static serialization
A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. If the file is in use during the first attempt, the storage manager cannot back up or archive the file. See also *serialization*. Contrast with *dynamic serialization*, *shared dynamic serialization*, and *shared static serialization*.

storage agent
A program that enables the backup and restoration of client data directly to and from storage attached to a storage area network (SAN).

storage area network (SAN)
A dedicated storage network that is tailored to a specific environment, combining servers, systems, storage products, networking products, software, and services.

storage hierarchy
(1) A logical order of primary storage pools, as defined by an administrator. The order is typically based on the speed and capacity of the devices that the storage pools use. The storage hierarchy is defined by identifying the next storage pool in a storage pool definition. See also *storage pool*.

(2) An arrangement of storage devices with different speeds and capacities. The levels of the storage hierarchy include: main storage, such as memory and direct-access storage device (DASD) cache; primary storage (DASD containing user-accessible data); migration level 1 (DASD containing data in a space-saving format); and migration level 2 (tape cartridges containing data in a space-saving format).

storage pool
A named set of storage volumes that are the destination that is used to store client data. A storage pool contains backup versions, archive copies, and files that are migrated from space manager client nodes. A primary storage pool is backed up to a copy storage pool. See also *primary storage pool*, *copy storage pool*, and *active-data pool*.

storage pool volume
A volume that has been assigned to a storage pool. See also *volume*, *active-data pool*, *copy storage pool*, and *primary storage pool*.

storage privilege class
A privilege class that gives an administrator the authority to control how storage resources for the server are allocated and used, such as monitoring the database, the recovery log, and server storage. See also *privilege class*.

stub A shortcut on the Windows file system that is generated by the hierarchical storage management (HSM) client for a migrated file that allows transparent user access. A stub is the sparse file representation of a migrated file, with a reparse point attached.

stub file
A file that replaces the original file on a local file system when the file is migrated to storage. A stub file contains the information that is necessary to recall a migrated file from Tivoli Storage Manager storage. It also contains additional information that can be used to eliminate the need to recall a migrated file.

stub file size
The size of a file that replaces the original file on a local file system when the file is migrated to Tivoli Storage Manager storage. The size that is specified for stub files determines how much leader data can be stored in the stub file. The default for stub file size is the block size defined for a file system minus 1 byte.

subscription
In a Tivoli environment, the process of identifying the subscribers that the profiles are distributed to. For Tivoli Storage Manager, a subscription is the process by which a managed server receives configuration information associated with a particular profile on a configuration manager. See also *managed server*, *configuration manager*, and *profile*.

system privilege class
A privilege class that gives an administrator the authority to issue all server commands. See also *privilege class*.

Systems Network Architecture (SNA)
The description of the logical structure, formats, protocols, and operational sequences for transmitting information through and controlling the configuration and operation of networks.

T

tape library
A set of equipment and facilities that support an installation's tape environment. The tape library can include tape storage racks, mechanisms for automatic tape mounting, a set of tape drives, and a set of related tape volumes mounted on those drives.

tape volume prefix
The high-level-qualifier of the file name or the data set name in the standard tape label.

target node
A client node for which other client nodes (called agent nodes) have been granted proxy authority. The proxy authority allows the agent nodes to perform operations such as backup and restore on behalf of the target node, which owns the data.

TCA See *trusted communications agent*.

TCP/IP
See *Transmission Control Protocol/Internet Protocol*.

threshold migration
The process of moving files from a local file system to Tivoli Storage Manager storage based on the high and low thresholds that are defined for the file system. Contrast with *demand migration*, *selective migration*, and *migration job*.

throughput
In storage management, the total bytes in the workload, excluding overhead, that are backed up or restored, divided by elapsed time.

timeout
A time interval that is allotted for an event to occur or complete before operation is interrupted.

timestamp control mode
A mode that determines whether commands preserve the access time for a file or set it to the current time.

Tivoli Storage Manager command script
A sequence of Tivoli Storage Manager administrative commands that are stored in the database of the Tivoli Storage Manager server. The script can run from any interface to the server. The script can

include substitution for command parameters and conditional logic.

tombstone object
A small subset of attributes of a deleted object. The tombstone object is retained for a specified period, and at the end of the specified period, the tombstone object is permanently deleted.

