Tivoli® Storage Manager for Enterprise Resource Planning

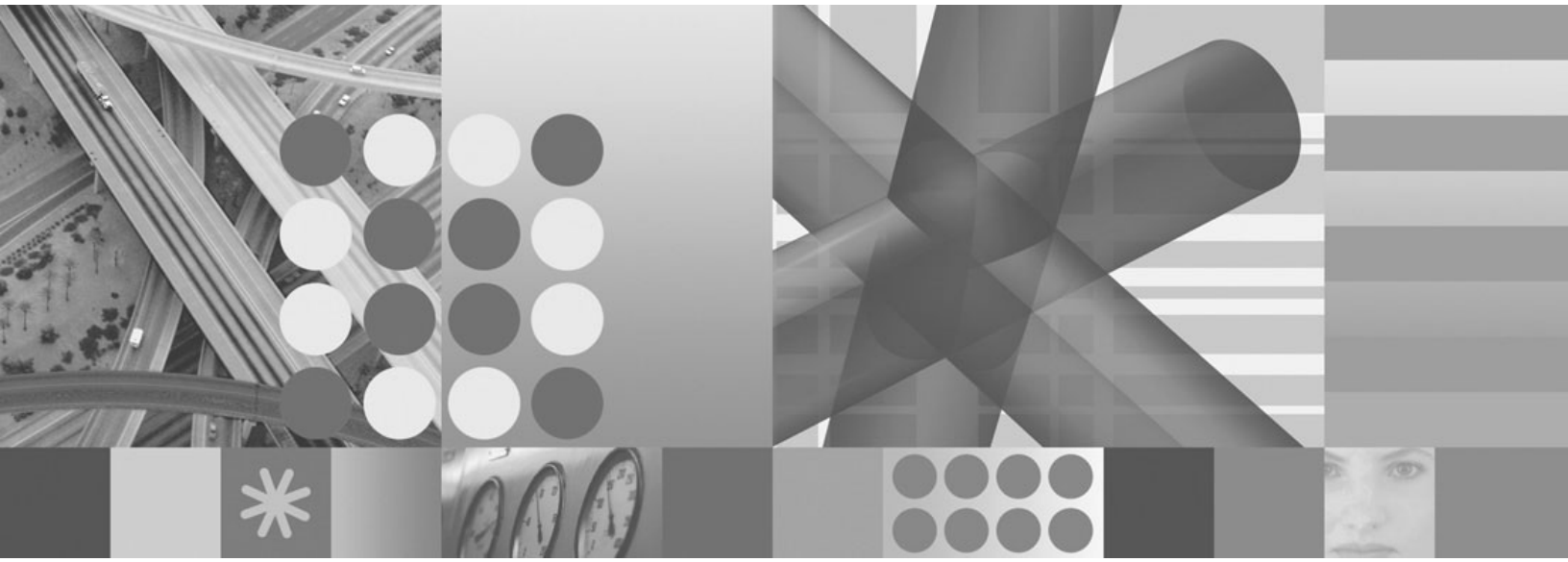
Version 6.1

Data Protection for SAP®
Installation and User's Guide for Oracle

SC33-6340-10

Tivoli® Storage Manager for Enterprise Resource Planning

Version 6.1



Data Protection for SAP®
Installation and User's Guide for Oracle

SC33-6340-10

Note
Before using this information and the product it supports, read the information in "Notices" on page 219.

Edition notice

This edition applies to Data Protection for *SAP*® Version 6 Release 1 Modification Level 0 (program number 5608-E05), available as a licensed program product, and to all subsequent releases and modifications until otherwise indicated in new editions.

Order publications through your IBM representative or the IBM branch office serving your area. Publications are not stocked at the addresses given below.

Address comments on this publication to:

IBM Deutschland Research and Development GmbH
Enterprise Solution Development
Dept. 3848
Schoenaicher Str. 220
71032 Boeblingen
Germany

FAX (Germany): 07031 16 3619
FAX (other countries): (+49) 7031 16 3619

Internet Web page: http://www.ibm.com/software/tivoli

Make sure to include the following in your comment or note:

- Title and order number of this publication
- Page number or topic related to your comment

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

Tables

Preface

This publication documents how to use IBM Tivoli Storage Manager for Enterprise Resource Planning Data Protection for *SAP*® Version 6.1 It describes the procedures needed to install and customize Data Protection for SAP which is the interface between SAP® and Tivoli Storage Manager.

Who Should Read This Publication

This publication (or topic collection) is intended for system programmers and administrators who are responsible for implementing a backup solution in an SAP environment using the Tivoli Storage Manager. It describes the procedures needed to install and customize Data Protection for SAP, the interface between SAP and the Tivoli Storage Manager. The reader should be familiar with the documentation for SAP, Tivoli Storage Manager, and Oracle.

This publication describes release V6.1, January 2009.

Publications

Tivoli® Storage Manager publications and other related publications are available online.

You can search all publications in the Tivoli Storage Manager Information Center: http://publib.boulder.ibm.com/infocenter/tsminfo/v6.

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

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

Tivoli Storage Manager publications

Publications are available for the server, storage agent, client, and Data Protection.

Table 1. Tivoli Storage Manager server publications

Publication title	Order number
IBM Tivoli Storage Manager Messages	GC23-9787
IBM Tivoli Storage Manager Performance Tuning Guide	GC23-9788
IBM Tivoli Storage Manager Problem Determination Guide	GC23-9789
IBM Tivoli Storage Manager for AIX Installation Guide	GC23-9781
IBM Tivoli Storage Manager for AIX Administrator's Guide	SC23-9769
IBM Tivoli Storage Manager for AIX Administrator's Reference	SC23-9775
IBM Tivoli Storage Manager for HP-UX Installation Guide	GC23-9782
IBM Tivoli Storage Manager for HP-UX Administrator's Guide	SC23-9770
IBM Tivoli Storage Manager for HP-UX Administrator's Reference	SC23-9776

Table 1. Tivoli Storage Manager server publications (continued)

Publication title	Order number
IBM Tivoli Storage Manager for Linux Installation Guide	GC23-9783
IBM Tivoli Storage Manager for Linux Administrator's Guide	SC23-9771
IBM Tivoli Storage Manager for Linux Administrator's Reference	SC23-9777
IBM Tivoli Storage Manager for Sun Solaris Installation Guide	GC23-9784
IBM Tivoli Storage Manager for Sun Solaris Administrator's Guide	SC23-9772
IBM Tivoli Storage Manager for Sun Solaris Administrator's Reference	SC23-9778
IBM Tivoli Storage Manager for Windows Installation Guide	GC23-9785
IBM Tivoli Storage Manager for Windows Administrator's Guide	SC23-9773
IBM Tivoli Storage Manager for Windows Administrator's Reference	SC23-9779
IBM Tivoli Storage Manager Server Upgrade Guide	SC23-9554
IBM Tivoli Storage Manager for System Backup and Recovery Installation and User's Guide	SC32-6543

Table 2. Tivoli Storage Manager storage agent publications

Publication title	Order number
IBM Tivoli Storage Manager for SAN for AIX Storage Agent User's Guide	SC23-9797
IBM Tivoli Storage Manager for SAN for HP-UX Storage Agent User's Guide	SC23-9798
IBM Tivoli Storage Manager for SAN for Linux Storage Agent User's Guide	SC23-9799
IBM Tivoli Storage Manager for SAN for Sun Solaris Storage Agent User's Guide	SC23-9800
IBM Tivoli Storage Manager for SAN for Windows Storage Agent User's Guide	SC23-9553

Table 3. Tivoli Storage Manager client publications

Publication title	Order number
IBM Tivoli Storage Manager for UNIX and Linux: Backup-Archive Clients Installation and User's Guide	SC23-9791
IBM Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and User's Guide	SC23-9792
IBM Tivoli Storage Manager for Space Management for UNIX and Linux: User's Guide	SC23-9794
IBM Tivoli Storage Manager for HSM for Windows Administration Guide	SC23-9795
IBM Tivoli Storage Manager Using the Application Program Interface	SC23-9793
Program Directory for IBM Tivoli Storage Manager z/OS Edition Backup-Archive Client	GI11-8912
Program Directory for IBM Tivoli Storage Manager z/OS Edition Application Program Interface	GI11-8911

Table 4. Tivoli Storage Manager Data Protection publications

Publication title	Order number
IBM Tivoli Storage Manager for Advanced Copy Services: Data Protection for Snapshot Devices Installation and User's Guide	SC33-8331
IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Installation and User's Guide	SC32-9059
IBM Tivoli Storage Manager for Databases: Data Protection for Oracle for UNIX and Linux Installation and User's Guide	SC32-9064
IBM Tivoli Storage Manager for Databases: Data Protection for Oracle for Windows Installation and User's Guide	SC32-9065
IBM Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP Installation and User's Guide for DB2	SC33-6341
IBM Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP Installation and User's Guide for Oracle	SC33-6340
IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino® for UNIX, Linux, and OS/400® Installation and User's Guide	SC32-9056
IBM Tivoli Storage Manager for Mail: Data Protection for Lotus Domino for Windows Installation and User's Guide	SC32-9057
IBM Tivoli Storage Manager for Mail: Data Protection for Microsoft Exchange Server Installation and User's Guide	SC23-9796
Program Directory for IBM Tivoli Storage Manager for Mail (Data Protection for Lotus Domino)	GI11-8909

Support information

You can find support information for IBM products from a variety of sources.

Getting technical training

Information about Tivoli technical training courses is available online.

Go to http://www.ibm.com/software/tivoli/education/.

Searching knowledge bases

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

You can begin with the Tivoli Storage Manager Information Center at http://publib.boulder.ibm.com/infocenter/tsminfo/v6. From this Web site, you can search all Tivoli Storage Manager publications.

Searching the Internet

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

To search multiple Internet resources, go to the support Web site for Tivoli Storage Manager at http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliStorageManager.html. From there, you can search a variety of resources including:

- IBM technotes
- IBM downloads

- IBM Redbooks®

If you still cannot find the solution to the problem, you can search forums and newsgroups on the Internet for the latest information that might help you resolve your problem. To share your experiences and learn from others in the user community, go to the Tivoli Storage Manager wiki at http://www.ibm.com/developerworks/wikis/display/tivolistoragemanager/Home.

