

IBM Storage Protect for Databases

Oracle Installation and User's Guide for UNIX and Linux

8.2.0



Contents

List of Tables	3
Who should read this guide	6
Publications	6
What's new	6
Protection for Oracle Server databases	7
Overview of Data Protection for Oracle	7
RMAN and Data Protection for Oracle	7
LAN-free data transfer	7
Migration and coexistence with Data Protection for Oracle	7
Automated failover for data recovery	8
Data Protection for Oracle installation	10
Installing Data Protection for Oracle	10
Installation prerequisites	10
Installing on an AIX® 64-bit operating system	11
Installing on a 64-bit HP-UX Itanium™ system	13
Installing on a Linux™ x86_64 system	14
Installing on a Linux™ on System z® system	15
Installing on a Solaris SPARC or Solaris x86 system	16
Configuring Data Protection for Oracle	19
Configuration with default settings	19
Configuring Data Protection for Oracle	20
Define Data Protection for Oracle options in the tdpo.opt file	21
Register the Data Protection for Oracle node to an IBM® Storage Protect server	24
Define IBM® Storage Protect options in the client options file	24
Define IBM® Storage Protect policy requirements	28
Initialize the password with an IBM® Storage Protect server	29
Protecting Oracle Server data	31
RMAN and Data Protection for Oracle	31
Starting RMAN	31
Editing RMAN scripts	32
The Duplex Copy function	34
Removing old backups	35
Setting up a schedule example	36
Setting up a schedule on the IBM® Storage Protect server	36
Setting up a schedule on the client machine NodeA1	37
Querying backup objects	40
Data deduplication with Data Protection for Oracle	40
Overview of data deduplication	40
Setting up for client-side data deduplication	41
Determining total data reduction	42
Commands and utilities for Data Protection for Oracle	44
tdpoconf and tdposync utilities	44
Command line syntax and characteristics	44
tdpoconf utility	44
tdposync utility	47
Accessibility features for the IBM® Storage Protect product family	54
Overview	54
Keyboard navigation	54
Interface information	54
Vendor software	54
Related accessibility information	54
Notices	55
Trademarks	56
Terms and conditions for product documentation	56
Privacy policy considerations	57
Glossary	58
Index	59

List of Tables

Table 1: AIX® 64-bit default installation directories	11
Table 2: Data Protection for Oracle AIX® 64-bit, utilities, and IBM® Storage Protect API package names	11
Table 3: HP-UX Itanium™ 64-bit default installation directories	13
Table 4: Data Protection for Oracle 64-bit and IBM® Storage Protect installable files and packages	13
Table 5: Linux™ x86_64 default installation directories	14
Table 6: Data Protection for Oracle Linux™ x86_64 and IBM® Storage Protect installable files and packages	14
Table 7: Linux™ on System z® (64-bit environment) default installation directories	15
Table 8: Data Protection for Oracle Linux™ on System z® (64-bit environment) and IBM® Storage Protect installable files and packages	15
Table 9: Solaris SPARC 64-bit default installation directories	17
Table 10: Data Protection for Oracle 64-bit and IBM® Storage Protect installable files and packages	17
Table 11	48

Note:

Before you use this information and the product it supports, read the information in “Notices” on page 55.

This edition applies to version 8, release 2 of IBM® Storage Protect for Databases: Data Protection for Oracle for AIX®, Linux™, HP-UX, or Solaris (product number 5725-X01) and to all subsequent releases and modifications until otherwise indicated in new editions.

About this publication

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

Data Protection for Oracle runs online or offline backups of Oracle 11g databases to IBM® Storage Protect storage. This integration with the RMAN Media Management API maximizes the protection of data, and provides a comprehensive storage management solution.

IBM® Storage Protect is a client/server licensed product that provides storage management services in a multiplatform computer environment.

Who should read this guide

The target audience for this publication includes system installers, system users, Oracle database administrators, IBM® Storage Protect administrators, and system administrators.

It is assumed that you have an understanding of the following applications:

- Oracle server
- IBM® Storage Protect server
- IBM® Storage Protect backup-archive client
- IBM® Storage Protect application programming interface

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

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

Publications

The IBM® Storage Protect product family includes IBM® Storage Protect Plus, , , and several other storage management products from IBM®.

To view IBM® product documentation, see [IBM® Documentation](#).

Data Protection for Oracle updates V8.1.23

This document provides information about what's new or what has changed in Data Protection for Oracle version 8.1.23.

What's new

The official product name IBM Storage® Protect for Databases - Data Protection for Oracle is now changed also in the user interfaces, command output, and other code-related messages.

Protection for Oracle Server databases

A brief overview of IBM® Storage Protect for Databases: Data Protection for Oracle is provided.

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 IBM® Storage Protect server.

Data Protection for Oracle currently supports Oracle 11g databases with the Oracle Recovery Manager. See [“Data Protection for Oracle installation” on page 10](#) 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 IBM® Storage Protect server. The IBM® Storage Protect 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 IBM® Storage Protect API calls to the IBM® Storage Protect 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 IBM® Storage Protect Storage Agent. Running Data Protection for Oracle in a LAN-free environment avoids constraints of the network. The load on the IBM® Storage Protect 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 an IBM® Storage Protect 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 information

[Configuring Data Protection for Oracle](#)

[Editing RMAN scripts](#)

Automated failover for data recovery

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

The IBM Storage® Protect 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 IBM Storage® Protect 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 IBM Storage® Protect Snapshot, 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 IBM Storage® Protect 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.