Transmission Control Protocol/Internet Protocol (TCP/IP)
An industry-standard, nonproprietary set of communication protocols that provides reliable end-to-end connections between applications over interconnected networks of different types.

transparent recall
The process that is used to automatically recall a file to a workstation or file server when the file is accessed. See also *recall mode*. Contrast with *selective recall*.

trusted communications agent (TCA)
A program that handles the sign-on password protocol when clients use password generation.

U

UCS-2 A 2-byte (16-bit) encoding scheme based on ISO/IEC specification 10646-1. UCS-2 defines three levels of implementation: Level 1-No combining of encoded elements allowed; Level 2-Combining of encoded elements is allowed only for Thai, Indic, Hebrew, and Arabic; Level 3-Any combination of encoded elements are allowed.

UNC See *Universal Naming Convention name*.

Unicode
A character encoding standard that supports the interchange, processing, and display of text that is written in the common languages around the world, plus some classical and historical texts. The Unicode standard has a 16-bit character set defined by ISO 10646.

Unicode-enabled file space
Unicode file space names provide support for multilingual workstations without regard for the current locale.

Unicode transformation format 8
Unicode Transformation Format (UTF), 8-bit encoding form, which is designed for ease of use with existing ASCII-based systems. The CCSID value for data in UTF-8 format is 1208.

Universal Naming Convention (UNC) name
A name that is used to access a drive or directory containing files shared across a network. The UNC name includes the system name and a SharePoint name that represents the shared drive or directory.

Universally Unique Identifier (UUID)
The 128-bit numeric identifier that is used to ensure that two components do not have the same identifier.

UTF-8 See *Unicode transformation format 8*.

UUID See *Universally Unique Identifier*.

V

validate
To check a policy set for conditions that can cause problems if that policy set becomes the active policy set. For example, the validation process checks whether the policy set contains a default management class.

version
A backup copy of a file stored in server storage. The most recent backup copy of a file is the active version. Earlier copies of the same file are inactive versions. The number of versions retained by the server is determined by the copy group attributes in the management class.

virtual file space
A representation of a directory on a network-attached storage (NAS) file system as a path to that directory.

virtual volume
An archive file on a target server that represents a sequential media volume to a source server.

volume
A discrete unit of storage on disk, tape or other data recording medium that supports some form of identifier and parameter list, such as a volume label or input/output control. See also *scratch volume*, and *storage pool volume*.

volume history file
A file that contains information about volumes that have been used by the server for database backups and for export of administrator, node, policy, or

server data. The file also has information about sequential-access storage pool volumes that have been added, reused, or deleted. The information is a copy of volume information that is recorded in the server database.

Volume Shadow Copy Service
A set of Microsoft application-programming interfaces (APIs) that you can use to create shadow copy backups of volumes, exact copies of files, including all open files, and so on.

VSS See *Volume Shadow Copy Service*.

VSS Backup
A backup operation that uses Microsoft Volume Shadow Copy Service (VSS) technology. The backup operation produces an online snapshot (point-in-time consistent copy) of Microsoft Exchange data. This copy can be stored on local shadow volumes or on Tivoli Storage Manager server storage.

VSS Fast Restore
A function that uses a Microsoft Volume Shadow Copy Service (VSS) software provider to restore VSS Backups (IBM Data Protection for Microsoft Exchange database files and log files) that reside on local shadow volumes.

VSS Instant Restore
A volume-level hardware-assisted Microsoft Volume Shadow Copy Service (VSS) function where target volumes that contain the snapshot are copied back to the original source volumes.

VSS offloaded backup
A backup operation that uses a Microsoft Volume Shadow Copy Service (VSS) hardware provider (installed on an alternate system) to move IBM Data Protection for Microsoft Exchange data to the Tivoli Storage Manager server. This type of backup operation shifts the backup load from the production system to another system.

VSS Restore
A function that uses a Microsoft Volume Shadow Copy Service (VSS) software provider to restore VSS Backups (IBM Data Protection for Microsoft Exchange database files and log files) that reside on Tivoli Storage Manager server storage to their original location.

W

wildcard character
A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace the wildcard character.

workstation
A terminal or personal computer at which a user can run applications and that is usually connected to a mainframe or a network.

worldwide name
A 64-bit, unsigned name identifier that is unique.

workload partition (WPAR)
A partition within a single operating system instance.

