IBM Tivoli Storage Manager for Databases
Data Protection for Oracle

Version 7.1.3
for UNIX and Linux

Installation and User's Guide

IBM Tivoli Storage Manager for Databases
Data Protection for Oracle
Version 7.1.3
for UNIX and Linux

Installation and User's Guide

Note:
Before you use this information and the product it supports, read the information in "Notices" on page 59.

Second edition (September 2015)

This edition applies to version 7, release 1, modification 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.

Contents

Tables

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 runs 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, and provides 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.

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

- AIX®
- HP-UX
- Linux
- Oracle Solaris

Publications

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

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

New for 7.1.3

The documentation has been updated to include information from APARs.

Language packs merged into the base package
In earlier updates, the language packages were installed separately. Starting with this update, the language packages are merged into the base package. Because the file merge is handled programmatically, there are no specific instructions related to this update. After the installation process is complete, like the base package, the languages are signed in the Windows registry.

Estimate compliance with license entitlements
From the Tivoli Storage Manager Operations Center, you can view front-end and back-end capacity usage to estimate compliance with license entitlements.

Important: The Tivoli Storage Manager client software needs to be at the latest level for the Operations Center to present complete data.

Chapter 1. Data Protection for Oracle

A brief overview of IBM Tivoli Storage Manager and 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. Consistency across different operating systems and hardware is provided.
- Increases administrator productivity

  Tivoli Storage Manager can reduce the cost of network administration by allowing administrators to:
  - 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 optimization 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 restore the data from these copies when required. The 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

These services migrate client files from expensive storage media to less expensive storage media, for example from disk to tape. 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:

  – Set client and server options.
  – Define devices.
  – Format storage volumes.
  – Add more 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 that is 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, “Data Protection for Oracle installation,” 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 programming interface (SBTAPI) 2.0. This SBTAPI communicates with RMAN and translates Oracle commands into Tivoli Storage Manager API calls to the Tivoli Storage Manager server.

You can use RMAN Data Protection for Oracle to run backup and restore functions that are listed.

- Full and incremental backup functions online or offline for:
  - Databases
  - Table spaces
  - Data files
  - Archive log files
  - Control files
- Full database restores while offline.
- Table space and data file restore 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. The load on the Tivoli Storage Manager server is decreased, allowing the server to support a greater number of simultaneous connections.

Data Protection for Oracle can be installed on a client with the Storage Agent (STA). The agents can be installed on a non-STA client. The backup data is sent over the LAN (TCP/IP) to the STA client. The STA client sends the data over the SAN LAN-free, directly to tape or disk.

In addition to specific LAN-free requirements, you must specify the following option:

lanfreetcpserveraddress
Specifies the TCP/IP address for a Tivoli Storage Manager Storage Agent.

Migration and coexistence with Data Protection for Oracle

The migration considerations to the new version of Data Protection for Oracle are provided.

- Existing backups that are created with a previous version of Data Protection for Oracle are restorable with Data Protection for Oracle 7.1.
- Backups that are created with Data Protection for Oracle 7.1 cannot be restored with previous versions of Data Protection for Oracle.

Related tasks:

Chapter 3, “Configuring Data Protection for Oracle,” on page 17

“Editing RMAN scripts” on page 32

Automated failover for data recovery

When there is an outage on the Tivoli Storage Manager server, Data Protection for Oracle can fail over to a secondary server for data recovery operations.

The Tivoli Storage Manager server that Data Protection for Oracle connects to for backup operations is called the *primary server*. When the primary server and the Data Protection for Oracle node are set up for node replication on the primary server, the node can be replicated to another Tivoli Storage Manager server, called the *secondary server*.

During normal operations, connection information for the secondary server is automatically sent to Data Protection for Oracle from the primary server. The secondary server information is saved to the client options file (`dsm.sys`) on the Data Protection for Oracle node. No manual intervention is required by you to add the information for the secondary server.

Each time Data Protection for Oracle logs on to the server for backup services, it attempts to contact the primary server. If the primary server is unavailable, Data Protection for Oracle automatically fails over to the secondary server. In failover mode, you can restore data that was replicated to the secondary server. When the primary server is online again, Data Protection for Oracle automatically fails back to the primary server the next time it connects to the server.

You can confirm that Data Protection for Oracle has failed over by looking for entries about the secondary server in the `dsierror.log` file.

Requirements: To ensure that automated client failover can occur, Data Protection for Oracle must meet the following requirements:

- Data Protection for Oracle must be at the V7.1 level.
- The primary server and secondary server must be at the V7.1 level.
- The primary and secondary servers must be set up for node replication.
- The Data Protection for Oracle node must be configured for replication with the `replstate=enabled` option in the node definition on the server.
- Before the connection information for the secondary server can be sent to Tivoli Storage FlashCopy Manager, the following processes must occur:
  - You must back up data at least one time to the primary server.
  - The Data Protection for Oracle node on the primary server must be replicated at least one time to the secondary server.

Restriction: The following restrictions apply to Data Protection for Oracle during failover:

- Any operation that requires data to be stored on the Tivoli Storage Manager server, such as backup operations, are not available. You can use only data recovery functions, such as restore or query operations.
- Schedules are not replicated to the secondary server. Therefore, schedules are not run while the primary server is unavailable.
- If the primary server goes down before or during node replication, the most recent backup data is not successfully replicated to the secondary server. The replication status of the file space is not current. If you attempt to restore data in failover mode and the replication status is not current, the recovered data might not be usable. You must wait until the primary server comes back online before you can restore the data.

Chapter 2. Data Protection for Oracle installation

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, AIX, and Linux.

Before you begin

Hardware, software, and operating system requirements must be met before you attempt 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 minimum hardware and software requirements for the Data Protection for Oracle release are available in the hardware and software requirements technote for each particular release. For current requirements, review the Hardware and Software Requirements technote for your version of Data Protection for Oracle. This technote is available in the *TSM for Databases - All Requirements Documents* website at http://www.ibm.com/support/docview.wss?uid=swg21218747. From the page, follow the link to the requirements technote for your specific release or update level.