Using IBM Support Assistant

At no additional cost, you can install on any workstation the IBM Support Assistant, a stand-alone application. You can then enhance the application by installing product-specific plug-in modules for the IBM products that you use.

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

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

For more information, see the IBM Support Assistant Web site at http://www.ibm.com/software/support/isa/.

Finding product fixes

A product fix to resolve your problem might be available from the IBM Software Support Web site.

You can determine what fixes are available by checking the Web site:

1. Go to the IBM Software Support Web site at http://www.ibm.com/software/tivoli/products/storage-mgr/product-links.html.
2. Click the **Support Pages** link for your Tivoli Storage Manager product.
3. Click **Download**, and then click **Fixes by version**.

Getting e-mail notification of product fixes

You can get notifications about fixes and other news about IBM products.

To receive weekly e-mail notifications about fixes and other news about IBM products, follow these steps:

1. From the support page for any IBM product, click **My support** in the upper-right corner of the page.
2. If you have already registered, skip to the next step. If you have not registered, click **Register** in the upper-right corner of the support page to establish your user ID and password.
3. Sign in to **My support**.
4. On the My support page, click **Edit profiles** in the left navigation pane, and scroll to **Select Mail Preferences**. Select a product family and check the appropriate boxes for the type of information you want.
5. Click **Submit**.
6. For e-mail notification for other products, repeat steps 4 and 5.

Contacting IBM Software Support

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

Before you contact IBM Software Support, follow these steps:

1. Set up a software maintenance contract.
2. Determine the business impact of your problem.
3. Describe your problem and gather background information.

Then see "Submit the problem to IBM Software Support" on page xvi for information on contacting IBM Software Support.

Setting up a software maintenance contract

Set up a software maintenance contract. The type of contract that you need depends on the type of product you have.

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as IBM DB2® and IBM WebSphere® products that run on Microsoft® Windows® or UNIX® operating systems), enroll in IBM Passport Advantage® in one of the following ways:
  - **Online:** Go to the Passport Advantage Web page at http://www.ibm.com/software/lotus/passportadvantage/, click **How to enroll**, and follow the instructions.
  - **By Phone:** For the phone number to call in your country, go to the IBM Software Support Handbook Web page at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html and click **Contacts**.
- For server software products, you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for server software products, go to the IBM Technical support advantage Web page at http://www.ibm.com/servers/.

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. For a list of telephone numbers of people who provide support for your location, go to the Software Support Handbook page at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html.

Determine the business impact

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

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

Describe the problem and gather background information

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

To save time, know the answers to these questions:

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

Submit the problem to IBM Software Support

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

Online

Go to the IBM Software Support Web site at http://www.ibm.com/software/support/probsub.html. Enter your information into the appropriate problem submission tool.

By phone

For the phone number to call in your country, go to the contacts page of the IBM Software Support Handbook at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html.

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. If a workaround is possible, IBM Software Support provides one for you to implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the Tivoli Storage Manager product support Web site at http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliStorageManager.html, so that users who experience the same problem can benefit from the same resolutions.

New for Data Protection for *SAP®* Version 6.1

The following new functionality has been added to Version 6.1 of Data Protection for *SAP®* for Oracle:

- Executable files on Windows platforms (except Java applets) now bear a digital signature.
- Install Anywhere has replaced Install Shield as the installation vehicle.
- As of version 7.1, the SAP BR*Tools components have a facility for invoking snapshot (in SAP® terminology, *volume*) backups and restores. Such requests received by TSM for ERP are redirected to the Tivoli Storage Manager for Advanced Copy Services (TSM for ACS) product (if it is installed). To facilitate the interaction of TSM for ACS with TSM for ERP when the user wants to perform a TSM backup of the snapshots produced, certain parameters have been added to the TSM for ERP profile for use by TSM for ACS. For more information, refer to the TSM for ACS documentation.
- AIX 6.1 is now supported.

Other changes include:

- Support for 32–bit platforms has been discontinued.

Chapter 1. Protection for SAP® database servers

Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for *SAP*® for Oracle protects SAP® system data and integrates with the database-specific utilities of IBM DB2, Oracle, and SAP BR* Tools, which are a set of database administration functions incorporated into SAP for Oracle databases. Data Protection for SAP improve the availability of SAP database servers and reduces administration workload with automated data protection features designed specifically for SAP environments.

Data Protection for SAP provides these features and functions.

Data Protection for *SAP*® for Oracle overview

Data Protection for *SAP*® for Oracle architecture and product features are discussed.

Data Protection for SAP and Tivoli Storage Manager provide a reliable, high performance, and production-oriented solution that enables back up and restore of Oracle-based SAP® systems. It is integrated with SAP backup and recovery utilities BRBACKUP, BRARCHIVE, BRRESTORE, and BRRECOVER, and applies SAP backup and recovery procedures. Data Protection for SAP is optimized for SAP databases and therefore provides efficient management of large data volumes.

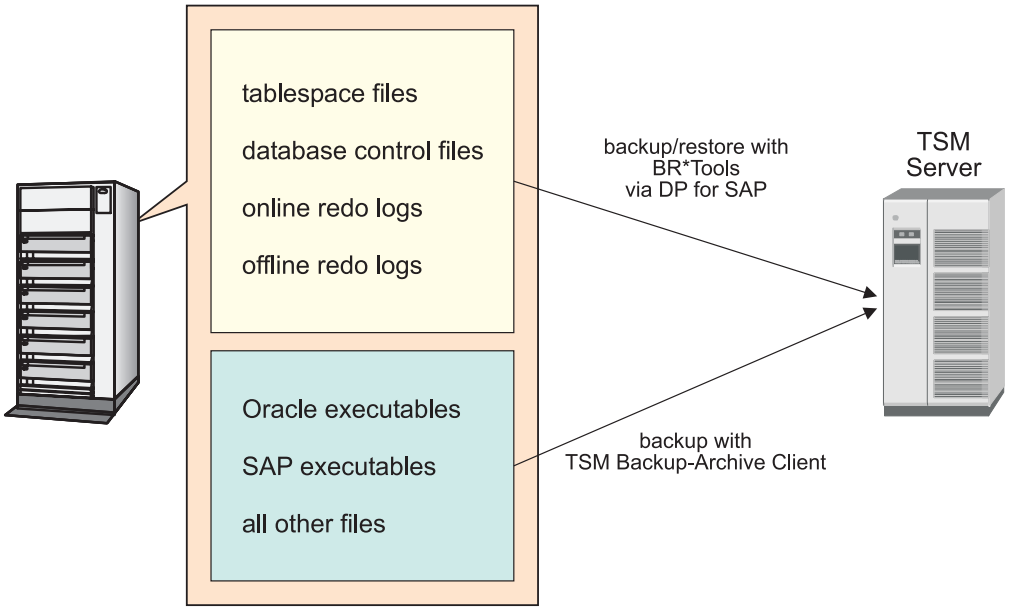


Figure 1. Scope of Data Protection for SAP for Oracle

As demonstrated in this graphic, SAP backup and recovery utilities center on database objects where more than 90% of the data resides on an SAP database server. As a result, Data Protection for SAP backs up and restores data files, control files, and online or offline redo logs.

Other files (such as SAP and Oracle executable files) can be backed up using the IBM Tivoli Storage Manager Backup-Archive Client. This is important for disaster

recovery purposes as all SAP and Oracle executable files must be available before using Data Protection for SAP and the BR*Tools. to restore and recover the database.

Data Protection for *SAP®* integration with SAP®

Data Protection for *SAP®* operates as an transparent link between Oracle and BR*Tools and Tivoli Storage Manager.

Data Protection for SAP provides two adapters:

backint
This executable file is called directly by SAP and is used to perform full database backups (online and offline) and back ups of control and redo log files.

orasbt.dll
This shared media management library is dynamically linked by Oracle RMAN. When a backup is performed using this shared library, SAP communicates through Oracle RMAN instead of Data Protection for SAP. Incremental backups are also available when using RMAN with this shared library.

Both adapters share the `init<SID>.utl` profile file. This file contains information that describes how to perform backups and restores and can be customized for the Data Protection for SAP environment. Both adapters also communicate with the Tivoli Storage Manager server through an API that is shared with other IBM Data Protection products. These adapters require that the Data Protection for SAP ProLE background process is running.