Data Protection for Oracle installation

Install IBM® Storage Protect 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 *IBM Storage Protect™ 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 IBM Storage Protect™ 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 IBM® Storage Protect 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 IBM® Storage Protect 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 IBM Storage Protect™ 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	<code>/usr/tivoli/tsm/client/oracle/bin64</code>
Data Protection for Oracle Utilities	<code>/usr/tivoli/tsm/client/oracle/bin64</code>
IBM® Storage Protect API 64-bit	<code>/usr/tivoli/tsm/client/api/bin64</code>

Table 2: Data Protection for Oracle AIX® 64-bit, utilities, and IBM® Storage Protect API package names	
Package	Package Name
Data Protection for Oracle 64-bit	<code>tivoli.tsm.client.oracle.aix.64bit</code>
Data Protection for Oracle Utilities	<code>tivoli.tsm.client.oracle.tools.aix.64bit</code>
Electronic License Agreement	<code>tivoli.tsm.loc.client.oracle.aix.64bit.ela</code>
IBM® Storage Protect API 64-bit	<code>tivoli.tsm.client.api.aix.64bit</code>

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 IBM® Storage Protect API package (`tivoli.tsm.client.api.aix.64bit`) and press F7.

- d. Highlight the Electronic License Agreement (`tivoli.tsm.loc.client.oracle.aix.64bit.e1a`) and press F7.
 - i. Set **ACCEPT new license agreements** to Yes.
 - ii. Set **Preview new license agreements** to No for the installation to proceed.
 - iii. 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 IBM® Storage Protect 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 IBM® Storage Protect 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.e1a
```

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

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

- If you have not installed the IBM® Storage Protect 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
```

```
installp -acgXYd /usr/sys/inst.images  
tivoli.tsm.loc.client.oracle.aix.64bit.e1a
```

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

```
installp -acgXYd /usr/sys/inst.images  
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 IBM Storage Protect™ 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	<code>/opt/tivoli/tsm/client/oracle/bin64</code>
Data Protection for Oracle Utilities	<code>/opt/tivoli/tsm/client/oracle/bin64</code>
Data Protection for Oracle Messages	<code>/opt/tivoli/tsm/client/oracle/bin64</code>
IBM® Storage Protect API	<code>/opt/tivoli/tsm/client/api/bin64</code>

Table 4: Data Protection for Oracle 64-bit and IBM® Storage Protect installable files and packages	
Component	Installable file or package
Data Protection for Oracle 64-bit base code, license, utilities	<code>TDP0racle64.bin</code>
IBM® Storage Protect API	<code>TIVsmCapi64</code>

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 IBM® Storage Protect 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, `TDP0racle64.bin`, on the command line and press Enter.
 - To install the product in console mode, enter the following command, and press Enter:

```
$ TDP0racle64.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 IBM Storage Protect™ 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
IBM® Storage Protect API	/opt/tivoli/tsm/client/api/bin64

Table 6: Data Protection for Oracle Linux™ x86_64 and IBM® Storage Protect 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
IBM® Storage Protect API Linux™ x86_64	TIVsm-API64.i386.rpm

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

Procedure

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

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

- 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.

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

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

- Issue the following command to install the IBM® Storage Protect 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 IBM Storage Protect™ 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®	<code>/opt/tivoli/tsm/client/oracle/bin64</code>
Data Protection for Oracle Utilities	<code>/opt/tivoli/tsm/client/oracle/bin64</code>
Data Protection for Oracle Messages	<code>/opt/tivoli/tsm/client/oracle/bin64</code>
IBM® Storage Protect API	<code>/opt/tivoli/tsm/client/api/bin64</code>

Table 8: Data Protection for Oracle Linux™ on System z® (64-bit environment) and IBM® Storage Protect installable files and packages	
Component	Installable file or package
Data Protection for Oracle Linux™ on System z® base code, license, utilities	<code>TDP-Oracle.s390x.bin</code>
IBM® Storage Protect API Linux™ on System z®	<code>TIVsm-API64.s390.rpm</code> , or <code>TIVsm-API64.s390x.rpm</code>

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 IBM® Storage Protect API installation package is stored on the DVD:

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

5. To install the IBM® Storage Protect 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 IBM Storage Protect™ 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
Data Protection for Oracle Utilities	/opt/tivoli/tsm/client/oracle/bin64
Data Protection for Oracle Messages	/opt/tivoli/tsm/client/oracle/bin64
IBM® Storage Protect API 64-bit	/opt/tivoli/tsm/client/api/bin64

Table 10: Data Protection for Oracle 64-bit and IBM® Storage Protect installable files and packages	
Component	Installable file or package
Data Protection for Oracle 64-bit base code, license, utilities	TDPoracle64.bin
IBM® Storage Protect API 64-bit	TIVsmCapi.pkg

Follow these instructions to install the IBM® Storage Protect 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 IBM® Storage Protect 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.

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 an IBM Storage Protect™ 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 [“Data Protection for Oracle installation” on page 10](#).

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

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

Note: If you are using Linux as your operating system, this link is not required.

About this task

Use the instructions to configure Data Protection for Oracle. Change the listed installation paths and library extensions according to the operating system you are using.

See [“Configuring Data Protection for Oracle” on page 20](#) for detailed instructions on how to customize Data Protection for Oracle for your environment and processing needs.

Procedure

1. Depending on your operating system, change to one of the following directories:
 - AIX® 64-bit operating system: /usr/tivoli/tsm/client/oracle/bin64
 - Linux operating system: /opt/tivoli/tsm/client/oracle/bin64
 - Windows™ 64-bit Server system: C:\Program Files\Tivoli\TSM\Agent0BA64
2. Copy the tdpo.opt.smp file to tdpo.opt.
3. Edit the tdpo.opt file to include these options:
For UNIX and Linux, these instructions use AIX® 64-bit as the example operating system.

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

4. Create a dsm.opt file as follows:
In the /usr/tivoli/tsm/client/oracle/bin64 directory, create a dsm.opt file, then edit the file to include the following server stanza:

```
servername TSM0racle
```

For more information about this option and the dsm.opt file, see [“Define IBM Storage Protect options in the client options file” on page 24](#).