Note:

- You must uninstall any previous version of Data Protection for Oracle, or the Tivoli Storage Manager API, before you install 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.
- The installation process does not overwrite the existing `dsm.opt` options file, `tdpo.opt` configuration file, or log files.

Minimum hardware requirements

Your system must meet the minimum hardware requirements for installing and operating Data Protection for Oracle in an AIX, Linux or UNIX environment.

The minimum hardware requirements for the Data Protection for Oracle release are available in the hardware and software requirements technote for each particular release. For current requirements, review the Hardware and Software Requirements technote for your version of Data Protection for Oracle. This technote is available in the TSM for Databases - All Requirements Documents website at http://www.ibm.com/support/docview.wss?uid=swg21218747. From the page, follow the link to the requirements technote for your specific release or update level.

Minimum software and operating system requirements

Your system must meet the minimum software requirements for operating Data Protection for Oracle in an AIX, Linux or UNIX environment.

The minimum software and operating system requirements for the Data Protection for Oracle release are available in the hardware and software requirements technote for each particular release. For current requirements, review the Hardware and Software Requirements technote for your version of Data Protection for Oracle. This technote is available in the TSM for Databases - All Requirements Documents website at http://www.ibm.com/support/docview.wss?uid=swg21218747. From the page, follow the link to the requirements technote for your specific release or update level.

Virtualization support

Information about the virtualization environments that can be used with Data Protection for Oracle is available in the IBM Tivoli Storage Manager guest support for virtual machines and virtualization website at: http://www.ibm.com/support/docview.wss?uid=swg21239546.

Installing on an AIX 64-bit operating system

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

Before you begin

Uninstall any previous version of Data Protection for Oracle, or the Tivoli Storage Manager API, before you install a new or updated version, but do not delete the license enablement file.

Data Protection for Oracle fix and interim fix packs do not contain a license enablement file.

About this task

All installable files on the DVD are in the `/usr/sys/inst.images` directory.

Table 1. 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 2. Data Protection for Oracle AIX 64-bit, utilities, 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`

Table 2. Data Protection for Oracle AIX 64-bit, utilities, and Tivoli Storage Manager API package names (continued)

Package	Package Name
Tivoli Storage Manager API 64-bit	`tivoli.tsm.client.api.aix.64bit`

Procedure

Use these instructions to install Data Protection for Oracle. These steps assume that your DVD drive is `/dev/cd0`.

1. Insert the Data Protection for Oracle DVD into the DVD drive.
2. Log in using the root user ID.
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 **SOFTWARE to install**. Press F4 to list available software.
8. Select the installable packages:
   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. Highlight the Electronic License Agreement (`tivoli.tsm.loc.client.oracle.aix.64bit.ela`) and press F7.
      1) Set **ACCEPT new license agreements** to `Yes`.
      2) Set **Preview new license agreements** to `No` for the installation to proceed.
      3) If **Preview new license agreements** is set to `Yes`, the installation starts 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 opens, press Enter.
10. To continue the installation procedure, press Enter when you are asked if you are sure.
11. Press F10 to exit the smitty installation environment. You can view the summary for more information about the installation.

Installing in silent mode on an AIX system

You can install Data Protection for Oracle in silent mode on a Unix, AIX, or Linux system. A silent installation runs independently without any intervention so that you are not required to monitor, or provide input.

Before you begin

Ensure that you have installed the Tivoli Storage Manager API before you install Data Protection for Oracle in silent mode.

About this task

This method is useful when you must install Data Protection for Oracle on a number of different computers with identical hardware. For example, a company might have 25 Oracle servers that are installed across 25 different sites. You can create an unattended installation package and make it available to the 25 sites. This method ensures a consistent configuration and avoids different people all entering Data Protection for Oracle parameters. The installation package can be placed on a DVD and sent to each site, or it can be placed on a file server for distribution.

Procedure

1. If you have installed the Tivoli Storage Manager API, change to the directory where the installation images for Data Protection for Oracle are stored.
2. Run the following command to install Data Protection for Oracle in silent mode: `installp -acgXYd`
3. Select the packages you want to install:

   ```
   installp -acgXYd
   /usr/sys/inst.images
   tivoli.tsm.loc.client.oracle.aix.64bit.ela
   tivoli.tsm.client.oracle.aix.64bit
   tivoli.tsm.client.oracle.tools.aix.64bit
   ```

   - If you have not installed the TSM API, change to the directory where the installation images for Data Protection for Oracle are stored, run the following command to install Data Protection for Oracle in silent mode:

     ```
     installp -acgXYd
     /usr/sys/inst.images
     tivoli.tsm.client.api.64bit
     tivoli.tsm.loc.client.oracle.aix.64bit.ela
     tivoli.tsm.client.oracle.aix.64bit
     tivoli.tsm.client.oracle.tools.aix.64bit
     ```

Installing on a 64-bit HP-UX Itanium system

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

Before you begin

Uninstall any previous version of Data Protection for Oracle, or the Tivoli Storage Manager API, before you install a new or updated version, but do not delete the license enablement file.

About this task

All installable files are in the /cdrom/oracle/hpuxia/ directory.

Table 3. 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 4. 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
Tivoli Storage Manager API	TIVsmCapi64

To install Data Protection for Oracle complete the following steps:

Procedure

1. Log in by using the root user ID.
2. Create a directory for mounting the DVD and set the appropriate permission to the directory by using the following commands:

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

3. Mount the DVD with the following command:

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

   where the device name is the DVD name. An example of device_name is /dev/dsk/c1t2d0.

4. To install the Tivoli Storage Manager API, issue this command:

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

5. Change to the cdrom/oracle/hpuxia/ directory where the Data Protection for Oracle installable file is located.
6. Install the Data Protection for Oracle product, utilities, and license by using one of the following methods:
   - Using the command line, type in the name of the installable file, TDPOracle64.bin, on the command line and press Enter.
   - To install the product in console mode, enter the following command, and press Enter:

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

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

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

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

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

Typically the file name is `TDPOracle64.bin`, however, if the installable file was downloaded from the FTP site, the file name might be different.