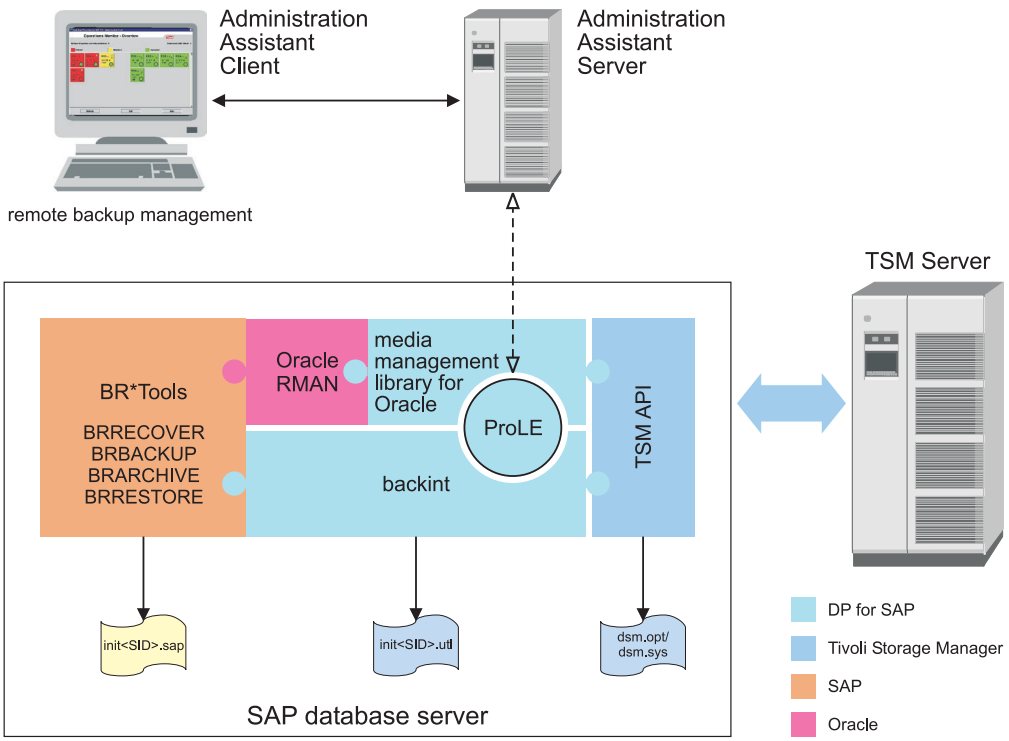


Figure 2. Integration of Data Protection for SAP with SAP

Data Protection for SAP also provides the Administration Assistant which is used to increase administrator productivity. The Administration Assistant can control multiple instances of Data Protection for SAP, communicates with Data Protection for SAP through TCP/IP, and typically resides on a different server. It is used to configure a Data Protection for SAP instance, monitor data transfer performance, backup status of the SAP system, and Tivoli Storage Manager server activity related to SAP. In addition, the Administration Assistant can remotely monitor and administer all Data Protection for SAP instances through an applet running on a Web browser. Information regarding how to use the Administration Assistant to register an SAP instance during installation or at a later time is available in "Specifying a new Administration Assistant function for Data Protection for *SAP*®" on page 75.

BACKINT interface

Data Protection for *SAP*® for Oracle provides the BACKINT interface to perform full online and offline backups of Oracle databases, control files, and redo log files. The BACKINT interface communicates directly with SAP®.Figure 3 shows the interaction between BR*Tools, Data Protection for SAP, and the BACKINT interface when performing a backup or restore.

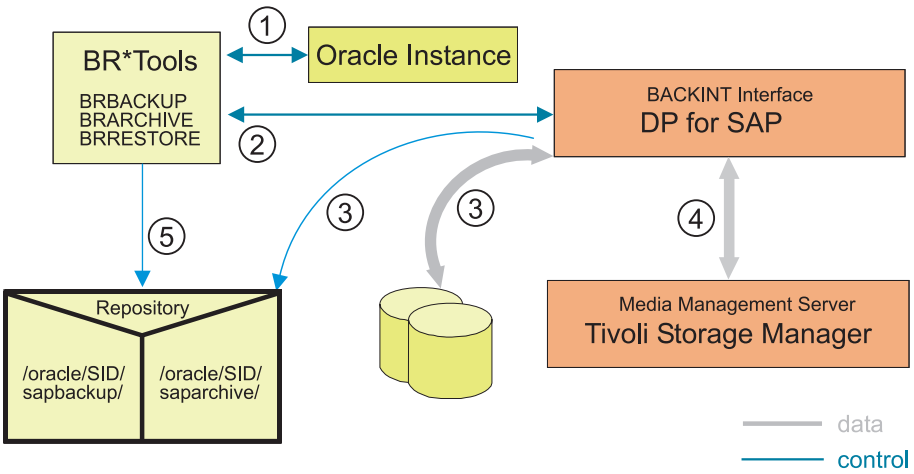


*Figure 3. Data Protection for SAP with BR*Tools using the BACKINT Interface*

The BR*Tools record the status of the Oracle data file backups and logfile backups by using tables contained within the Oracle database and system data. This information enables SAP to automatically restore the correct data files and their specific database transaction log files (redo log files), if necessary. The data files reside in the Oracle database (Oracle Instance). Data Protection for SAP runs as a separate process, independently from the database. It receives the data through the BACKINT interface and saves the data to the Tivoli Storage Manager server.

A backup operation proceeds in the following order (see circled numbers):

1. The BR*Tools utility BRBACKUP informs Oracle which data is to be backed up. It then places the database in the proper 'online or offline backup state.
2. BRBACKUP calls Data Protection for SAP through the BACKINT interface with a list of all files to be backed up.
3. Data Protection for SAP reads all requested files from the database and reports back to BRBACKUP. BRBACKUP adds these files to the repository that contains all processed backups.

4. BACKINT saves the data to the Tivoli Storage Manager server.
5. The BR*Tools update the file repository with status information about the files.

Oracle Backup/Restore and Data Protection for *SAP®*

The SAP® database administration provides four tools (referred to as the BR*Tools) for Oracle databases:

- BRBACKUP: Provides online or offline partial or full backups of tablespaces.
- BRARCHIVE: Provides back ups of archived redo log files.
- BRRESTORE: Provides system-guided restore of Oracle backups.
- BRRECOVER: Provides recover capabilities.

These SAP database administration tools offer all the functions necessary to administer a database. Oracle also provides a Recovery MANager administration utility (referred to as RMAN) which is required to perform an incremental backup. Data Protection for SAP integrates with SAP BR*Tools and Oracle RMAN to provide unattended, 24-hour, 7-days-per-week production backup and restore tasks.

Oracle Recovery Manager (RMAN)

Oracle RMAN is used to perform a backup, restore and recover operation of an Oracle database. RMAN is also required when performing an incremental backup.

Make sure to review SAP® support information regarding how to configure SAP on your operating system to perform a backup using RMAN with your database version. SAP information is available at SAP Service Marketplace (*http://service.sap.com/*).

When operating RMAN, Data Protection for *SAP®* is loaded by one (or more) Oracle processes as a shared library. These Oracle processes decide on how many parallel sessions are opened, when a session is opened and closed, and which data object (table space) is included in the session. Some of the above mentioned parameters must be configured for RMAN. Depending on how RMAN is used, these parameters can be configured either within the RMAN script or within the BR*Tools configuration file (init<SID>.sap).

If you want to use parallel sessions with RMAN, make sure you configure at least the same number of sessions within the Data Protection for SAP configuration file as you configure for RMAN (see also “Multiple Sessions” on page 103 and “Multiple Servers” on page 102).

Figure 4 on page 5 shows the interaction between BR*Tools, Data Protection for SAP, Oracle RMAN, and Data Protection for SAP when performing a backup or restore.

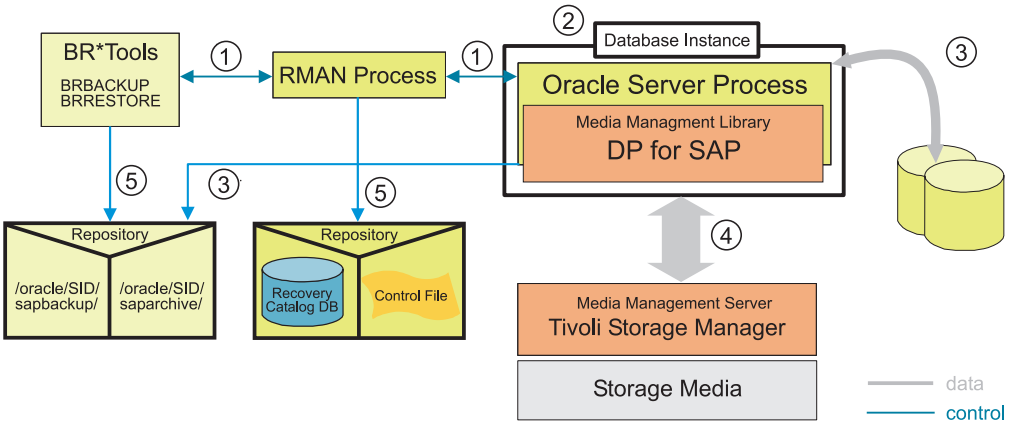


*Figure 4. Data Protection for SAP with BR*Tools using the RMAN Interface*

The BR*Tools use tables contained within the Oracle database and system data to record status information for the database and redo log backups.This information allows SAP to restore the correct data and their corresponding redo logs. The data files reside in the Oracle Instance of the Oracle database.

Data Protection for SAP runs as a linked library controlled by the Oracle Server Process.

A backup operation proceeds in the following order (see circled numbers):

1. The BR*Tools utility BRBACKUP informs Oracle RMAN which data is to be backed up. It then places the database in the proper online or offline backup state.
2. The Oracle server process loads Data Protection for SAP and communicates with it through the Oracle Media Management API.
3. Data Protection for SAP reads the requested data from the database and reports back to BRBACKUP. BRBACKUP adds this data to the repository that contains all processed backups.
4. Data Protection for SAP saves the data to the Tivoli Storage Manager server.
5. The BR*Tools update the file repository with status information about the data. RMAN uses a control file to maintain its own repository for a separate recovery catalog database.

Administration Assistant function for Data Protection for *SAP®*

The Administration Assistant comprises the client component and three server-level components (Server, Database Agent, and Database). Operations data is maintained in an internal database which helps prevent an insufficient memory problem in SAP® environments where a large number of Data Protection for *SAP®* for Oracle instances are active. The internal database used by the Administration Assistant is managed by either the open-source database product Apache Derby or IBM DB2 data server. The use of DB2 is in no way dependent on use of the DB2 version of Data Protection for SAP. A DB2 Administration Assistant database can also be used in an Oracle environment. Apache Derby is bundled with, and installed by, the Administration Assistant. For more information on Apache Derby, see

`http://db.apache.org/derby/`

If you prefer using the IBM DB2 data server, an existing DB2 installation must be present. It will be configured by the Administration Assistant. For more information on DB2, see

`http://www.ibm.com/software/data/db2/`

The server-level components are installed together on one system (standard installation) or distributed across multiple systems (distributed installation). An example of a multiple system installation could be when the Server component resides on one system and the database components reside on a second system; or, each component is installed on a separate system. This type of distributed installation helps alleviate CPU loads on a single-system configuration (in large-scale environments) by distributing this load over two or three separate systems. If CPU load is not an issue, the single-system installation is typically used. The distributed installation requires that all connecting Data Protection for SAP instances be version 5.4 or higher. If a single-system installation is selected, earlier Data Protection for SAP versions can also connect to the Administration Assistant.