Index

Numerics

64-bit Solaris SPARC
  installation instructions 17

A

accessibility features 61
AIX
  hardware requirements 5
AIX 6.1
  options 24
AIX 64-bit
  communication methods 6
  installation instructions 8
  installation requirements 6
  operating system requirements 6
  software requirements 6
archive copy group 32

B

backdelete
  and Data Protection for Oracle node 27
  and Tivoli Storage Manager policy 32
backup copy group values 32
backups
  automating 40
  removing 40
bkdb.log 35
bkdb.scr
  and the Tivoli Storage Manager scheduler 40, 41, 42
books
  See publications

C

client deduplication
  considerations 45
  setting up 45
command line syntax
  characteristics 49
commands
  Oracle
    change 40
  tdpoconf password 50
  tdpoconf showenvironment 51
  tdposync
    query 57
    syncdb 54
  Tivoli Storage Manager server
    query actlog xvi
    query association 41
    query node xvi, 39
    query schedule 41
commmethod
  description 29
communication methods
  AIX 64-bit 6
  HP-UX 6
compression 29
configure
  with default settings 21
configuring
  Data Protection for Oracle 21
configuring Data Protection for Oracle 23
control file 52, 54
conventions
  typeface xvii
customer support
  contact xiii

D

data deduplication
  overview 44
  using 44
data deduplication reduction
  determinining 46
Data Protection for Oracle
  and Oracle databases 35
  configuring 21, 27
  generating trace file xvi
  installation requirements
    AIX 64-bit 6
    HP-UX 6
    Linux 6
  installing 5
  overview 1, 2
  protecting data 35
  recommendations 53
  Recovery Manager (RMAN) 2
  reference 49
  reporting problems xv
  supported Oracle versions 2
  Tivoli Storage Manager policy requirements 32
  updates xxi
  version migration 3
Data Protection for Oracle utilities
  using 49
deduplication
  using 44
defining a schedule
  on the client machine 42
  on the Tivoli Storage Manager server 41
definitions 67
disability 61
documentation
  See publications
dsierror.log
  problem determination xv
dsm.opt
  description 27
  problem determination xv
  required options 29
dsm.sys
  description 27
  recommended options 29
  required options 28
dsmi_log 24
dsmi_orc_config 24
  and the Tivoli Storage Manager scheduler 42
duplex copy
  considerations 39
  overview 38

E

education
  see Tivoli technical training xi
enablelanfree 30
example
  tdposync query command 57
examples
  duplex copy 39
  include/exclude 32
  invoking RMAN 35
  removing backups 40
  RMAN script
    send command 37
  RMAN scripts 37
  tdpoconf password command 50
  tdpoconf showenvironment command 51
  tdposync syncdb command 54
    pick window 56
  Tivoli Storage Manager scheduler 41
expiration of objects 32

F

fixes, obtaining xiii

G

glossary 67

H

hardware requirements
  AIX 5
  HP-UX 5
  Linux 5
  Solaris 5
  UNIX and Linux 5
HP-UX
  communication methods 6
  hardware requirements 5
  installation requirements 6
  operating system requirements 6
  software requirements 6
HP-UX Itanium 2 64-bit
  options 24

© Copyright IBM Corp. 1998, 2011

HP-UX Itanium 64-bit
installation instructions 10
HP-UX PA-RISC 64-bit
options 24

I

IBM Publications Center vii, x
IBM Support Assistant xii
inclexcl
and Tivoli Storage Manager policy 32
include
and duplex copy 39
and Tivoli Storage Manager policy 32
description 30
installation
instructions
64-bit Solaris SPARC 17
AIX 64-bit 8
HP-UX Itanium 64-bit 10
Linux x86 32-bit 12
Linux x86_64 13
Linux zSeries 64-bit 15
node name registration 26
prerequisites 5
requirements
AIX 64-bit 6
HP-UX 6
Linux 6
Solaris SPARC 64-bit 6
installation requirements
Solaris SPARC 64-bit 6
installing
Data Protection for Oracle 5
Internet, searching for problem resolution xi, xiii

K

keyboard 61
knowledge bases, searching xi

L

LAN-free data transfer
description 3
options 30
Linux
hardware requirements 5, 6
installation requirements 6
operating system requirements 6
software requirements 6
Linux on POWER
options 24
Linux x86 32-bit
installation instructions 12
Linux x86_64
installation instructions 13
options 24
Linux zSeries 64-bit
installation instructions 15
options 24