Installing on a Linux x86_64 system

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

Before you begin

Uninstall any previous version of Data Protection for Oracle, or the Tivoli Storage Manager API, before you install a new or updated version, but do not delete the license enablement file.

About this task

All installable files are in the `/cdrom/oracle/linux86_64` directory.

Table 5. Linux x86_64 default installation directories

Linux	Default Installation Directories
Data Protection for Oracle Linux x86_64	`/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 6. 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`
Tivoli Storage Manager API Linux x86_64	`TIVsm-API64.i386.rpm`

Follow these installation steps to install directly from the Data Protection for Oracle DVD:

Procedure

1. Log in using the root user ID.
2. Mount the Data Protection for Oracle DVD to */cdrom*:

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

3. Create a /cdrom directory on the Linux on System z® system if one does not exist, and mount /cdrom to the /cdrom directory on the Linux on System z system.

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

   where *hostname* is the system with the accessible DVD device.

4. Change to the <cdrom>/oracle/linux86_64/api directory where the installation package is located:

```
$ 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
```

6. Change to the cdrom/oracle/linux86_64 directory where the Data Protection for Oracle installable file is located:

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

   Note: cdrom is the drive where the DVD is mounted.

7. Enter the name of the installable file, TDP-Oracle.x86_64.bin, and press Enter to install Data Protection for Oracle:

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

   - To install the product in console mode, enter the following command:

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

   - To install the product in silent mode, enter the following command:

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

   - To install the product in GUI mode, enter the following command:

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

   Typically the file name is TDP-Oracle.x86_64.bin, however, if the installable file was downloaded from the FTP site, the file name might be different.

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

Installing on a Linux on System z system

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

Before you begin

If you must uninstall a previous version, see the information that is provided:

Uninstall any previous version of Data Protection for Oracle, or the Tivoli Storage Manager API, before you install a new or updated version, but do not delete the license enablement file.

About this task

All installable files are stored in the `/media/oracle/linuxz64` directory.

Table 7. Linux on System z (64-bit environment) default installation directories

Linux	Default Installation Directories
Data Protection for Oracle Linux on System z	`/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 8. Data Protection for Oracle Linux on System z (64-bit environment) and Tivoli Storage Manager installable files and packages

Component	Installable file or package
Data Protection for Oracle Linux on System z base code, license, utilities	`TDP-Oracle.s390x.bin`
Tivoli Storage Manager API Linux on System z	`TIVsm-API64.s390.rpm`, or `TIVsm-API64.s390x.rpm`

Use the following procedure to install directly from the Data Protection for Oracle DVD:

Procedure

1. Log in using the root user ID.
2. Mount the Data Protection for Oracle DVD to `/media`:

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

3. Mount `/media` to the */media* directory on the Linux system. The */<media>* directory must exist on the Linux system:

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

Note: The `hostname` is the system with the accessible DVD device identified in Step 1.

4. Change to the <media>/oracle/linuxz64/api directory where the Tivoli Storage Manager API installation package is stored on the DVD:

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

5. To install the Tivoli Storage Manager API, issue the following command:

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

6. Change to the <media>/oracle/linuxz64 directory where the Data Protection for Oracle installable file is located:

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

   Note <media> is the drive where the DVD 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 the product in console mode, type in the following command, and press Enter:

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

   - To install the product in silent mode, type in the following command, and press Enter:

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

   - To install the product in GUI mode, type in the following command and press Enter:

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

   Typically the file name is TDP-Oracle.s390x.bin, however, if the installable file was downloaded from the FTP site, the file name might be different.

Installing on a Solaris SPARC or Solaris x86 system

Use these instructions to install Data Protection for Oracle on a Solaris SPARC or Solaris x86 operating system.

Before you begin

Uninstall any previous version of Data Protection for Oracle, or the Tivoli Storage Manager API, before you install a new or updated version, but do not delete the license enablement file.

About this task

All installable files are stored in the /cdrom/oracle/solaris directory.

Table 9. Solaris SPARC 64-bit default installation directories

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

Table 9. 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 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
Tivoli Storage Manager API 64-bit	TIVsmCapi.pkg

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

Procedure

1. With the DVD inserted, log in using the root user ID.
2. To install the Tivoli Storage Manager API, issue the command:

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

3. Change to the /cdrom/oracle/solaris directory where the Data Protection for Oracle installable file is located:

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

4. Enter the name of the installable file, TDPoracle64.bin, and press Enter to install Data Protection for Oracle:

   ```
   $ TDPoracle64.bin
   ```

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

   - To install the product in console mode, type in 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
     ```

Typically the file name is `TDPoracle64.bin`, however, if the installable file was downloaded from the FTP site, the file name might be different.

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

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

   b. Shut down all Oracle instances that use `$ORACLE_HOME`.
   c. Navigate to the `$ORACLE_HOME/lib` directory.
   d. Symbolically link the library file to `libobk.so` by using this command:

      ```
      $ 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.

Before you begin

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.

About this task

Review all configuration information before you run any configuration tasks.

Configuration with default settings

Use the Data Protection for Oracle quick configuration option to quickly configure with default settings and minimal configuration tasks. Setup time is minimized and you proceed quickly to a state where you can begin backing up your Oracle databases.

Before you begin

Install Data Protection for Oracle. For detailed installation instructions, see Chapter 2, "Data Protection for Oracle installation," on page 5.

After Data Protection for Oracle is installed, make sure that the following link exists:

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

About this task

Use the instructions 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, change the installation paths and library extensions in this procedure for the operating system in use.

See "Configuring Data Protection for Oracle" on page 19 for detailed instructions on how to customize Data Protection for Oracle for your environment and processing needs.

Procedure

1. 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 20.

2. In this 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 "Define Tivoli Storage Manager options in the client options file" on page 23.

3. Make sure the dsm.sys file for the backup-archive client /usr/tivoli/tsm/client/ba/bin64/dsm.sys is not linked with the API client dsm.sys file /usr/tivoli/tsm/client/api/bin64/dsm.sys. For some options, identical values in both files can lead to a malfunction.