Each system hosting an Administration Assistant component can be running UNIX, Linux, or Windows. Separate configuration files are maintained by the Server (assist.cfg) and Database Agent (dbagent.cfg) component. User profiles ensure that a client user can access the data of only those SAP database servers for which permission has been granted.

This figure shows the communication relationships of the Administration Assistant components (port numbers shown are defaults).

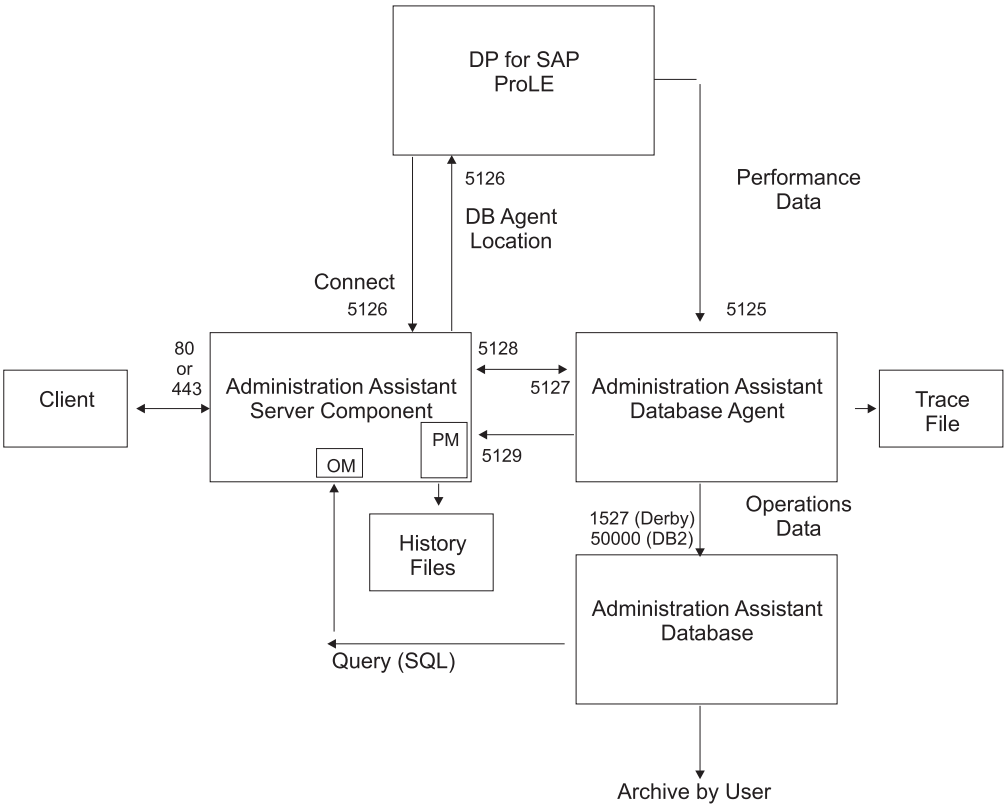


Figure 5. Administration Assistant function for Data Protection for SAP® Components (with Default Port Numbers)

The Server component waits for the client requests for connections using either the HTTP or HTTPS protocols and also for connect requests (through TCP/IP) from the Data Protection for SAP ProLE service. After connecting to the Server component, the Data Protection for SAP ProLE service connects and communicates directly with the Database Agent to send backup and restore data requested through the Data Protection for SAP instance. The Database Agent collects this data and stores all information related to the Operations Monitor in the Administration Assistant database through the Database component. The Database Agent forwards performance data to the Administration Assistant Server component, which records it in history files. The retention time for this data is definable at installation time (default 14 days). This data is accessed when the clients request any of the Administration Assistant monitoring or analysis functions. The Administration Assistant server-level components must be running and connected to the Data Protection for SAP ProLE service during the backup and restore operations in order to receive and store the history data. The existence of the database-related components is transparent to the client user.

An SAP system landscape contains several SAP systems, such as production, development, test, and education systems. A single Administration Assistant Server component can monitor many SAP database servers. A typical example is shown in Figure 6.

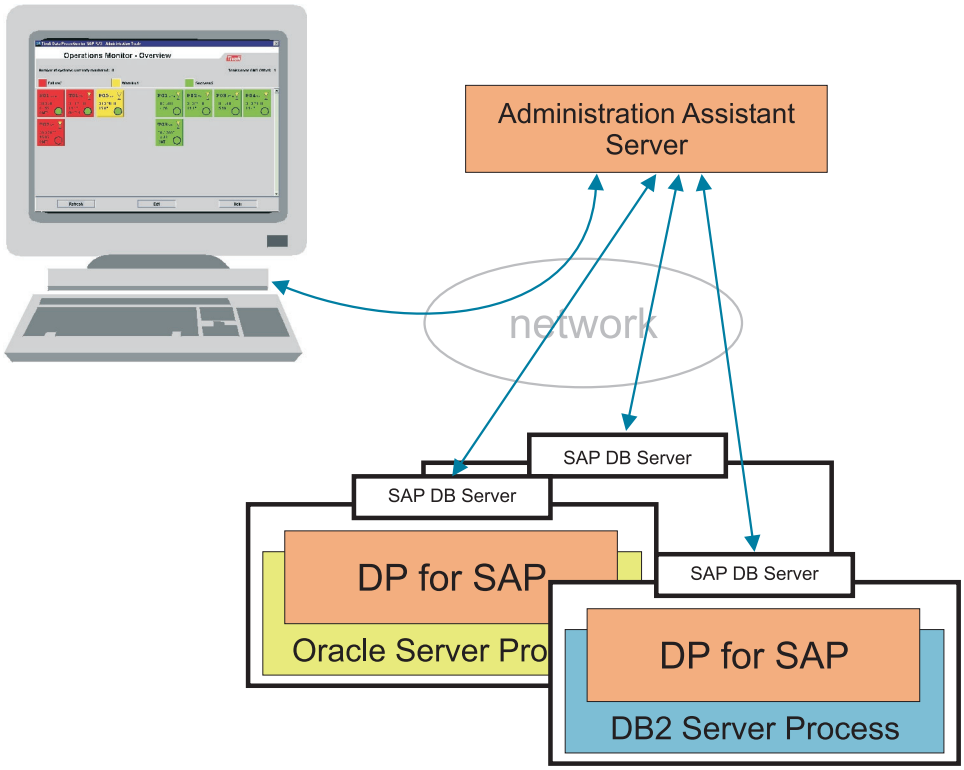


Figure 6. Example of an SAP Landscape

The Administration Assistant client is started from a browser by invoking the URL of the Server component host. The client is implemented as a Java™ applet that communicates with the Server component through a remote method invocation (RMI) connection.

- When the Administration Assistant Server component is started in non-secure mode (keyword nonsecure defined in the Server configuration file `assist.cfg`),

it accepts connect requests from a client to its HTTP port using the HTTP protocol. In this case, further communication between the client and server is via TCP/IP.

- When the Server component is started in secure mode (keyword nonsecure omitted from the Server configuration file), it accepts connect requests from a client to its HTTPS port through the HTTPS secure protocol. In this case, the Secure Sockets Layer (SSL) protocol is employed for all communication between the Administration Assistant clients and the Server component. The latest SSL protocol (Version 3) can be found at http://wp.netscape.com/eng/ssl3/.

The latest information on PKI with X.509 certificate can be found on the Web page of the IETF Working Group 'Public Key Infrastructure (X.509) (pkix)' at: http://www.ietf.org/html.charters/pkix-charter.html . XML- or HTML-format reports can be created by the Administration Assistant graphical user interface (or through a command-line interface from a scheduling client). The scheduling client is implemented as a Java application that communicates with the Administration Assistant Server component through an RMI connection.

Administration Assistant function for Data Protection for *SAP®*: Features

The Administration Assistant provides these features:

Monitor Operations
A centralized view of the backup status information for all SAP® systems registered with the Administration Assistant server is provided. Summaries of the backup status of all or a selection of SAP systems are available as well as detailed information on all backup runs of a specific SAP system. Thresholds can be defined to enable alerting under certain conditions.

View Performance Data
Performance information during Data Protection for *SAP®* for Oracle backup or restore operations is displayed. The Administration Assistant also saves this performance data and provides a graphical presentation for later analysis.

Simulate backup / restore
Configuration changes or production restores can be tested without changing the production environment or compromising production data. This function is provided for Oracle databases in combination with the BACKINT interface.

Configure systems
Configuration of the SAP backup profiles, the Data Protection for SAP profile, and the IBM Tivoli Storage Manager files for each of the SAP systems registered with the Administration Assistant server is provided. Online information also supports configuration. Additionally, profiles can be copied from one system to another system. When configuration changes are performed using the Administration Assistant, a configuration history is maintained so that a previous configuration can be reused.

Request problem support
This feature sends support requests directly to IBM. Although support requests contain user-specified problems the Administration Assistant automatically collects and forwards additional information, such as profiles and error logs.

Manage report templates
This allows the generation and maintenance of templates for producing reports.

Administer users
This feature defines user IDs and permissions in order to access the server component from the Administration Assistant client.

The primary documentation for the Administration Assistant is the integrated online help. The Administration Assistant also provides administrator-created reports in XML or HTML format that are generated from the output of *Monitor operations, View performance data,* and *Simulate backup / restore*.

Minimizing backup and restore processing with Data Protection for Snapshot Devices

Although Data Protection for *SAP*® for Oracle provides extensive storage capabilities, business-critical databases might demand even faster recovery operations. Data Protection for SAP and the product, *IBM Tivoli Storage Manager for Advanced Copy Services Data Protection for Snapshot Devices* (formerly known as Data Protection for FlashCopy Devices for SAP) provides back up and restore capabilities for the SAP® database on IBM FlashCopy® devices (such as IBM DS6000™ or DS8000®, IBM SAN Volume Controller (SVC), IBM Enterprise Storage Server®), or IBM System Storage™ N series devices with snapshot capability. These products can minimize downtime of the production systems by exploiting point-in-time copy functions exploited by these products.