5. Change to the `/usr/tivoli/tsm/client/api/bin64` directory. Edit the `dsm.sys` file to include another server stanza with the following options:

```
servername TSM0racle
tcpserveraddress site.xyzinc.com
tcpport 1500
nodename NodeA1
passwordaccess generate
passworddir /home/oracle
```

Replace `site.xyzinc.com` with the IP address of the IBM® Storage Protect server to which Data Protection for Oracle backs up data. Replace `/home/oracle` with the Oracle database instance user's home directory.

For more information about these options and the `dsm.sys` file, see [“Define IBM Storage Protect options in the client options file” on page 24](#).

6. Register the node to the IBM® Storage Protect server with the following command:

```
REG nodename NodeA1 hostname_oracle password maxnumnp=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.

7. Make sure that the `<oracle user>` has the following permissions:
 - Read (`r`) permission to `/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/bin64` and `/usr/tivoli/tsm/client/api/bin64` directories.
8. 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 44](#).
9. Run the **`tdpoconf showenvironment`** command to view and confirm your configuration. For more information about this command, see [“showenvironment command” on page 46](#).
10. 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 an IBM® Storage Protect server.
3. Define IBM® Storage Protect options in the `dsm.opt` and `dsm.sys` files.
4. Define IBM® Storage Protect policy requirements.

5. Initialize the password with an IBM® Storage Protect server.

Result

If you would like to configure Data Protection for Oracle using default settings, see [“Configuration with default settings” on page 19](#) 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 IBM Storage Protect™ `errorlognameoption` is specified in the `dsm.sys` file (for the stanza that is used by Data Protection for Oracle), the `errorlognameoption` overrides the value that is specified by `dsmi_log`. If the `errorlognameoption` 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_logoption` 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 IBM® Storage Protect 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 IBM®

Storage Protect client user options file is in a directory other than the Data Protection for Oracle installation directory.

tdpo_enablescriptinput

You can automate the maintenance of IBM® Storage Protect Data Protection for Oracle without the need for user interaction. You can set the `tdpo_enablescriptinput` option to allow the **tdposync** utility to receive input from a script or batch file.

You can specify the following options:

Yes

The **tdposync** utility can receive redirected input that allows the utility to run in batch mode.

No

The **tdposync** utility must be run in interactive mode and requires user input to complete its run. This option is the default.

Attention: If you run the **tdposync** command interactively and the `tdpo_enablescriptinput` is set to **Yes**, the input for the Oracle password is shown in plain text. To obfuscate the password, set the `tdpo_enablescriptinput` to **No**.

tdpo_fs

Specify a file space name on the IBM® Storage Protect 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 IBM® Storage Protect 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 `passwordddir` 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 `passwordddir` 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 IBM® Storage Protect 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 IBM Storage Protect™ API and not Data Protection for Oracle that negotiates which login credentials to use with the IBM® Storage Protect 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 IBM Storage Protect™ 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 IBM® Storage Protect 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 IBM® Storage Protect 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 34 for specific details on using management class options.

Register the Data Protection for Oracle node to an IBM® Storage Protect server

The Data Protection for Oracle node name and password when required must be registered to the IBM® Storage Protect server before you can begin requesting backup and restore services. The process of setting up a node name and password with the IBM® Storage Protect server is called registration.

About this task

The following information is needed to register Data Protection for Oracle with the IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect administrator:

- The policy domain to which your client node belongs.
A policy domain contains policy sets and management classes that control how IBM® Storage Protect 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 IBM® Storage Protect administrator can specify the server to compress files. If the IBM® Storage Protect administrator specifies that the compression decision belongs to the client **compressionclient**, you must specify **compressionyes** 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 IBM® Storage Protect server.
- The authority to delete backup data from IBM® Storage Protect storage.
The Data Protection for Oracle node can only delete backed up data from IBM® Storage Protect storage if the IBM® Storage Protect administrator registers the node with `backdeleteauthority`. Specify the following option to allow `backdeleteauthority`:
`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 IBM® Storage Protect server when the next inventory expiration occurs. This expiration also makes the previously used storage space available for new use.

Define IBM® Storage Protect options in the client options file

You must define some IBM® Storage Protect options after the Data Protection for Oracle node is registered to the IBM® Storage Protect server:

About this task

- These options are defined in the IBM® Storage Protect client system options file `dsm.sys`, and client user options file `dsm.opt` by default.

- Note, the IBM® Storage Protect 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 `thedsmi_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 IBM® Storage Protect client system options file `dsm.sys` by default, must be in the directory where the IBM® Storage Protect API is installed.
- Data Protection for Oracle provides sample IBM® Storage Protect options files that you can modify for this purpose. These sample files are in the Data Protection for Oracle installation directory.
- The IBM® Storage Protect administrator can provide you with the TCP server address **tcpserveraddress** and communication method **commmethod** for connecting Data Protection for Oracle to the IBM® Storage Protect server.

Required options

You must set required IBM® Storage Protect client options to operate Data Protection for Oracle.

Specify the required options in the IBM® Storage Protect client system options file `dsm.sys` by default in the directory where the IBM® Storage Protect API is installed.

passwordaccess

Specify whether you want Data Protection for Oracle or the IBM Storage Protect™ 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 IBM Storage Protect™ API to manage the password, specify `passwordaccess generate`.

generate

The IBM Storage Protect™ API manages all password actions after the password is created with the **tdpoconf password** command. The IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect server.

tcpserveraddress

Specify the TCP/IP address in the stanza for the IBM® Storage Protect server to be used for Oracle backups. When the IBM® Storage Protect 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 IBM® Storage Protect server. Note, this option requires other IBM® Storage Protect options, depending on the communication method you specify.

Required option in the dsm.opt file

Specify this option in the IBM® Storage Protect client user options file `dsm.opt` in the directory that is specified by the `thedsmi_orc_configuration`:

servername

Specify a IBM® Storage Protect 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 IBM® Storage Protect client options that you can use when you are configuring Data Protection for Oracle.

You can specify other options in the IBM® Storage Protect client system options file `dsm.sys`.

compression

Specify whether the IBM® Storage Protect API compresses data before it sends it to the IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect 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 `compressionno` 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 IBM® Storage Protect server activity log file. Run the IBM® Storage Protect server **QUERY ACTLOG** command in the IBM® Storage Protect 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 IBM®

Storage Protect server. See the **SET ACTLOGRETENTION** command in the *IBM® Storage Protect 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 IBM® Storage Protect API deduplicates data before it sends it to the IBM® Storage Protect 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 IBM Storage Protect™ administrator allows client-side data deduplication.

You can determine if objects are deduplicated by running the **tdposync query** command or by examining the IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect server with the object in the server database. Although IBM Storage Protect™ 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.encrypt` statement 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 `enableclientencryptkeyyes`.
3. Specify `encryptiontypeAES128`, or `AES256`.
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® Storage Protect 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 information

[LAN-free data transfer](#)

Define IBM® Storage Protect policy requirements

Data Protection for Oracle requires special IBM® Storage Protect 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 IBM® Storage Protect backup storage pool have unique file names, they never expire on the IBM® Storage Protect server. As a result, Data Protection for Oracle requires the following IBM® Storage Protect policy domain settings:

Backup copy group values

Data Protection for Oracle provides the `tdposync` utility to remove unwanted backup objects from the IBM® Storage Protect server. Set the following IBM® Storage Protect backup copy group options:

- `verdeleted 0`
- `retonly 0`

When Data Protection for Oracle marks a backup object inactive, that object is deleted from the IBM® Storage Protect 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 IBM® Storage Protect 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

IBM® Storage Protect uses management classes to manage backups on the IBM® Storage Protect 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 IBM® Storage Protect 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 `incl excl` entry under the server stanza you use in the `dsm.sys` file:

```
incl excl /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 `thetdpo_fsoption`. If a file space name other than the default value `adsmorc` is used:

- a. You must specify the file space name with `thetdpo_fsoption`.
- b. You must specify the file space name that is defined in `thetdpo_fsoption` 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 IBM® Storage Protect storage, so an archive copy group is not required, although it can exist.

See your IBM® Storage Protect administrator or see the *IBM® Storage Protect Administrator's Guide* for more information about defining or updating IBM® Storage Protect policy domains and copy groups.

Initialize the password with an IBM® Storage Protect server

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

Related information

tdpoconf utility

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 IBM® Storage Protect server through Data Protection for Oracle.

About this task

Data Protection for Oracle provides an interface between Oracle Media Management API calls and IBM® Storage Protect 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 IBM® Storage Protect server activity log file. Run the IBM® Storage Protect server **QUERY ACTLOG** command in the IBM® Storage Protect 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 IBM Storage Protect™ options to the IBM Storage Protect™ API.

Before you begin

To send options from the IBM Storage Protect™ to the IBM Storage Protect™ API, you must specify the **send** command in an RMAN script.

About this task

Use the **send** command to set IBM Storage Protect™ options such as `TCPServeraddress` and `TCPport` to the IBM Storage Protect™ API. You can customize the actions that the script takes without updating the existing Data Protection for Oracle or IBM Storage Protect™ 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 IBM Storage Protect™ API options files.

- You can specify multiple IBM Storage Protect™ API options in the same **send** command.
- The `ENABLELANFREE` and `DEDUPPLICATION` options are mutually exclusive. If both options are defined, client-side data deduplication does not occur.
- The `ENABLECLIENTENCRYPTKEY` and `DEDUPPLICATION` options are also mutually exclusive. If both options are defined, client-side data deduplication does not occur.
- You can specify any IBM Storage Protect™ API option with the **send** command.
- Specify the **send** command in an RMAN script. You can specify one or more IBM Storage Protect™ options in a **send** command string. The **send** command string can contain up to 512 bytes.
To back up an Oracle database to the IBM® Storage Protect 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' '-TCPSEVER=halley -TCPPOINT=1601 -ENABLEDEDUPCACHE=YES';

```

Result

Data Protection for Oracle passes the command string to the IBM Storage Protect™ API. The IBM Storage Protect™ 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 IBM Storage Protect™ 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 information

[RMAN script examples](#)

RMAN script examples

Sample RMAN scripts illustrate how to create parallel backup streams to IBM® Storage Protect server storage.

Example

In these examples, to back up to IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect servers because it cannot be restored.

You can maintain one Data Protection for Oracle options file and change the IBM Storage Protect™ 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 IBM® Storage Protect server. The IBM® Storage Protect 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 IBM® Storage Protect 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.

Result

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 IBM® Storage Protect server. Likewise, if you specify **set duplex =4** and allocate two channels in the RMAN backup script, RMAN will start eight sessions to the IBM® Storage Protect 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 IBM® Storage Protect server. The node definition option on the IBM® Storage Protect server **maxnummp** determines the maximum number of mount points a client node can use on the IBM® Storage Protect server during a backup operation. View the maximum mount points that are allowed by the IBM® Storage Protect server for a particular node by entering the **query node** command from an IBM® Storage Protect Administrative Client prompt:

```
q node f=d
```

See the appropriate *IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect server with RMAN.

Before you begin

Ensure that **backdelete=yes** is specified by the IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect server

Define a schedule on the IBM® Storage Protect server to automatically run online backups of Oracle server databases.

Before you begin

Ensure that your system meets the minimum hardware, software, and operating system requirements. For more information, see [“Data Protection for Oracle installation” on page 10](#)

On a Solaris SPARC operating system or on a 64-bit version of HP-UX Itanium operating system, use the latest compatible version of the IBM® Storage Protect BA client along with the latest versions of Data Protection for Oracle and IBM® Storage Protect API.

Procedure

To set up a schedule on the IBM® Storage Protect server:

1. Define the following schedule on the IBM® Storage Protect server. You can enter the command on the IBM® Storage Protect server console or on an administrative client. The administrative client does not have to be running on the same system as the IBM® Storage Protect 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](#)” on page 37:

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

Result

- A backup schedule is now defined on the IBM® Storage Protect 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 IBM® Storage Protect **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 IBM® Storage Protect backup-archive client is installed on `NodeA1` in the `/usr/tivoli/tsm/client/ba/bin64` directory.
- Data Protection for Oracle is installed on `NodeA1` in the `/usr/tivoli/tsm/client/oracle/bin64` directory.
- An AIX® operating system is used.

Scheduling Data Protection for Oracle backups with the IBM® Storage Protect scheduler requires special configuration issues to be addressed. This procedure addresses this issue by creating `dsm.sys` files from which to associate stanzas for your client, Data Protection for Oracle, and scheduled backups.

The `passwordaccess generate` option is more secure and convenient for every-day use than the `passwordaccess prompt` option. The `passwordaccess generate` option is the recommended setting for Data Protection for Oracle.

In a default installation, the IBM® Storage Protect 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 not a default installation, see the *Enable non-administrators to manage their own data* chapter in the IBM® Storage Protect client manual.

Procedure

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

1. Create `dsm.sys` files in both the `/usr/tivoli/tsm/client/ba/bin64` and the `/usr/tivoli/tsm/client/api/bin64` directories, if these files do not exist.
2. 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's `dsm.sys` file `/usr/tivoli/tsm/client/api/bin64/dsm.sys` because for some options, identical values in both files can lead to malfunction.
 - a. Add a **servername** stanza to `/usr/tivoli/tsm/client/ba/bin64/dsm.sys` for the file system backups that are associated with your IBM® Storage Protect backup archive client.
For example:

```
servername    TSMbackup
commethod     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 IBM® Storage Protect backup archive client. The default directory location is `/usr/tivoli/tsm/client/ba/bin64`.

- b. Create **servername** stanzas in both `dsm.sys` files using 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 file `/usr/tivoli/tsm/client/api/bin64/dsm.sys`.

For the scheduler associated with Data Protection for Oracle, a stanza from the same **servername** parameter must be in the file `/usr/tivoli/tsm/client/ba/bin64/dsm.sys`. When the password expires, and the new node credentials are stored to TSM.PWD, `passwordaccess generate` couples the password with the **servername** from the `dsm.sys` file.

Ensure that the following six options are identical in both files.

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

Most of the other options will be different in each file. Some specific options cannot be the same in each file.

- c. 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`. These different values prevent concurrent write access to the same file by Data Protection for Oracle, which is running as `oracle` user and the scheduler, which is running as `root`.

- d. To the stanza `servername TSMOracle` in `/usr/tivoli/tsm/client/ba/bin64/dsm.sys`, you can add options specific to the scheduler.
For example:

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

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

3. The temporary switching from `passwordaccess generate` to `passwordaccess prompt` can become necessary when your existing Oracle backups in IBM® Storage Protect storage, with a certain owner, need to be accessed by a user with a different user name. For example, when you restore 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.

Examples:

Specify `TDPO_OWNER` as `oraxyz` in order to access files in IBM® Storage Protect storage, whose OWNER is `oraxyz`.

Specify `TDPO_OWNER` in order to access files in IBM® Storage Protect storage, whose OWNER is empty.

For this scenario, you must also set `TDPO_NODE` and `TDPO_PSWDPATH` in your `TDPO_OPTFILE` and rerun `tdpoconf password`.

The `servername TSMOracle` setting must be specified in the `dsm.opt` file that is 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`, associated with Data Protection for Oracle. For example:

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

4. 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 IBM Storage Protect server” on page 36](#). 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
```

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

```
#!/bin/ksh
export ORACLE_HOME=/orc11g/app/oracle/product/11.2.0
export PATH=$ORACLE_HOME/bin:$PATH
rman target agnttest/agtnttest@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/agtnttest@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.

6. 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); }
```

7. Log in as the root user to the system where Data Protection for Oracle is installed as node name NodeA1.
8. 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=TSMOracle
```

Data Protection for Oracle is now enabled for scheduled backups.

Querying backup objects

Use the **tdposync query** command to query the IBM® Storage Protect 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 IBM® Storage Protect during the backup operation.

Related information

[Query command](#)

[Data deduplication with Data Protection for Oracle](#)

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 IBM® Storage Protect 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 IBM Storage Protect™: client-side data deduplication and server side data deduplication.

Client-side data deduplication is a data deduplication technique that is used on the IBM Storage Protect™ API to remove redundant data during backup processing before the data is transferred to the IBM® Storage Protect 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 IBM® Storage Protect 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 IBM Storage Protect™ 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 IBM® Storage Protect 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 IBM® Storage Protect 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
```

Result

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 IBM Storage Protect™ server activity log for the total data reduction.

You can also use the performance monitor feature in the IBM Storage Protect™ server to verify the percentage of data that has been deduplicated. The performance monitor feature is part of the IBM Storage Protect™ 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
tcp 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 IBM® Storage Protect 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 IBM Storage Protect™ 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 IBM® Storage Protect server deduplicated pool, the cache is reset and the backup operations fails. The IBM Storage Protect™ API does not attempt the backup again.

- When IBM® Storage Protect 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 information

[Query command](#)

[Determining total data reduction](#)

Determining total data reduction

You can determine the percentage of total data reduction by querying the IBM Storage Protect™ 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:

$$\text{Deduplication reduction} = (1 - 2272805 / 9961472) = 0.7718$$

- 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,

$$\text{Compressed by} = (1 - 52253 / 2272805) = 0.9770$$

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

$$\begin{aligned} \text{Total data reduction} &= (1 - \text{bytes after compression} / \text{bytes processed}) \\ &= (1 - 52253 / 9961472) = 0.9948 \end{aligned}$$

Result

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 IBM Storage Protect™ server to verify the percentage of data that has been deduplicated. The performance monitor feature is part of the IBM Storage Protect™ 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
```

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 IBM® Storage Protect.
- Query objects that are backed up on the IBM® Storage Protect 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 IBM® Storage Protect server.