4. 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 system that 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.

5. Make sure that 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 in the /usr/tivoli/tsm/client/oracle/bin and /usr/tivoli/tsm/client/api/bin directories.

6. Change to the /usr/tivoli/tsm/client/oracle/bin64 directory and run the **tdpoconf password** command as the <oracle user> to generate the password file.

   For more information about this command, see "**password** command" on page 46.

7. Run the **tdpoconf showenvironment** command to view and confirm your configuration.

   For more information about this command, see "**showenvironment** command" on page 47.

8. As <oracle user>, run the 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, 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 "RMAN and Data Protection for Oracle" on page 31.

Configuring Data Protection for Oracle

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

Procedure

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.

Results

If you would like to configure Data Protection for Oracle using default settings, see "Configuration with default settings" on page 17 for instructions.

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.

About this task

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 recognizes within an RMAN script is the fully qualified path name to the `tdpo.opt` file. Therefore, some RMAN scripts must 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)'
```

For further information about RMAN scripts, see "Editing RMAN scripts" on page 32 for further information. Note, 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 uppercase characters only.

If the **`TDPO_OPTFILE`** variable is not provided, Data Protection for Oracle uses the `tdpo.opt` file 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 that are defined in the `tdpo.opt` file.
- By default, the `tdpo.opt` file is in the directory where Data Protection for Oracle is installed.
- You can specify options in the `tdpo.opt` file in both uppercase or lowercase type. However, the **`TDPO_OPTFILE`** variable must be specified in uppercase characters only.

Available Data Protection for Oracle options

The options that can be set in the tdpo.opt file for Data Protection for Oracle are described.

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.

If the Tivoli Storage Manager errorlogname option is specified in the dsm.sys file (for the stanza that is used by Data Protection for Oracle), the errorlogname option overrides the value that is 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 Oracle users.

For error log files, create a directory for the error logs and have the dsmi_log option point to that directory. The user who is running 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 the 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 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 1-1024 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 that is 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, when passwordaccess generate is specified, Data Protection for Oracle uses the value of the passworddir option that is specified in the dsm.sys file and does not use the tdpo_pswdpath option. However, the directory that is 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 that is used during operations with the Tivoli Storage Manager server. The node name can contain a string of 1-1024 characters. You must use a node name that is different from the backup-archive client node name.

It is the Tivoli Storage Manager API and not Data Protection for Oracle that negotiates which login credentials 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. It then ignores the value of the `nodename` option that is specified in the `dsm.sys` file. If you do not specify a value for the `passwordaccess` option, the default value is `prompt`. 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 with 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. If the password for the Data Protection for Oracle node is unknown because of the `passwordaccess generate` setting, you can reset the password for the production node on the Tivoli Storage Manager server. After the password is reset, use the new password to run the **tdpoconf password** command. Reset the password on the production system to set the password for the next backup. Also, reset the password on the alternate system to set the password for the restore operation.
- 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 that you want to use to display dates.

You can specify a number, 0 - 5. The default value is 1.

`0` Use the locale-specified date format.

`1` `MM/DD/YYYY` (Default value)

`2` `DD-MM-YYYY`

`3` `YYYY-MM-DD`

`4` `DD.MM.YYYY`

`5` `YYYY.MM.DD`

tdpo_num_fmt

This option specifies the format that you want to use to display numbers. You can specify a number, 1 - 6. The default value is 1.

1 1,000.00 (Default value)

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 that you want to use to display time.

You can specify a number, 0 - 4. The default value is 1.

0 Use the locale-specified time format.

1 23:00:00 (Default value)

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 that is used for copy 2 in the RMAN duplex copy command.

tdpo_mgmt_class_3

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

tdpo_mgmt_class_4

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

Note: See "The Duplex Copy function" on page 35 for specific details on using management class options.

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

The Data Protection for Oracle node name and password when 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.

About this task

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

- Data Protection for Oracle node name:

  The node name identifies the instance on which Data Protection for Oracle is installed. 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.
- Initial password:

  Specify the password that 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, define a unique policy domain 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, specify a different domain for the 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`. This enables the Data Protection for Oracle node to compress objects before it sends 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, 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.

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:

About this task

- These options are defined in the Tivoli Storage Manager client system options file `dsm.sys`, and client user options file `dsm.opt` by default.
- Note, the Tivoli Storage Manager client user options file `dsm.opt` by default, that you must edit for Data Protection for Oracle is in the directory that is 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 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 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 to operate Data Protection for Oracle.

Specify the required options in the Tivoli Storage Manager client system options file `dsm.sys` by default 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 as the default. When you specify `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 you specify these values, use the **tdpoconf password** command as root user to create the password and password file `TDPO.nodename` on the local system. When `passwordaccess prompt` is specified, the user must be aware of the password expiration date. A backup failure might 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 with 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 you are running unattended scheduled backups because it ensures that the backup never fails with an expired password. When you are 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 you are specifying `passwordaccess generate`:

- `tdpo_node`
- `tdpo_owner`
- `tdpo_pswdpath`

After you specify `passwordaccess generate` and the other 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 that you want to use to identify a stanza that contains the options that are used for connecting to the Tivoli Storage Manager

server. The name must match the name that is specified by the servername option in the dsm.opt file. Note, the name does not have to be the actual name of a Tivoli Storage Manager server.

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, 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 in the directory that is specified by the dsmi_orc_config option:

servername

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

Other configuration options to consider

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

You can specify other options in the Tivoli Storage Manager client system options file dsm.sys.

compression

Specify whether the Tivoli Storage Manager API compresses data before it sends 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 allowed only if the Tivoli Storage Manager administrator leaves the compression decision to the node. Enabling compression affects performance in three ways:

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

When any of the following conditions exist, you should specify yes:

- 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.

When any of the following conditions exist, you should specify no:

- The system that is running Data Protection for Oracle has a processor overload. The added processor 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 is stored.

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. 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 it sends 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 if objects are 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 must use either one option or the other, but not both options together.

The deduplication and enableclientencryptkey options are also mutually exclusive. Therefore, you must 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 must 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, which is used by the Oracle node, would be as follows:

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

Make sure that the **FORMAT** parameter specifies a unique name for the backup. If the object name exists on the Tivoli Storage Manager server, the backup might fail with an RC=8 error that is 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 to restore an encrypted object.

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

You can specify the databases that 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, 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 about the enableclientencryptkey option.

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

Related concepts:

"LAN-free data transfer" on page 3

Define Tivoli Storage Manager policy requirements

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

About this task

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 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. Set the following Tivoli Storage Manager backup copy group options:

- `verdeleted 0`
- `retonly 0`

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 with the Data Protection for Oracle interface or with the `tdposync` utility. Note, an inactive backup object cannot be restored through RMAN with 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 with the Data Protection for Oracle interface or with the `tdposync` utility. Note, 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 might be different from the wanted settings for the regular Tivoli Storage Manager backup-archive clients, you must have a different management class that is defined for Data Protection for Oracle. You must define a separate policy domain where the default management class has the required settings. 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 that is 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 that is defined in the `tdpo_fs` option in the `include/exclude` statement.

All the files that are 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 about defining or updating Tivoli Storage Manager policy domains and copy groups.

Initialize the password with a Tivoli Storage Manager server

The administrator must run the `tdpoconf` utility program to set the password before you use Data Protection for Oracle.

Related reference:

"tdpoconf utility" on page 46

Chapter 4. Protecting Oracle Server data

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

Before you begin

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

RMAN and Data Protection for Oracle

You can run full or partial, offline, or online backups with Oracle. When 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.

About this task

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

Starting RMAN

Use RMAN to back up and restore an Oracle database.

About this task

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

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

RMAN starts 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 example, RMAN creates a log file, `bkdb.log`, in the current working directory. If an error occurs, the error stack is logged to the log file.

Attention: For backup and restore operations in a Linux environment, Oracle recommends that the Oracle *LD_ASSUME_KERNEL* variable is 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 is displayed:

```
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)
```

Editing RMAN scripts

You must edit existing RMAN scripts to use **TDPO_OPTFILE**=*fully qualified path and file name of options file* variable in place of other environment variables.

About this task

Data Protection for Oracle does not recognize environment variables that are specified in an RMAN script. The only environment variable Data Protection for Oracle recognizes in an RMAN script is the fully qualified path name to the `tdpo.opt` file. The *TDPO_OPTFILE* variable can be specified in either lowercase 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.

Sending options with 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.

Before you begin

To send options from the Tivoli Storage Manager to the Tivoli Storage Manager API, you must specify the **send** command in an RMAN script.

About this task

Use the **send** command to set 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. 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 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 does not occur.
- The ENABLECLIENTENCRYPTKEY and DEDUPLICATION options are also mutually exclusive. If both options are defined, client-side data deduplication does not occur.
- You can specify any Tivoli Storage Manager API option with the **send** command.

Procedure

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. 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';
```

Results

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. The message returns an 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
- FASTQUERYBACKUP
- E2AOBJNAME
- ALLOWWILDCARDCH
- DEDUPCACHEPATH
- ENABLEDEDUPCACHE
- EXCLUDE.ENCRYPT
- FORCEFAILOVER
- ENABLEARCHIVERETENTIONPROTECTION

Related tasks:

"RMAN script examples"

RMAN script examples

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

Example

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 system have multiple network cards, you can back up your data with multiple network paths to improve network throughput. Your environment is set up as follows:

- The Oracle system 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 or 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 servers because it cannot be restored.

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 eight 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.

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. The backup can then be stored on different backup media.

About this task

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 that is 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 about the use of this Oracle parameter.

For example, to create four backup copies:

Procedure

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.

Results

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.

Note: Take note of the considerations provided:

- The duplex copy feature does not use *include* statements. It uses the management classes that are specified in the `tdpo.opt` file.
- You receive an error message if you specify **`set duplex =4`** in the RMAN backup script and do not define enough `tdpo_mgmt_class` options in the `tdpo.opt` file.
- To place duplicate copies on different media:

  - Make sure that the storage pool information for each backup copy group within the management classes is not the same.
  - Make sure that backups from these different storage pools are not moved to the same storage pool later.
- Duplicate data is sent across the network.
- 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 is a multiple of the duplex value. As a result, make sure that 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 can use on the Tivoli Storage Manager server during a backup operation. View the maximum mount points that are 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 about this option.

Review your current Oracle documentation about the duplex backup function.

Removing old backups

Data Protection for Oracle uses the Tivoli Storage Manager backup repository. Each database backup creates an object with a unique name. Since these objects have unique names, they always remain active and never expire. The database administrator (DBA) can control and coordinate copies that are removed from the Tivoli Storage Manager server with RMAN.

Before you begin

Ensure that **backdelete**=*yes* is specified by the Tivoli Storage Manager administrator during registration of your node. Specifying this parameter gives you permissions to delete backup objects.

About this task

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

Removing a backup example

A sample script for removing an old backup is provided.

About this task

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;