Data Protection for Snapshot Devices product information is available at this Web site:

`http://www.ibm.com/software/tivoli/products/storage-mgr-advanced-copy-services/`

.

Chapter 2. Planning for Data Protection for *SAP®* for Oracle operations

Planning information regarding how to define an appropriate backup strategy for your SAP® system is provided.

The strategy you choose is dependent on your specific requirements. Consider these questions when reviewing this information:

- What type of events do you wish to protect your SAP® system against?
- How large is your database?
- What is the transaction rate of your database?
- How fast do you need to recover from a failure?
- What backup windows are available?

Planning a Backup Strategy for Your Oracle Database

To help prevent the loss of data associated with the Oracle database, back up these Oracle files and logs on a regular basis:

Data files
Files belonging to a specific tablespace (data files) are backed up by BRBACKUP. This is done at the file level, where offline or online backups are possible.

Control files
The control file is backed up by BRBACKUP whenever a tablespace backup occurs. Oracle provides mirroring of the control file to protect the running database system against corruption of this active file. The AIX LVM facilities can also be used to mirror these files.

Online redo logs
Online redo logs are backed up by BRBACKUP whenever a full offline database backup occurs. Oracle provides mirroring of the redo log files to protect the running database system against corruption of these active files. The AIX LVM facilities can also be used to mirror these files.

Offline redo logs
Offline redo logs are backed up by BRARCHIVE. You can specify that the redo logs be deleted from their original location when BRARCHIVE completes successfully. Additional information is available in "Cooperation of Data Protection for *SAP®* for Oracle with BRARCHIVE" on page 119.

SAP® system data and Oracle system data should also be backed up on a regular basis using the Tivoli Storage Manager backup-archive client incremental backup feature.

Figure 7 on page 12 shows the various backup scenarios within an SAP database server machine.

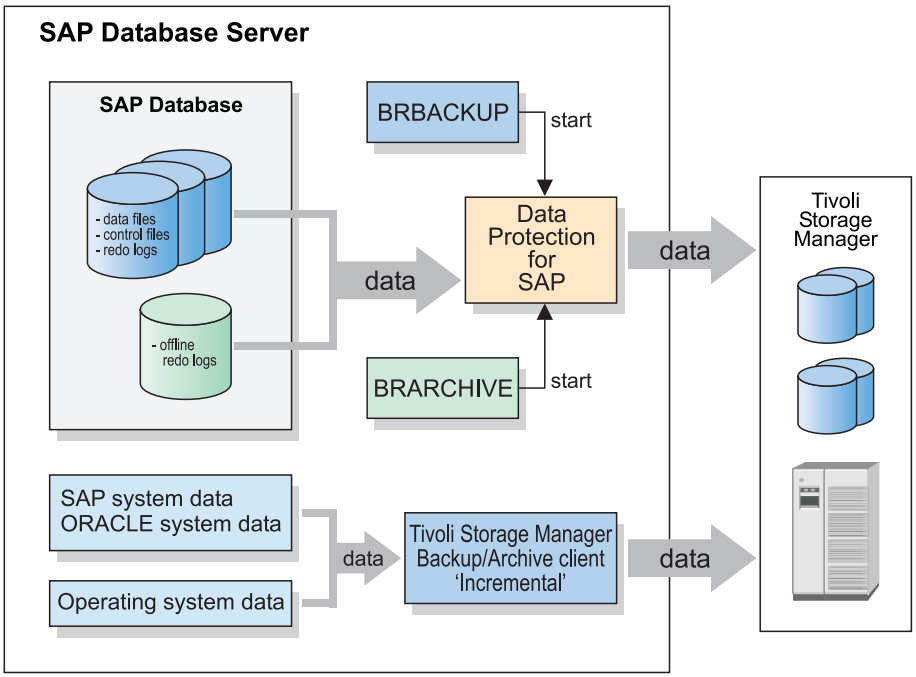


Figure 7. Backup Scenarios Within an SAP® Oracle Environment

Although the database is backed up with Data Protection for SAP, note that SAP, Oracle and operating system protocols are backed up directly by the Tivoli Storage Manager backup-archive client.

Planning a Backup Strategy for the Operating System

To help prevent a complete loss of the operating system, use operating system utilities (such as `mksysb` for AIX®) to perform system backups. Such backups should be performed after installing, updating, or upgrading the operating system. This will allow you to start your system from the backup medium. A configured TCP/IP environment and Tivoli Storage Manager Backup-Archive client installation should be included in a base backup in order to be able to restore all user dependent data.

Planning a Backup Strategy for Backup Protocols and Profiles

Every BRBACKUP and BRARCHIVE operation performs two actions. The first action backs up these type of objects:

- SAP® data files
- database control files
- online redo log files
- offline redo log files

Note that the type of object backed up depends on the action started (see previous section).

The second action backs up these profile and protocol files:

- BR*Tools profile (`init<SID>.dba`)
- BR*Tools Initialization profile (`init<SID>.sap`)
- Data Protection for SAP profile (`init<SID>.utl`)

- Oracle profile (`init<SID>.ora`)
- BRBACKUP summary log (`back<SID>.log`)
- BRARCHIVE summary log (`arch<SID>.log`)
- BRBACKUP/BRARCHIVE detailed log
- BR*Tools main log (`reorg<SID>.log`)
- Structure log (`struct<SID>.log`)

These profiles and protocols are required by the BR*Tools whenever a backup, restore, or recovery is performed. Unless these profile and protocol files have been backed up using a file system backup, they can only be restored using Data Protection for *SAP*® for Oracle. Data Protection for SAP File Manager can be used to restore one of these files (when lost) before running a BRRESTORE or BRRECOVER command. See "Data Protection for *SAP*® for Oracle File Manager" on page 71 for details. The directories and file systems that containing these profile and protocol files should be backed up separately. This helps prevent excessive recovery processing times when using Data Protection for SAP or the Data Protection for SAP File Manager in a disaster recovery situation.

Profile and protocol files are located in these directories:

UNIX or Linux

Directory	File
`/oracle/<SID>/sapreorg`	BR*Tools and structure logs
`/oracle/<SID>/sapbackup`	BRBACKUP logs
`/oracle/<SID>/saparch`	(BRARCHIVE logs
`/oracle/<SID>/dbs`	Profiles

Windows

Directory	File
`<drive>:\oracle\<SID>\sapreorg`	BR*Tools and structure logs
`<drive>:\oracle\<SID>\sapbackup`	BRBACKUP logs
`<drive>:\oracle\<SID>\saparch`	BRARCHIVE logs
`<drive>:\orant\database`	Profiles

Planning a Backup Strategy for SAP® System Data

In order to protect the system against the loss of SAP® executable files, user data, or even operating system data, use the Tivoli Storage Manager backup-archive client incremental backup feature. You can use the client to define an include-exclude list of files that to be backed up during incremental backup operation. The include-exclude list should exclude all relevant database data that has been backed up or archived by Data Protection for *SAP*® for Oracle, such as data files, the control file, and online or offline redo logs. See "Include/Exclude List Sample (UNIX and Linux)" on page 144 or "Include/Exclude List Sample (Windows)" on page 145 for example include-exclude lists. Example include-exclude list files are also provided in the Data Protection for SAP installation directory.

The information saved with the BRBACKUP and BRARCHIVE utilities is usually located in the following file systems or directories. Add these directories to the list

of paths to be excluded in the Tivoli Storage Manager backup-archive client include-exclude list. These entries will prevent the database from being backed up twice.

UNIX or Linux

```
/oracle/<SID>/saparch/
/oracle/<SID>/sapdata1/
/oracle/<SID>/sapdata2/
/oracle/<SID>/sapdata3/
/oracle/<SID>/sapdata4/
/oracle/<SID>/sapdata5/
/oracle/<SID>/sapdata6/
     .
     .
     .
/oracle/<SID>/origlogA/
/oracle/<SID>/origlogB/
```

Windows

```
<drive>:\oracle\<SID>\saparch\
<drive>:\oracle\<SID>\sapdata1\
<drive>:\oracle\<SID>\sapdata2\
<drive>:\oracle\<SID>\sapdata3\
<drive>:\oracle\<SID>\sapdata4\
<drive>:\oracle\<SID>\sapdata5\
<drive>:\oracle\<SID>\sapdata6\
     .
     .
     .
<drive>:\oracle\<SID>\origlogA\
<drive>:\oracle\<SID>\origlogB\
```

Database Server Considerations

In general, the production (SAP® database) server is the most critical component for data transfer. This is especially when parallelism is applied as described in "Performance Options of Data Protection for *SAP*® for Oracle" on page 96. As a result, special attention should be given to these items:

CPU power
Data transfer, data compression, local, or LAN-free backup operations can cause significant demands on the database server CPU. These demands are in addition to the application load caused by online backups. In many environments, the CPU is the most critical constraint. The CPU load for LAN-free backups (Managed System for SAN) can be significantly reduced by managing the buffers as described in "Buffer Copies" on page 98.

I/O paths
Fast disk attachments with internal busses (like a peripheral component interface) and file system features (like caching or reading ahead) can improve data transfer rates. These attachments and features can be especially useful for backup and restore operations that contain a significant number of files and large data volumes.

Volume Manager settings
Volume Manager provides volume mirroring options that can significantly reduce the data transfer rate during restore operations. As a result, not using volume mirroring options during restore operations can improve the data transfer rate.

Disk layout
The manner in which the database files are laid out can affect data transfer rates. Since Data Protection for SAP allows parallel access to database files during backup and restore operations, distribute data across several disks in order to take advantage of this feature.

Database size
The size of a database can be reduced by offloading inactive data to an external archive. For archive support, refer to the companion product *DB2 CommonStore for SAP*. This *CommonStore* product is database independent and therefore can also be used with Oracle. See "Archiving Inactive Data" on page 18 for additional information.

Size of the database files
When similar files are the same size, multiplexing can be used to improve data transfer rates.