M

management class
for automatic expiration 32
manuals
See publications
maxnummp 39
migration considerations 3

N

New in this version xxi
nocatalog
and tdposync syncdb command 54
node name
registration 26
numcatalogs
and tdposync syncdb command 54
numorcintstances
and tdposync syncdb command 54

O

operating system requirements
AIX 64-bit 6
HP-UX 6
Linux 6
Solaris SPARC 64-bit 6
options 24
Oracle RMAN send command
using 36
outfile
and tdpoconf showenvironment command 51
overview
data deduplication 44
Data Protection for Oracle 1

P

Passport Advantage xiv
passwordaccess 28
performance monitor on Tivoli Storage Manager server 45
pick window 56
policy domain 32
problem determination
describing problem for IBM Software Support xiv
determining business impact for IBM Software Support xiv
guidelines xv
submitting a problem to IBM Software xv
protecting data
Data Protection for Oracle 35
publications
download vii
order vii
search vii
Tivoli Storage FlashCopy Manager x
Tivoli Storage Manager viii

Q

querying backup objects 44

R

reference
Data Protection for Oracle 49
retonly
and Tivoli Storage Manager policy 32
RMAN
description 2
invoking 35
scripts 36
send command 36

S

schedbkdb.scr 42
scripts 36
send command
in an RMAN script 36
sample script 37
using 36
servername
and dsm.opt 29
and dsm.sys 28
and the Tivoli Storage Manager scheduler 42
set duplex 39
setting up client deduplication 45
software requirements
AIX 64-bit 6
HP-UX 6
Linux 6
Solaris SPARC 64-bit 6
Tivoli Storage Manager API 6
software support
describing problem for IBM Software Support xiv
determining business impact for IBM Software Support xiv
submitting a problem xv
Software Support
contact xiii
Solaris
hardware requirements 5
Solaris SPARC 32-bit
options 24
Solaris SPARC 64-bit
hardware requirements 6
installation requirements 6
operating system requirements 6
options 24
software requirements 6
Solaris x86 32-bit
options 24
Solaris x86_64
options 24
support contract xiv
support information x
support subscription xiv
syntax diagrams xvii

T

tcpserveraddress 29
tdpo_date_fmt 25
tdpo_fs 24
tdpo_mgmt_class_2 26

tdpo_mgmt_class_3 26
tdpo_mgmt_class_4 26
tdpo_node 25
tdpo_num_fmt 26
TDPO_OPTFILE
  and tdpoconf password command 50
  and tdpoconf showenvironment command 51
  and tdposync syncdb command 54, 57
  example 23
tdpo_owner 24
tdpo_pswdpath 24
tdpo_time_fmt 26
tdpo_trace_file xvi
tdpo.opt
  and version migration 3
  description 23
  problem determination xv
tdpoconf
  and password initialization 33
  and tdpo.opt 23
  description 50
  for problem determination xv
  password command 50
    example 50
    syntax diagram 50
    TDPO_OPTFILE 50
  showenvironment command 51
    example 51
    outfile 51
    syntax diagram 51
    TDPO_OPTFILE 51
tdpoerror.log
  how to specify 24
  problem determination xv
tdposync
  and tdpo.opt 23
  considerations 53
  description 52
  query command 57
    example 57
    syntax diagram 57
    TDPO_OPTFILE 57
  syncdb command 54
    example 54
    nocatalog 54
    numcatalogs 54
    numorcintstances 54
    pick window 56
    syntax diagram 54
    TDPO_OPTFILE 54
tdposync syncdb command
  pick window 56
Tivoli Storage Manager
  functions 1
  management class 32
  policy requirements 32
  scheduler 40
  services 1
Tivoli Storage Manager API
  requirements 6
Tivoli Storage Manager API trace file xvi
Tivoli Storage Manager server
  requirements 6
Tivoli technical training xi
trace file, generating xvi
tracefile xvi
training, Tivoli technical xi
typeface conventions xvii

U

UNIX and Linux
  hardware requirements 5
using data deduplication 44

V

verdeleted
  and Tivoli Storage Manager policy 32

Product Number: 5608-E04

Printed in USA

SC27-4019-00