}
```

Refer to the Oracle RMAN manual for more information about the **change** command and its options.

Setting up a schedule example

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

About this task

For consistency, this procedure uses specific information. However, you can define a command file with any set of commands you choose. You can then 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.

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.

Procedure

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 you proceed 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 on page 37:

   ```
   define association PolicyA1 daily_orcbkup NodeA1
   ```

   The following message must display before you proceed to "Setting up a schedule on the client machine NodeA1":

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

Results

- A backup schedule is now defined on the Tivoli Storage Manager server.
- The backup schedule runs the scheduler backup script `schedbkdb.scr`. The backup scripts run the command script `mysched.scr`, which runs the RMAN backup script `bkdb.scr` in the `/home/oracle/sched` directory.
- The backup runs daily 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.

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`.

About this task

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 becomes out of sync between Data Protection for Oracle and the scheduler. Specify **passwordaccess** `generate`. If **passwordaccess** `prompt` is already specified, you can prevent password expiration by typing in 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.

Procedure

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

1. Create a `dsm.sys` file in the `/usr/tivoli/tsm/client/ba/bin` directory if one does not exist. Add the following `servername` stanzas:

a. Add a servername stanza for the file system backups that are 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 that is 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 that are 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 that 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 that 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 script is the scheduler backup script that was defined for the scheduler in "Setting up a schedule on the Tivoli Storage Manager server" on page 37. The scheduler backup script runs the command script mysched.scr, which runs the RMAN backup script bkdb.scr. This example shows 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.scris 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. 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. Log in as the root user to the system 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.

What to do next

For security, in a default installation, the Tivoli Storage Manager client's trusted communications agent (**dsmtca**) allows both root access for the scheduler and non-root access for Data Protection for Oracle to read and write the same password file `TSM.PWD` in **passworddir**. If your system is set up otherwise, see the *Enable non-administrators to manage their own data* topic in the Tivoli Storage Manager client documentation.

Create **servername** stanzas in both `dsm.sys` files by the same **servername** as in the `dsmi_orc_config` file which is set in your `TDPO_OPTFILE`.

For Data Protection for Oracle, the stanza must be in the following file path: `/usr/tivoli/tsm/client/api/bin64/dsm.sys`

For the scheduler associated with Data Protection for Oracle a stanza by the same **servername** must be in the following file path: `/usr/tivoli/tsm/client/ba/bin64/dsm.sys`

Ensure the following 6 options are identical in both files:

- `servername TSMOracle`
- `tcpserveraddress site.xyzinc.com`
- `tcpport 1500`
- `nodename NodeA1`
- `passwordaccess generate`
- `passworddir /home/oracle`

Other options can or even must be different in both files.

To the stanza servername TSMOracle in /usr/tivoli/tsm/client/api/bin64/dsm.sys, you can add options specific to Data Protection for Oracle, for example:

```
INCLUDE /adsmorc/.../DB* mgmtclassnameforDBs
INCLUDE /adsmorc/.../LOG* mgmtclassnameforLogs
enablelanfree yes
lanfreecommmethod sharedmem
* errorlogname /home/oracle/dsierror__NodeA1.log
```

When the option DSMI_LOG is set in your TDPO_OPTFILE to point to a directory with read and write permissions for the Oracle user, you don't need to set **errorlogname** in /usr/tivoli/tsm/client/api/bin64/dsm.sys.

However, if you decide to set **errorlogname** for Data Protection for Oracle, then its value must be different from **errorlogname** in /usr/tivoli/tsm/client/ba/bin64/dsm.sys, to prevent concurrent write access to the same file by Data Protection for Oracle running as oracle user and the scheduler running as root.

To the stanza servername TSMOracle in /usr/tivoli/tsm/client/ba/bin64/dsm.sys you may add scheduler specific options, for example:

```
schedmode prompted
tcpclientport 1502
schedlogname /home/root/dsmsched_NodeA1.log
* commmethod tcpip <- unnecessary because it's default.
errorlogname /home/root/dsmerror_NodeA1.log
```

When using passwordaccess generate, the options TDPO_NODE, TDPO_OWNER, and TDPO_PSWDPATH must not be set in your TDPO_OPTFILE.

The temporary switching from passwordaccess generate to passwordaccess prompt can become necessary when existing Oracle backups in Tivoli Storage Manager storage with a certain OWNER need to be accessed by a user with a different user name, for example, when restoring a database to a system with another Oracle user name. In this type of situation you can avoid the typical restore error ANS1302E (RC2). No objects on server match query by setting /usr/tivoli/tsm/client/api/bin64/dsm.sys to passwordaccess prompt, because this allows specifying a **TDPO_OWNER** in your **TDPO_OPTFILE**, who is different from the name of the user who is restoring the data.

For this scenario you also have to complete the following steps:

1. Set **TDPO_NODE** and **TDPO_PSWDPATH** in your **TDPO_OPTFILE**.
2. Rerun **tdpoconf password**.

Querying backup objects

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

About this task

When you issue the **tdposync query** command, information about a backup object is displayed. Information is listed including the size and date of the backup, and whether the object is compressed, encrypted, or deduplicated by the Tivoli Storage Manager during the backup operation.

Related tasks:

"Data deduplication with Data Protection for Oracle"

Related reference:

"**Query** command" on page 53

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 on either the client or server to use with the **DEDUP** parameter on the **REGISTER NODE**, or **UPDATE NODE** server command.

Setting up 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.

About this task

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
```

Results

After you 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 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 use either one option or the other, but not both options together.
- The **deduplication** and **enableclientencryptkey** options are also mutually exclusive. Therefore, you can 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" on page 44

Related reference:

"**Query** command" on page 53

Determining total data reduction

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

About this task

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
  ```

Results

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 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
```

Chapter 5. Commands and utilities for Data Protection for Oracle

The Data Protection for Oracle commands and utilities are used to protect Oracle Server data.

tdpoconf and tdposync utilities

Set up and maintain Data Protection for Oracle with the tdpoconf and tdposync utilities. Find the utilities in the directory where Data Protection for Oracle is installed.

Use the Data Protection for Oracle utilities to do the following tasks:

- Set up and maintain Data Protection for Oracle with the tdpoconf utility. The utility is also used for password maintenance.
- Synchronize the RMAN catalog and Oracle control file by using tdposync. The utility is used to delete Oracle backups that are stored on the Tivoli Storage Manager.
- Query objects that are backed up on the Tivoli Storage Manager by using the tdposync utility.

Command line syntax and characteristics

Guidelines for the command line syntax for the Data Protection for Oracle utilities.

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 uppercase.
- Optional parameters begin with a dash (-).
- Optional parameters can display in any order.
- Some keyword parameters require a value that is 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 quotation marks.

tdpoconf utility

The tdpoconf utility provides setup tasks for configuring Data Protection for Oracle. The utility uses the tdpo.opt file that is stored in the installation directory to centralize information for setup purposes.