Backup types.
Online backups save database files, control files, and redo logs non-disruptively. On the other hand, more data is saved to redo log files during an online backup. The amount of data saved to redo logs during an online backup may be decreased when using the file-online mode provided by SAP, while such a backup will take longer. Incremental backups will reduce the backup time and the amount of data to be sent to the backup server while restore time may be increased. For incremental backups, Oracle RMAN must be employed. For details on backup options, refer to your Oracle and SAP documentation.

Network Considerations

Consider these items when setting up the network:

LAN-free backup
LAN-free backup can reduce the load on the network and on the Tivoli Storage Manager server, thus improving data transfer rates. When using LAN-free backup, make sure fiber channel adapter capacity to the SAN can accommodate the data transfer rates of the disk reads and tape writes.

Network bandwidth
Experience reveals that the effective throughput capacity is approximately half of the theoretical network bandwidth. For high-speed networks (such as Gigabit Ethernet LAN), the network adapters limit the throughput rather than the network itself.

Network topology
A dedicated backbone network that is used only for backup and restore operations can improve the data transfer rate.

TCP options
Use TCP options that are the most beneficial for your environment.

Multiple Paths
Data Protection for *SAP*® for Oracle allows you to increase the overall throughput rate to the backup server by specifying multiple network paths. Details are provided in "Multiple Network Paths" on page 104.

Backup Server Considerations

Consider these items when setting up the Tivoli Storage Manager server. Note that Data Protection for *SAP*® for Oracle uses the Tivoli Storage Manager archive function for all backup activities:

Dedicated backup server
A dedicated backup server allows sharing of resources and provides an efficient resource utilization.

CPU power
Observations show that for a given data throughput, the CPU load on the backup server is approximately 60% of that on the database server. Therefore, backup server CPU power is not quite as critical as the CPU power of the database server. However, demands on the Tivoli Storage Manager server CPU do increase when several clients access a single Tivoli Storage Manager server.

Storage hierarchy
Backup of large data files should be directed to tape in order to achieve the highest transfer rates. If disks must be used, it is recommended to use one disk pool per session. Small files (such as log files) should be directed to disk storage first and then be migrated to tape collectively to avoid excessive tape mounts.

Parallel sessions
The Tivoli Storage Manager server allows using several tape drives in parallel to store data. This can increase overall data throughput. In order to exploit this feature, the corresponding Tivoli Storage Manager node must be allowed the appropriate number of mount points and the device class must be allowed the appropriate mount limits.

Detailed information on how to set up Tivoli Storage Manager for use with Data Protection for SAP can be found in "Alternate or parallel backup paths and backup servers" on page 17 and "Configure the Tivoli Storage Manager server" on page 57.

Storing data on a Tivoli Storage Manager server

Data Protection for SAP transfers data to and from the backup server through single or multiple (parallel) sessions to the Tivoli Storage Manager server. Each session must have a storage device associated with it. The SAP backup ID is persistently linked with each backup file. This backup ID can be used later to determine all files required for a complete restore.

In SAP® terminology 'backup' (BRBACKUP) means backup of data files, 'archive' (BRARCHIVE) means the backup of archived redo log files. Data Protection for *SAP*® for Oracle uses the Tivoli Storage Manager archive function for both backup types.

Tape storage is the preferred media for storing the database contents as this is proven to provide the best data throughput for backup and restore. In addition, the backup file sequence is maintained for restore which improves restore processing time. A disk-tape storage hierarchy is recommended for backing up log files, each log file should be backed up immediately after it is placed in the archive directory. This provides the best protection against data loss and eliminates the need to mount a tape for each 20 MB file.

Collocation is a Tivoli Storage Manager function that ensures client data is maintained together on one tape. Collocation should be deactivated in these situations:

- Deactivate collocation for Data Protection for SAP backups when enabling parallel sessions for use with multiple tape drives in parallel.
- Deactivate collocation when using the multiple log copy function as described in "Automation Options for Data Protection for *SAP*® for Oracle" on page 99.

SAP administration tools can generate information about backups that reside on the Tivoli Storage Manager server. This is performed by viewing the local (detailed) backup log or using the Data Protection for SAP File Manager (`backfm`). In addition to viewing backups, File Manager also allows the administrator to bypass SAP tools in order to query, delete, or restore backups and files.

To improve availability (alternate servers) or performance (multiple servers), configure Data Protection for SAP to use multiple Tivoli Storage Manager servers. Consider the location of all backup data before removing a Tivoli Storage Manager server from the Data Protection for SAP profile. Since Data Protection for SAP only accesses those servers defined in its profile, be cautious when removing a Tivoli Storage Manager server if it contains valid backup data.

Database backups are typically retained for a specified period and then become obsolete. In order to manage backup storage space efficiently, delete obsolete backups so that the tape storage space can be reclaimed. There are two ways to perform this deletion:

- Set an appropriate archive retention period with Tivoli Storage Manager options.
- Use the Data Protection for SAP backup version control function. When the number of backup versions (specified by this function) is exceeded, entire backup generations (such as full backups and all related redo log backups, are automatically deleted.

Note: Be aware that the SAP backup log may still list deleted (expired) backups since this log cannot be updated by Data Protection for SAP.

Alternate or parallel backup paths and backup servers

In Data Protection for *SAP*® terminology, path denotes a connection between a Tivoli Storage Manager client (Tivoli Storage Manager node) and a Tivoli Storage Manager server. A set of communication parameters are also set for each defined communication path. A Tivoli Storage Manager server network address is an example of a communication path. This set of communication parameters is called client option data and is collected under a logical server name. The logical server name is determined by the user. On UNIX or Linux systems, all client option data can be stored in a single file. this file is the client system option `dsm.sys` file. On Windows systems, the client option data for each logical server must be stored in separate client option files that have the file name `<servername>.opt`. For example, if there are two logical Tivoli Storage Manager servers *fast* and *slow*, then two client option files `fast.opt` and `slow.opt` are required. Windows also requires an additional client user option file, `dsm.opt`. All option files must reside in the same directory.

Data Protection for *SAP*® for Oracle can use several communication links between Tivoli Storage Manager clients in order to control alternate backup paths and alternate backup servers. This feature can increase throughput by transferring data over multiple paths simultaneously or to and from several servers in parallel. It

can improve the availability of the Tivoli Storage Manager client-to-server communication and enable disaster recovery backup to a special (remote) Tivoli Storage Manager server.

Each path in the `init<SID>.utl` profile is defined by a server statement and the corresponding definitions in the Tivoli Storage Manager client system option file `dsm.sys` (UNIX and Linux) or `<server>.opt` (Windows). See also "Sample Data Protection for *SAP*® for Oracle Profile for UNIX or Linux" on page 129 or "Sample Data Protection for *SAP*® for Oracle Profile for Windows" on page 134). The `SERVER <server 1..n>` statement denotes Tivoli Storage Manager servers defined in the Data Protection for SAP profile. This corresponds to the statement `SERVERNAME <server 1..n>` in the Tivoli Storage Manager client option file(s). These servers are identified by their `TCPSERVERADDRESS` and can be located on one system (multiple paths) or several systems (multiple servers). `SESSIONS` denotes the number of parallel session that Data Protection for SAP schedules for the given path. If only one path is used, `SESSIONS` must be equal to `MAX_SESSIONS`, which specifies the total number of parallel sessions to be used (equivalent to number of tape drives/management classes). Data Protection for SAP attempts to communicate with the Tivoli Storage Manager server using the first path in the profile. If this proves successful, Data Protection for SAP starts the number of parallel sessions as specified for this path. If the attempt was unsuccessful, this path is skipped and Data Protection for SAP continues to the next path. This process continues until as many sessions are active as were specified in the total session number (`MAX_SESSIONS`). If this number is never reached (for example, because several paths were inactive), Data Protection for SAP terminates the backup job.

Archiving Inactive Data

Data Protection for *SAP*® for Oracle creates a database image that is stored at the bit level and therefore, is designed for routine backup operations. Outdated backups must be restored into the same exact environment they were originally taken from in order to access the data from within SAP® applications. This requires maintaining older versions of SAP, operating system, database, and Tivoli Storage Manager data to rebuild this original environment. SAP provides archiving functions that can display business documents that are designated with long term retention requirements. These business documents are format-independent and can be used for auditing and other legal purposes. Archived data can then be removed from the operational database to reduce the database size and improve backup and restore processing time.

Long term archive requirements can be achieved with the IBM DB2 CommonStore for SAP product. Be aware that the DB2 CommonStore for SAP product is database independent and can be used with Oracle. This product accesses the SAP ArchiveLink interface and uses Tivoli Storage Manager to archive the following document types:

- inactive data (data retention)
- printlists (e.g. reports)
- outgoing documents (e.g. printed output like invoices, bills)
- incoming documents (e.g. digitized fax, scanned letters, audio)
- local documents (e.g. text, spreadsheets, pictures, graphics)
- inactive data

This demonstrates how Tivoli Storage Manager is used as an integrated repository for backup and archive tasks. DB2 CommonStore for SAP product information is available at this Web site: http://www.ibm.com/software/data/commonstore/

sap/.

Restore versus Backup

The majority of this section has addressed issues related to optimizing backups. In most cases, configuration changes and infrastructure problems affect both backup and restore operations similarly. Therefore, modifications supporting a fast backup while also exploiting resources can also be considered applicable to the restore operation. Generally, it is recommended to tune the backup and then run a restore test to verify that restore still works in a satisfactory manner.

During a restore operation, the values of these parameters are determined by their settings during the corresponding backup:

Compression
If compression is used during the backup, data needs to be decompressed.

Multiplexing
The same level of multiplexing as was used during backup is automatically applied during restore.

Multiple servers
When a backup is performed using multiple servers, the same servers must be online and available during the restore operation.