You are prompted to enter both the old and new passwords, if you do not provide them, 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:

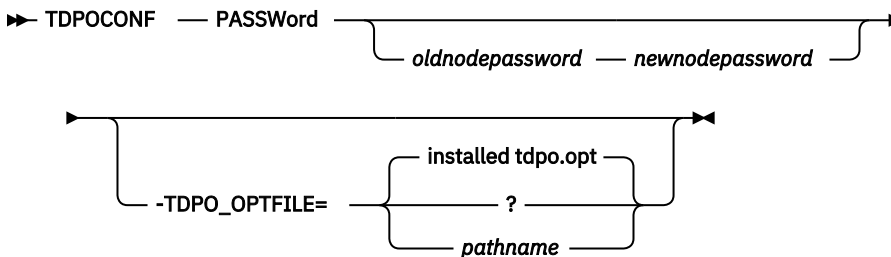
passwordaccess prompt

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_nodeoption` 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_pswdpathoption`. If the `tdpo_pswdpathoption` 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_nodeoption` in the `tdpo.opt` file. Data Protection for Oracle uses the value of the `nodenameoption` that is specified in the `dsm.sys` file. If the `tdpo_pswdpathoption` is specified in the `tdpo.opt` file, it is ignored. For more information, see the description of the `tdpo_pswdpathoption` in [“Available Data Protection for Oracle options” on page 21](#).

Syntax



Optional parameters

oldnodepassword

Specifies the current (old) password you want to change.

newnodepassword

Specifies the new password.

The password is not case-sensitive and can be composed of 1 to 63 of the following characters:

```

a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
~ ! @ # $ % ^ & * _ - + = ' | ( ) { } [ ] : ; < > , . ? /
  
```

Enclose all parameters that contain one or more special characters in quotation marks. Without quotation marks, the special characters can be interpreted as shell escape characters, file redirection characters, or other characters that have significance to the operating system.

-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

Example

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

```

*****
* IBM Protect for Databases Utility          *
* Password file initialization/update program *
*                                           *
*****
ANU0260I Password successfully changed.

```

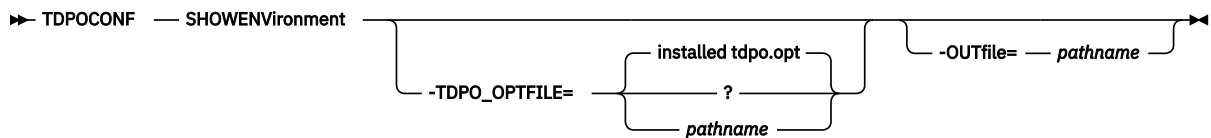
showenvironment command

Use the **showenvironment** command to query the IBM® Storage Protect 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 IBM® Storage Protect API and IBM® Storage Protect 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

Example

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

```

Data Protection for Oracle Information
Version:          8
Release:          1
Level:            0
Sublevel:         0
Platform:         64bit TDPO Linux86-64
IBM Protect Server Information
Server Name:      TMSERVER_ORC
Server Address:   TMSERVER
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 IBM® Storage Protect server stanza in the `dsm.sys` file, not the name of the IBM® Storage Protect server.

tdposync utility

The **tdposync** utility checks for items on the IBM® Storage Protect 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 IBM® Storage Protect, 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 49](#) and [“PICK window” on page 51](#) 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 IBM® Storage Protect server. In cases where objects are not found on the IBM® Storage Protect server, RMAN tries to delete backup sets from the IBM® Storage Protect 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 IBM® Storage Protect server. Therefore, this utility 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 IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect server.
4. Displays a list of files that exist on the IBM® Storage Protect 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 IBM® Storage Protect server.

You can automate the maintenance of IBM® Storage Protect Data Protection for Oracle without the need for user interaction. You can use an input file to allow the **tdposync** utility to receive input from a script or batch file.

Example

For example, `tdposync syncdb < input.txt`

The `input.txt` file contains the required responses to the prompts for information as in the following example:

```

06/01/2016
06/07/2016
rman
rman
orcl
+
o
y

```

The description of each line of the `input.txt` file is listed in the following table:

06/01/2016	# from date
06/07/2016	# to date
rman	# RMAN user
rman	# RMAN password
orcl	# Oracle connection string
+	# pick windows selection, + selects all objects
o	# proceed with the operation
y	# confirm

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 IBM® Storage Protect 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 IBM® Storage Protect server, you must use **-numcatalogs=number**. This action is necessary so that **tdposync** has all the information to correctly query both Oracle and the IBM Storage Protect™. 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 **-numinstances=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 IBM® Storage Protect server. To back up each Oracle target database to its own file space, use the `tdpo_fsoption` 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 IBM® Storage Protect. 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:

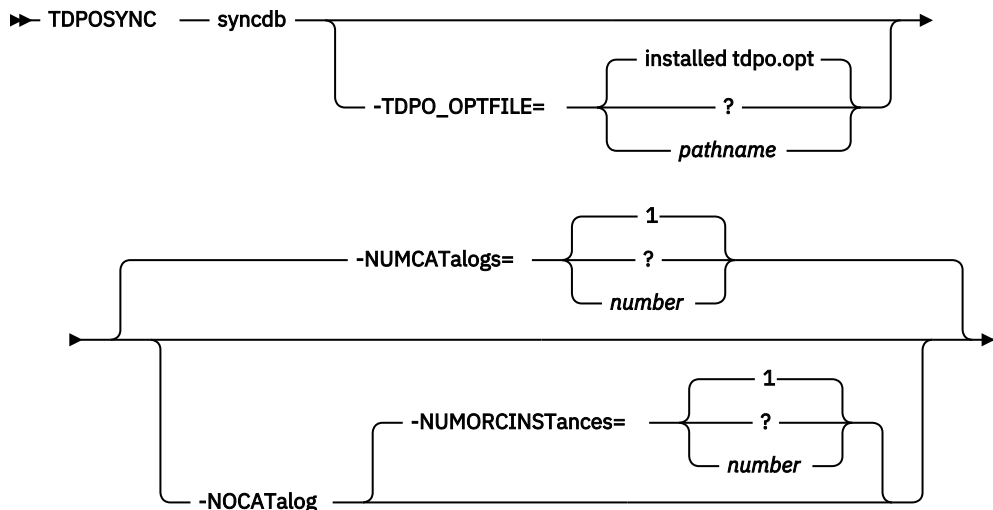
```
login/password@connectstring
```

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 IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect 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 IBM Storage Protect™ 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 IBM® Storage Protect 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

Example

Synchronize the IBM Storage Protect™ 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 Protect for Databases:
Data Protection for Oracle
Version 8, Release 1, Level 0.0
(C) Copyright IBM Corporation 1997, 2016. All rights reserved.

From Date (01/01/1990): 10/20/2016
To Date (10/28/2016): 10/28/2016

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

Synchronize the IBM Storage Protect™ 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 Protect for Databases:
Data Protection for Oracle
Version 8, Release 1, Level 0.0
(C) Copyright IBM Corporation 1997, 2016. All rights reserved.
From Date (01/01/1990): 10/20/2016
To Date (10/28/2016): 10/28/2016

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 IBM® Storage Protect 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

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  <D>=Down  <T>=Top  <B>=Bottom  <R>=Right  <L#>=Left
<G#>=Goto Line #  <#>=Toggle Entry  <+>=Select All  <->=Deselect All
<#:#+>=Select A Range  <#:#->=Deselect A Range  <0>=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 IBM® Storage Protect server.

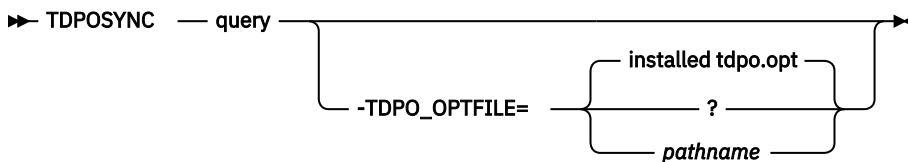
Query command

Use this command to query the IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect 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 IBM® Storage Protect 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/Agent0BA64/tdpo.opt`) is used.

Description of the output fields

Name

Object name on the IBM® Storage Protect server; for instance, `/fs/h1/l1`.

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 IBM® Storage Protect 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.

AES-256

The object was encrypted by using AES-256 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 IBM® Storage Protect server for information about objects that are backed up

The command to be run is `tdposync query`.
The following output is displayed:

```
IBM Protect for Databases:
Data Protection for Oracle
Version 8, Release 1, Level 0
(C) Copyright IBM Corporation 1997, 2014. All rights reserved.

From Date (01/01/2016):

To Date (07/02/2016):

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 IBM Storage Protect™ server activity log for the ANU2526I message.

Accessibility features for the IBM® Storage Protect product family

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

Overview

The IBM® Storage Protect family of products includes the following major accessibility features:

- Keyboard-only operation
- Operations that use a screen reader

The IBM® Storage Protect family of products uses the latest W3C Standard, [WAI-ARIA 1.0](#), to ensure compliance with US Section 508 and [Web Content Accessibility Guidelines \(WCAG\) 2.0](#). To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by the product.

The product documentation in IBM® Documentation is enabled for accessibility.

Keyboard navigation

This product uses standard navigation keys.

Interface information

User interfaces do not have content that flashes 2 - 55 times per second.

Web user interfaces rely on cascading style sheets to render content properly and to provide a usable experience. The application provides an equivalent way for low-vision users to use system display settings, including high-contrast mode. You can control font size by using the device or web browser settings.

Web user interfaces include WAI-ARIA navigational landmarks that you can use to quickly navigate to functional areas in the application.

Vendor software

The IBM® Storage Protect 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 accessibility information about its products.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service
800-IBM-3383 (800-426-3383)
(within North America)

For more information about the commitment that IBM has to accessibility, see [IBM Accessibility](#).

Notices

This information was developed for products and services offered in the US. This material might be available from IBM® in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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
US

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

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

IBM® Director of Licensing
IBM® Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
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.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

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

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

COPYRIGHT LICENSE:

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

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

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.

The registered trademark Linux® is used pursuant to a sublicense from the Linux® Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

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.

Red Hat®, OpenShift®, Ansible®, and Ceph® are trademarks or registered trademarks of Red Hat®, Inc. or its subsidiaries in the United States and other countries.

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

VMware, VMware vCenter Server™, and VMware vSphere™ are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

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

Index

48

- and Oracle databases 31
- configuring 24
- installing 10
- management class 28
- overview 7, 7
- policy requirements 28, 28
- Recovery Manager (RMAN) 7
- silent installation 12
- supported Oracle versions 7
- updates 6
- version migration 7

A

- About this publication 6
- accessibility features 54
- AIX 6.1
 - options 21
- AIX 64-bit
 - installation 11
- archive copy group 28
- automated 8

B

- backdelete**
 - and node 24
 - and policy 28
- backup copy group values 28
- backups**
 - removing 35
- bkdb.log 31
- bkdb.scr
 - and the scheduler 36, 37

C

- command line syntax**
 - characteristics 44
- commands**
 - query association 36
 - query node 34
 - query schedule 36
- Oracle**
 - change 36
- tdpoconf password 44
- tdpoconf showenvironment 46
- tdposync**
 - query 52
 - syncdb 49
- commmethod**
 - description 25
- compression 26
- configure**
 - Quick configuration 19

- with default settings 19
- configuring 20
- configuring**
 - Data Protection for Oracle 19
- control file 47, 49