Use the following commands with the tdpoconf utility:

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

password command

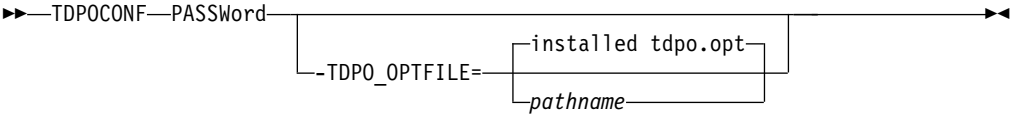
Use the **password** command to create a password or change an existing password on the Tivoli Storage Manager server. You are prompted to enter both the old and new passwords when you use this utility to change the password.

Be aware of the following requirements that are 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 is the value that is specified by the tdpo_node option in the Data Protection for Oracle options file specified with the *TDPO_OPTFILE* variable. This file is in the directory that is 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 runs 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 file is created in the directory that is specified by the passworddir option that is 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 that is specified in the dsm.sys file. If the tdpo_pswdpath option is specified in the tdpo.opt file, it is ignored. For more information, see the description of the tdpo_pswdpath option in "Available Data Protection for Oracle options" on page 20.

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

An output example of the **tdpoconf password** command is provided:

```
************************************************************
*  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.
```

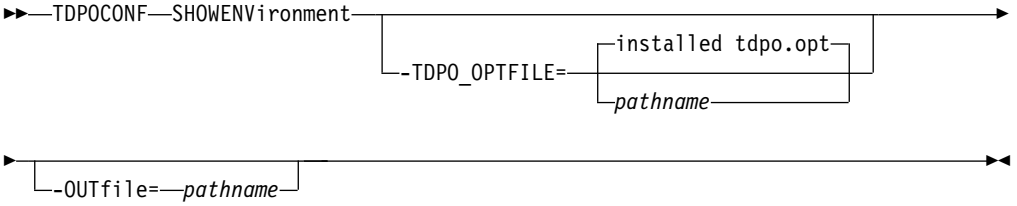
`showenvironment` command

Use the **showenvironment** command to query the Tivoli Storage Manager server with the options that are 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 if you are troubleshooting setup errors for Data Protection for Oracle. If the password file is not initialized properly, the output of the `tdpoconf showenvironment` command reports the error.

Tip: To ensure that the environment is set up correctly before you use RMAN, direct the setup output to a file with the `–outfile` option.

Syntax



Optional parameters

-TDPO_OPTFILE=*pathname*
This parameter specifies the fully qualified path name to the `tdpo.opt` file. The options file 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 in the output on screen.

Example

The following example shows the output of the **tdpoconf showenvironment** command:

```
Data Protection for Oracle Information
 Version:              7
 Release:              1
 Level:                3
 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.
```

Tip: The `Server Name` identifies the Tivoli Storage Manager server stanza in the `dsm.sys` file, not the name of the Tivoli Storage Manager server.

tdposync utility

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 by removing unwanted objects from the Tivoli Storage Manager, and reclaim space on the server.

Attention: Deleted files and inactive files cannot be restored. When you are using this utility to delete files, ensure that you do not log in to the wrong node name. You might query a different database than intended, and delete files in error. Ensure that the node name in the PICK window is the one you need. See "Optional parameters" on page 50 and "PICK window" on page 52 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 they are deleted, RMAN can no longer identify these backups through the catalog or control file even though the file 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 that are marked as expired, RMAN still considers these objects as existing. If you run the **tdposync** utility 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 the 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 a list of files that exist on the Tivoli Storage Manager server 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

To run the tdposync utility successfully, resynchronize the Oracle catalogs with the target databases. If you are using multiple Oracle catalogs, use the **numcatalogs** parameter. Each Oracle database must be backed up to the Tivoli Storage Manager server.

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

- Resynchronize Oracle catalogs with the target databases before you run 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.
- By default, Data Protection for Oracle prompts you to synchronize with one Oracle catalog at a time. 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 the 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, 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 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.

  Restriction: 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, one for each target database. The possibility of showing wrong information in the PICK window is minimized.

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

- 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:

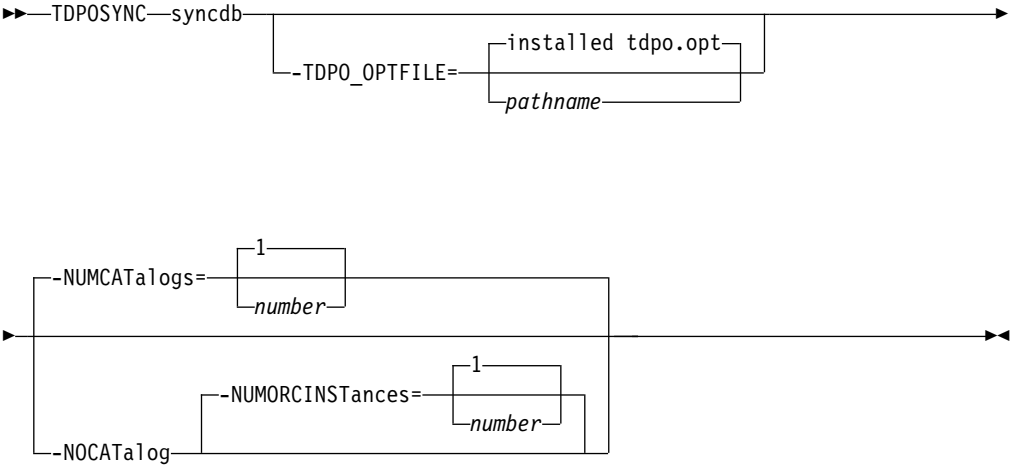
  ```
  login/password@connectstring
  ```

  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.

syncdb command

The **syncdb** command synchronizes Oracle catalog databases or the Oracle control file with the Tivoli Storage Manager server.

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 do the original backup operations.

-NUMCATalogs=*number*

This parameter specifies the number of Oracle catalog databases that you want to synchronize. It 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.