Creating multiple redo log copies

Data Protection for *SAP*® for Oracle can save a number of copies of each redo log by using different Tivoli Storage Manager server management classes. By creating multiple redo log copies on separate physical media, the administrator can restore and recover a database even if a backup tape becomes corrupt. This list identifies Data Protection for SAP profile keywords that are relevant in this multiple redo log context:

- Keyword BRARCHIVEMGTCLASS denotes the Tivoli Storage Manager server management classes to be used when saving redo logs. With the use of different management classes, the backup media targeted for redo logs is separated from the backup media targeted for the database objects. Different redo log copies can also be saved to different backup media.
- Keyword REDOLOG_COPIES allows the administrator to initiate the creation of multiple backup copies of each redo log. By creating multiple copies on separate physical media, the database administrator is able to restore and recover an Oracle database in an SAP® environment even if a backup tape becomes corrupt or lost.
- Keyword MAX_SESSIONS specifies the maximum number of sessions that a single Data Protection for SAP instance is allowed to access to the Tivoli Storage Manager server.

These rules describe how Data Protection for SAP satisfies a request to back up redo log files:

- Data Protection for SAP creates as many backup copies of each redo log as are specified by the REDOLOG_COPIES keyword.
- Data Protection for SAP requires that there are as many archive management classes (as defined by the BRARCHIVEMGTCLASS keyword) as there are redo log copies requested. To best protect against the loss of data, it is important that

the different management classes are linked to different storage pools within Tivoli Storage Manager storage so that the various redo log copies reside different backup media.

- When RMAN is used, Data Protection for SAP requires that the maximum number of sessions (as defined by the MAX_SESSIONS keyword) is greater than or equal to the number of redo log copies requested. A setup with a smaller number of sessions is not recommended with the BACKINT interface.
- Data Protection for SAP cannot control the order in which Tivoli Storage Manager processes the requests. Therefore, an administrator cannot rely on sessions to be processed in the order they were started by Data Protection for SAP.

Planning for using IBM HACMP for AIX

This section provides information about Data Protection for *SAP®* for Oracle that is useful when planning for HACMP fail-over configurations. This example uses the mutual takeover configuration (each node can take over the other node). If the application server and database server are installed on different hosts, the described actions need to be taken on the database servers only.

This figure illustrates the takeover environment:

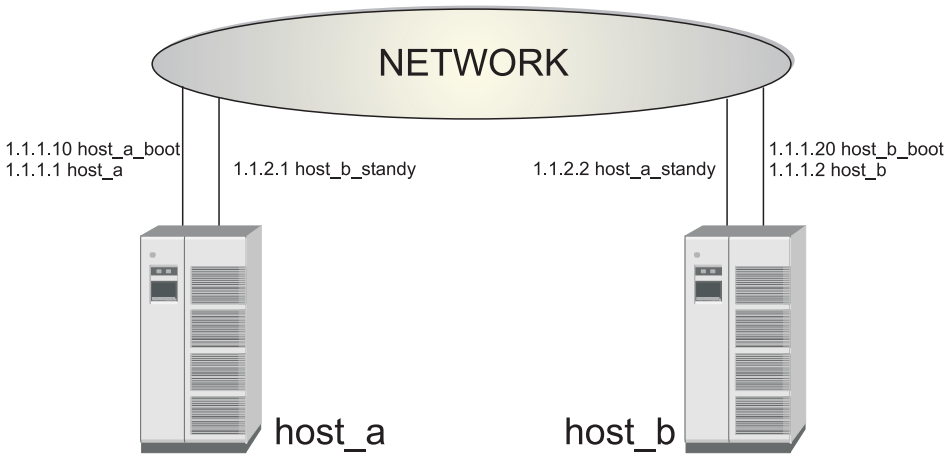


Figure 8. Sample Environment for HACMP Takeover

HACMP impact on Data Protection for *SAP®* for Oracle

A list of Data Protection for *SAP®* for Oracle components that are impacted by HACMP are provided.

Files

- The installation directory is `/usr/tivoli/TSM/tdp_r3`.
- Lock files are located in `/var/tdp_r3`.
- Disk sorting files are located in `/var/tdp_r3`.
- There is only one ProLE running on each host (even after takeover).
- Each SAP® system has its own Data Protection for SAP configuration files (`init<SID>.utl`, `init<SID>.bki`) in `$ORACLE_HOME/dbs`.

Dependencies

- Both hosts should have the same level of Tivoli Storage Manager API installed.

- Both hosts must be Data Protection for SAP.
- On both hosts, the dsm.sys file (in /usr/Tivoli/Tivoli Storage Manager/client/api/bin/dsm.sys) must contain all server names required for takeover.

Communication

`Backint` connects to `ProLE` using the following procedure:

- Retrieves the IP address for localhost (should be 127.0.0.1 for IPv4).
- Retrieves the `backint` service (should be 57323 for the 64-bit version).
- Connects to 127.0.0.1:<backint service>.

Digital Signing of Executable Files for Windows Systems

As of version 6.1, the Data Protection for *SAP*® for Oracle executable files (except .jar files) for Windows systems have a digital signature. The following files are affected:

- Passport Advantage package for Windows
- Data Protection for *SAP*® installation files
  - <version>-TIV-TSMERPORA-WinIA64.exe
  - <version>-TIV-TSMERPORA-WinX64.exe
- The Data Protection for *SAP*® application executable files
  - backfm.exe
  - backint.exe
  - createinfo.exe
  - prole.exe
  - orasbt.dll

Code signing employs digital IDs, also known as certificates.

Having a valid digital signature ensures the authenticity and integrity of an executable file. It identifies the software publisher as IBM Corporation to the person who downloads or executes it. However, it does not mean that the end-user or a system administrator implicitly trusts the publisher. A user or administrator must make the decision to install or run an application on a case-by-case basis, based on their knowledge of the software publisher and application. By default, a publisher is trusted only if its certificate is installed in the Trusted Publishers certificate store.

The customer can see the digital signature for any .EXE, .DLL, or installation wizard of Data Protection for *SAP*® using one of the following methods:

1. The digital signature can be viewed from the Digital Signature tab of Properties of the signed file. If you select the IBM Corporation item and click Details, you will see more information about the IBM Certificate and the entire chain of trusted Certificate Authority signatures.
2. In the case of the installation wizard, there is also the possibility to see the IBM digital signature from the software publisher link displayed in the Security Warning window.

A warning is issued if the installation executable file is downloaded from a site that is not listed as a trusted site. The security warning is not related to the fact that executable files contain digital certificates. It is related to the security zone policy of the site you download the file from. There is also another condition to be

met: the executable must be stored on an NTFS disk. Windows Server 2008 includes Internet Explorer 7, and its default security configurations are set according to the Internet Explorer Enhanced Security Configuration on four different security zones: Internet, local intranet, trusted, and restricted sites. The Internet Explorer Enhanced Security Configuration component (also known as Microsoft Internet Explorer hardening) reduces a server's vulnerability to attacks from Web content by applying more restrictive Internet Explorer security settings. As a consequence, Internet Explorer Enhanced Security Configuration may prevent some Web sites from displaying properly or performing as expected. It may also prevent users and administrators from accessing resources with Universal Naming Convention (UNC) paths on a corporate intranet. Refer to this document for more information on managing Internet Explorer Enhanced Security Configuration: http://www.microsoft.com/downloads/details.aspx?FamilyID=d41b036c-e2e1-4960-99bb-9757f7e9e31b&DisplayLang;=en You might get a security warning displayed whenever you run an executable file downloaded using the Internet Explorer from a URL or UNC that is not a member of the trusted security zone.

When a downloaded file is saved to a disk formatted with NTFS, it will update the meta data for the file with the zone (Internet or restricted-) it was downloaded from. The meta data is saved as an Alternate Data Stream (ADS), which is a feature of NTFS with which the same filename can be used to cover multiple data streams. When opening a file which includes an ADS that identifies it as being from another zone, the Attachment Execution Services (AES) software is activated, which reacts to the following file categories as described:

- **High risk:** Blocks the file from being opened when the file is from the restricted-zone: The following security warning is issued:

```
Windows Security Warning:
Windows found that this file is potentially harmful.
To help protect your computer, Windows has blocked access to this file.
```

- **Moderate risk:** Prompts with a warning before the file is opened when the file is from the Internet zone:

```
Open File - Security Warning:
      The publisher could not be verified. Are you sure you want to run this software?
```

- **Low risk**: Opens the file with no warnings.

Warning messages do not prevent the file from being used.

Note: This is different from configuring the Web Server with a digital certificate. During the installation of the Administration Assistant, the customer has the option to generate a self-signed certificate for the AA server and to use it to configure the security communication over HTTPS between the Administration Assistant server component and the clients. Alternatively there is the possibility to configure the security communication later after the installation completes using the instructions provided under ″Configuring for Secure Communication″.

Chapter 3. Installing Data Protection for *SAP®* for Oracle for V6.1

Information needed to install the various Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for *SAP®* for Oracle components is provided.

Review the appropriate prerequisite information before attempting to perform any installation tasks.

Note: As of TSM 6.1, Data Protection for *SAP®* and the Administration Assistant function for Data Protection for *SAP®* are installed via InstallAnywhere rather than InstallShield. Slightly modified procedures are required to employ console mode (non-graphical user interface) or perform a silent installation. See "Installing Data Protection for *SAP®* for Oracle in Silent Mode" on page 25.

Furthermore, Windows executable files (except Java) contain a digital signature to certify that the software originated by IBM. For more information, see "Digital Signing of Executable Files for Windows Systems" on page 21.

Required installation tasks

Data Protection for *SAP®* for Oracle must be installed on all SAP® database servers. The following tasks are required to set up Data Protection for SAP:

1. Verify the Data Protection for *SAP®* for Oracle package is complete. See the README.1ST file on each installation disc (or disc image) for a description of the contents.
2. Verify that the prerequisites are met as described in "Prerequisites" on page 24.
3. Review planning sheet information as described in "Data Protection for *SAP®* for Oracle (base product) planning sheet" on page 146.
4. (Optional) Install the Administration Assistant function for Data Protection for *SAP®* prior to installing Data Protection for SAP. Data Protection for SAP can automatically connect to the Administration Assistant as part of its installation procedure. Details are available in "Administration Assistant function for Data Protection for *SAP®*: Features" on page 8.
5. Install Data Protection for SAP as described in "Installing Data Protection for *SAP®* for Oracle on UNIX or Linux" on page 26 or "Installing Data Protection for *SAP®* for Oracle on Windows" on page 28. See "Upgrade the Data Protection for *SAP®* for Oracle V6.1 base product" on page 35 when upgrading a previous version of Data Protection for SAP.
6. Perform post-installation tasks as such as "Configure the Tivoli Storage Manager client options" on page 54 and "Configure the Tivoli Storage Manager server" on page 57.
7. Verify the installation completed successfully as described in "Verify the installation" on page 39.