D

- data deduplication**
 - overview 40
 - using 40
- data deduplication reduction**
 - determining 42
- Data Protection for Oracle**
 - configuring 19
 - installing 10
 - protecting data 31
 - reference 44
- deduplication**
 - using 40
- defining a schedule**
 - on the 36
 - on the client machine 37
- disability 54
- dsm.opt**
 - description 24
 - required options 25
- dsm.sys**
 - description 24
 - recommended options 26
 - required options 25
- dsmi_log 21
- dsmi_orc_config 21
- dsmi_orc_config**
 - and the scheduler 37
- duplex copy**
 - considerations 34
 - overview 34

E

- enablelanfree 26
- example**
 - tdposync query command 52
- examples**
 - duplex copy 34
 - include/exclude 28
 - invoking RMAN 31
 - removing backups 36
- RMAN script**
 - send command 33
- RMAN scripts 33
- scheduler 36
- tdpoconf password command 44
- tdpoconf showenvironment command 46
- tdposync syncdb command 49

- tdposync syncdb command
 - pick window [51](#)
- expiration of objects [28](#)

F

- failover
 - [8](#)
 - overview [8](#)

H

- hardware requirements
 - AIX environment [10](#)
- HP-UX Itanium 2 64-bit
 - options [21](#)
- HP-UX Itanium 64-bit
 - installation instructions [13](#)
- HP-UX PA-RISC 64-bit
 - options [21](#)

I

- IBM Knowledge Center [6](#)
- inclexcl
 - and policy [28](#)
- include
 - and policy [28](#)
 - and duplex copy [34](#)
 - description [26](#)
- installation
 - AIX 64-bit [11](#)
 - instructions
 - Linux on system z [15](#)
 - Linux x86_64 [14](#)
 - node name registration [24](#)
 - prerequisites [10](#)
- installing
 - AIX [12](#)
 - Data Protection for Oracle [10](#)
 - HP-UX Itanium 64-bit [13](#)
 - silently [12](#)

K

- keyboard [54](#)
- Knowledge Center [6](#)

L

- LAN-free data transfer
 - options [26](#)
- Linux environment
 - hardware requirements [10](#)
 - HP-UX
 - hardware requirements [10](#)
 - Solaris [10](#)
- Linux on POWER
 - options [21](#)
- Linux on System z 64-bit
 - installation instructions [15](#)
- Linux x86_64
 - installation instructions [14](#)

- options [21](#)
- Linux zSeries 64-bit
 - options [21](#)

M

- management class
 - for automatic expiration [28](#)
- maxnummp [34](#)
- migration considerations [7](#)
- Minimum software requirements [10](#)

N

- New in this version [6](#)
- nocatalog
 - and tdposync syncdb command [49](#)
- node name
 - registration [24](#)
- numcatalogs
 - and tdposync syncdb command [49](#)
- numorcintstances
 - and tdposync syncdb command [49](#)

O

- operating system requirements [10](#)
- options [21](#)
- Oracle RMAN send command
 - using [32](#)
- outfile
 - and tdpoconf showenvironment command [46](#)
- overview
 - [7](#)
 - data deduplication [40](#)

P

- passwordaccess [25](#)
- pick window [51](#)
- policy domain [28](#)
- prerequisites [10](#)
- protecting data
 - Data Protection for Oracle [31](#)
- publications [6](#)

Q

- querying backup objects [40](#)

R

- reference
 - Data Protection for Oracle [44](#)
- retonly
 - and policy [28](#)
- RMAN
 - description [7](#)
 - invoking [31](#)
 - scripts [32](#)
 - scripts
 - send command [32](#)

S

- `schedbkdb.scr` 37
- `scripts` 32
- send command**
 - in an RMAN script 32
 - sample script 33
 - using 32
- servername**
 - and `dsm.opt` 25
 - and `dsm.sys` 25
 - and the scheduler 37, 37
- `set duplex` 34
- Solaris SPARC 32-bit**
 - options 21
- Solaris SPARC 64-bit**
 - options 21
- Solaris x86 32-bit**
 - options 21
- Solaris x86_64**
 - options 21

T

- `tcpserveraddress` 25
- tdpo.opt**
 - and version migration 7
 - description 21
- `tdpo_date_fmt` 21
- `tdpo_enablescriptinput` 21
- `tdpo_fs` 21
- `tdpo_mgmt_class_2` 21
- `tdpo_mgmt_class_3` 21
- `tdpo_mgmt_class_4` 21
- `tdpo_node` 21
- `tdpo_num_fmt` 21
- TDPO_OPTFILE**
 - and `tdpoconf password` command 44
 - and `tdpoconf showenvironment` command 46
 - and `tdposync syncdb` command 49, 52
 - example 21
- `tdpo_owner` 21
- `tdpo_pswdpath` 21
- `tdpo_time_fmt` 21
- `tdpoconf` 44
- tdpoconf**
 - and password initialization 29
 - and `tdpo.opt` 21
 - description 44

- `password` command 44
- password command**
 - example 44
 - syntax diagram 44
 - TDPO_OPTFILE 44
- `showenvironment` command 46
- showenvironment command**
 - example 46
 - outfile 46
 - syntax diagram 46
 - TDPO_OPTFILE 46
- `tdpoconf` utility 44
- tdpoerror.log**
 - how to specify 21
- `tdposync` 44
- tdposync**
 - and `tdpo.opt` 21
 - considerations 48
 - description 47
 - query command 52
 - query command**
 - example 52
 - syntax diagram 52
 - TDPO_OPTFILE 52
 - `syncdb` command 49
 - syncdb command**
 - example 49
 - `nocatalog` 49
 - `numcatalogs` 49
 - `numorcintstances` 49
 - `pick` window 51
 - syntax diagram 49
 - TDPO_OPTFILE 49
- tdposync syncdb command**
 - `pick` window 51

U

- UNIX environment**
 - hardware requirements 10
- using data deduplication 40
- utilities**
 - using 44

V

- verdeleted**
 - and policy 28
- virtualization support 10

© Copyright International Business Machines Corporation 1998, 2025

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