You are prompted for start and end dates for your query. Then you are prompted for the following information for each catalog:

- `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, the following information is requested:

- `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 shows all objects that are not in sync.

Example

Synchronize the Tivoli Storage Manager database with the RMAN catalog and the RMAN backup history, with the **tdposync syncdb** command. The following output is displayed:

```
Command: TDPOSYNC syncdb

Output:
IBM Tivoli Storage Manager for Databases:
Data Protection for Oracle
Version 7, Release 1, Level 0.0
```

```
(C) Copyright IBM Corporation 1997, 2013. All rights reserved.

From Date (01/01/1990): 01/01/2013
To Date (01/05/2013): 12/12/2013

Catalog 1 User Name: rman
Catalog 1 Password: rman
Catalog 1 Connect String: rman
```

Synchronize the Tivoli Storage Manager database with the RMAN backup history and the Oracle control file using the **tdposync syncdb** command. The following output is displayed:

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

Output:
IBM Tivoli Storage Manager for Databases:
Data Protection for Oracle
Version 7, Release 1, Level 0.0
(C) Copyright IBM Corporation 1997, 2013. All rights reserved.
From Date (01/01/1990): 01/01/2013
To Date (01/05/2013): 12/12/2013

Oracle Database 1 User Name: OrcUser1
Oracle database 1 Password: OrcUser1pw
Oracle database 1 Connect String: Oracle_DB_A

Oracle Database 2 User Name: OrcYser2
Oracle database 2 Password: OrcUser2pw
Oracle database 2 Connect String: Oracle_DB_B
```

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 you are selecting files for deletion. If you are unsure that the files in question are out of synchronization, do further research before you delete them. Deleted files cannot be restored.

Example

The PICK window shows the node names, and names the files that are backed up. The following example shows the output that is displayed for a node called `AGENT_NODE`:

```
Node Name: AGENT_NODE
  Owner Name: oracle10g

              Backup Date            Size        Backup Name
        ---------------------------------------------------------------
     1. | 01/09/2014  09:19:59       108.01MB    /adsmorc//1kc2cnfv_1_1
     2. | 01/02/2014  11:36:20       56.25MB     /adsmorc//4kc3cnfv_1_1
     3. | 01/02/2014  07:14:30       102.00MB    /adsmorc//4qcgdhfr_1_1
     4. | 01/02/2014  07:21:38       78.10MB     /adsmorc//4ocf8999_1_1
     5. | 01/09/2014  11:00:11       10.99MB     /adsmorc//4ocf8999_1_2
     6. | 01/09/2014  11:00:12       32.07MB     /adsmorc//4ocf8999_1_3
     7. | 01/09/2014  11:00:13       623.90MB    /adsmorc//4rch25jk_1_1
     8. | 01/09/2014  11:00:14       441.61MB    /adsmorc//4rch25jk_1_2
     9. | 01/09/2014  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 that are selected for deletion are marked by a plus (+). To delete selected files:

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

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

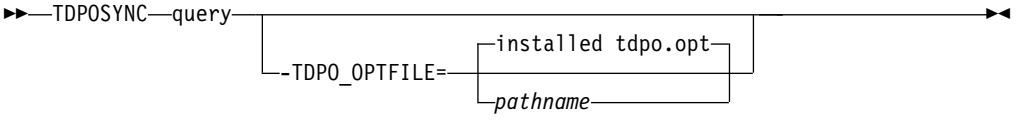
`Query` command

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

The **query** command uses the options that are 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 (`/Program Files/Tivoli/TSM/AgentOBA64/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.

The **Owner** 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
Lists whether an object was compressed during the backup operation.

Encryption Type
Lists 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
Lists whether an object underwent client-side data deduplication.

Examples

Use the `tdposync query` command to find information about backed up objects, encryption type and data deduplication.

Query the Tivoli Storage Manager server for information about objects that are backed up
The command to be run is `tdposync query`.

The following output is displayed:

```
IBM Tivoli Storage Manager for Databases:
Data Protection for Oracle
Version 7, Release 1, Level 1.0
(C) Copyright IBM Corporation 1997, 2014. All rights reserved.

From Date (01/01/2014):

To Date (07/02/2014):

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

Name ............................... /adsmorc//df_722435657_35_1
Owner...............................
Size ............................... 2,010 KB
Creation Date / Time ............... 07/02/2013 10:08:20
Compressed ......................... Yes
Encryption Type .................... None
Client-deduplicated ................ No

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

...
```

Finding the encryption type

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.

Finding data deduplication information

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

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 IBM Tivoli Storage Manager family of products includes the following accessibility features:

- Keyboard-only operation using standard operating-system conventions
- Interfaces that support assistive technology such as screen readers

The command-line interfaces of all products in the product family are accessible.

Tivoli Storage Manager Operations Center provides the following additional accessibility features when you use it with a Mozilla Firefox browser on a Microsoft Windows system:

- Screen magnifiers and content zooming
- High contrast mode

The Operations Center and the Tivoli Storage Manager server can be installed in console mode, which is accessible.

The Operations Center help system is enabled for accessibility. For more information, click the question mark icon on the help system menu bar.

Vendor software

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

IBM and accessibility

See the IBM Human Ability and Accessibility Center (http://www.ibm.com/able) for information about the commitment that IBM has to accessibility.

Notices

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

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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

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

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

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

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

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
US

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

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

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

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

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

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

```
Portions of this code are derived from IBM® Corp. Sample Programs.
© Copyright IBM® Corp. _enter the year or years_. All rights reserved.
```

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 www.ibm.com/legal/copytrade.shtml.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linear Tape-Open, LTO, and Ultrium are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

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

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

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

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights Except as expressly granted in this permission, no other permissions,

licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled “Cookies, Web Beacons and Other Technologies,” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Glossary

A glossary is available with terms and definitions for the IBM Tivoli Storage Manager family of products.

See Tivoli Storage Manager glossary (http://www.ibm.com/support/knowledgecenter/SSGSG7_7.1.3/tsm/glossary.html).

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

Index

T

U

V

Product Number: 5608-E04

Printed in USA