Note these additional requirements:

- Data Protection for SAP can be installed and operated for SAP® systems with Oracle databases employing a standard file system or raw logical volumes.
- Be aware of the minor differences between UNIX or Linux and Windows versions of Data Protection for SAP. For example, UNIX or Linux uses the path

separator "/" and Windows uses the path separator "\" with a drive letter. Insignificant differences are documented where applicable.

Installing the Data Protection for *SAP®* for Oracle V6.1 base product

Information needed to install the Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for *SAP®* for Oracle base product is provided.

Perform the installation tasks for the appropriate operating system.

Prerequisites

The installation packages are located on the Data Protection for *SAP®* for Oracle product installation disk, disk image (from Passport Advantage), and occasionally on the IBM public FTP server. Initial installations must always be done from the disc or image. Refer to the file `README.1ST` in the root path for information on where to find documents on the disc or image, and follow the appropriate installation description below. See the README.1ST file in the root directory of the disc or image for a list of its contents.

If you are going to upgrade from an earlier version of Tivoli Data Protection for R/3 or Data Protection for SAP in your environment, you have the option to either upgrade from the product disc or image, or to download the latest version from the IBM FTP server. See *http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliStorageManagerforEnterpriseResourcePlanning.html* . For the specific procedure for upgrading from an earlier version, refer to "Upgrade the Data Protection for *SAP®* for Oracle V6.1 base product" on page 35.

These products must be installed before attempting to install Data Protection for SAP:

- Oracle Database
- SAP® R/3 or SAP e-business Solution, based on Oracle

  The SAP Service Marketplace (*http://service sap.com/*) provides the most current information related to SAP features, product versions, and maintenance levels that are compatible with your version of SAP R/3 or SAP. .
- Tivoli Storage Manager backup-archive client

  For information on configuration of the Tivoli Storage Manager API client, refer to "Configure the Tivoli Storage Manager client options" on page 54. TCP/IP must be ready for communication between the Tivoli Storage Manager server and the Tivoli Storage Manager client.
- An operating system level supported by SAP and the Tivoli Storage Manager client

The Release Notes file on the Tivoli Information Center contains the most current information related to Data Protection for SAP hardware, software, operating system, and maintenance levels.

In case Data Protection for SAP is to be installed on a distributed file system, the root user needs read and write access to the file system for the duration of the installation. For more information on the installation in a distributed file system, refer to: "Configuring Data Protection for *SAP®* for Oracle in a Distributed File System" on page 49.

Installation planning forms for Data Protection for SAP and the Administration Assistant are available in the `planning_sheet` (UNIX and Linux) or

`planning_sheet.txt` (Windows) files located in the installation directory. They are also available for printing in "Data Protection for *SAP*® for Oracle (base product) planning sheet" on page 146. Once prerequisites are met and installation planning information is completed, Data Protection for SAP is ready to be installed.

Installing Data Protection for *SAP*® for Oracle in Silent Mode

Information on installing the product without using a graphical user interface.

To support target systems without a window manager, the setup program supports deploying an installation in console mode. An installation running in console mode suppresses the graphical wizard panel display available with a GUI installation. Instead, user data entry and status messages are displayed on the console or in the command prompt window.

You can optionally use a response file for silent, or unattended, installation.

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

```
./<version>-TIV-TSMERPORA-<platform>.bin [-i console] -r=<properties file>
```

1. Create the response (properties) file, such as installer.properties.
2. Invoke the executable file with the -i console option (console mode) and the -f option if a properties file was generated

   ```
   .<version>-TIV-TSMERPORA-<platform>.bin -i silent -f <properties file>
   ```

   The <properties file> specification must contain a full path.

Sample properties file:

```
#Has the license been accepted
#----------------------------
LICENSE_ACCEPTED=TRUE

#SID
#---
SID=<SID>

#Path Configuration
#------------------
SAP_BR_TOOL=/usr/sap/&ltSID&gt;/SYS/exe/run/
SAP_CFG_FILE=/oracle/&ltSID>/10201_IA64/dbs

#TSM Configuration
#-----------------
TSMUTL_YESNO=\"Yes (recommended for first time installation)\",\"\"
TSMUTL_YESNO_1=Yes (recommended for first time installation)
TSMUTL_YESNO_2=
TSMUTL_YESNO_BOOLEAN_1=1
TSMUTL_YESNO_BOOLEAN_2=0
TSMUTL_SERVERADRESSE=<TSMServer>
TSMUTL_NODE=R3NODE TSMUTL_BACKUPMGM=MDBDISK1
TSMUTL_ARCHIVEMGM=MLOG1 MLOG2

#RMAN Support
#------------
RMANYES=0
RMANNO=1

#Administration Assistant
#------------------------
NAMEPORTAA_ADRESSE=<AAServer>
NAMEPORTAA_PORT=5126
```

Note that lines starting with '#' are treated as comments.

Installing Data Protection for *SAP®* for Oracle on UNIX or Linux

Data Protection for *SAP®* for Oracle for these operating systems is delivered as a single executable file for each platform. Packages on the FTP server contain 'FTP' prior to the platform designation.

- For a disc or disc image, the name has the format:

  `<version>-TIV-TSMERPORA-<platform>`

When the file is launched, Data Protection for SAP guides you through the installation procedure. Read the descriptions carefully and follow the guidelines that are displayed on the panels.

Shared libraries have different file extensions on different UNIX or Linux platforms. Within the following the section, the file extensions of shared libraries are represented as '*<ext>*'. Replace this text with the extension applying to your platform:

Table 5. File Extensions for Shared Libraries

Operating System	Extension
AIX	a
HP-UX	sl
Linux	so
Solaris	so

In the following description you have to replace the directory name ora<bit> in the installation path. Depending on the version of Data Protection for SAP you have installed, you must replace it with

Directory name	Bit-width version of DP for SAP
ora	32
ora64	64

Perform the following tasks to install Data Protection for SAP on a UNIX or Linux system:

1. Log in as the *root* user on the SAP database server machine.
2. If the Oracle RMAN interface will be used, configure the Tivoli Storage Manager backup-archive client on your SAP database server as described in "Configure the Tivoli Storage Manager client options" on page 54.
3. Make sure the DISPLAY variable is set to view the installation prompts through a graphical X-Window.
4. Invoke the appropriate Data Protection for SAP installation file for your operating system and your Oracle database.
5. Perform these tasks if the Oracle RMAN interface was selected during the installation process:
   a. Set the Data Protection for SAP password for Tivoli Storage Manager as described in "7. Determine the Tivoli Storage Manager password method" on page 61.
   b. Make sure /usr/lib is specified in the library path environment of your system.
   c. Customize the SAP backup profile init<SID>.sap to use RMAN by adding this text:

```
backup_dev_type=rman_util
rman_parms="ENV=(XINT_PROFILE=<path>/init<SID>.utl,
PROLE_PORT=<portnumber>,&BR_INFO)"
```

      Locate the appropriate *ProLE* port number in the /etc/services file. Look for port name tdpr3ora64.
6. If the Oracle RMAN interface was not selected during the installation process, create these links:

```
cd $ORACLE_HOME/rdbms/lib
ln -s /usr/tivoli/tsm/tdp_r3/ora64/libtdp_r3.<ext> /usr/lib/libobk.<ext>
ln -s /usr/lib/libobk.<ext> $ORACLE_HOME/lib/libobk.<ext>
```

7. View the summary at the end of the installation dialog. The summary displays the Data Protection for SAP installation path where the installation log file (log.txt) is located.

These modifications are automatically performed to your system during installation:

- An entry is created in /etc/inittab that automatically starts the "ProLE" daemon.
- An entry is created in /etc/services for internal communication.

These files are installed in the Data Protection for SAP installation directory:

```
backint
prole
createinfo
backfm
initSID.bki
libtdp_r3.<ext>
archive.ksh
backup.ksh
crontab.sample
dsm.opt
dsm.sys
gensortfile.sh
SanFSsetupFS.sh (AIX only)
inclexcl.list
README
README_TSMERP<version><language>.html
TIPHINTS
agent.lic (Only after installation from disc or disc image. This file is not
present in the packages available on the FTP server.)
```

The `_uninst` folder is also created, which contains additional files.

These Data Protection for SAP configuration files are installed in the SAP directory (typically, /oracle/SID/dbs):

```
init<SID>.utl
init<SID>.bki
agent.lic (copy of file in installation directory)
```

Installing Data Protection for *SAP®* for Oracle on Windows

Note: As of TSM 6.1, Data Protection for *SAP®* for Oracle and the Administration Assistant function for Data Protection for *SAP®* are installed via InstallAnywhere rather than InstallShield. Slightly modified procedures are required to employ console mode (non-graphical user interface) or perform a silent installation. .

Furthermore, Windows executable files (except .jar files) contain a digital signature to certify that the software originated from IBM. For more information, see "Digital Signing of Executable Files for Windows Systems" on page 21.

Data Protection for SAP for Windows is delivered as a single executable file (`.exe`) for each platform. Packages on the FTP server contain 'FTP' prior to the platform designation.

Data Protection for SAP for these operating systems is delivered as a single executable file for each platform. The packages are named as follows:

- The package name on the disc (or disc image):

  ```
  <version>-TIV-TSMERPORA-<platform>
  ```

Perform these tasks to install Data Protection for SAP on a Windows system:

1. Log in as a user with Administrator authority on the SAP database server machine.
2. If the RMAN interface is to be installed:
   a. Stop the `OracleService<SID>` service.
   b. Configure the Tivoli Storage Manager backup-archive client on your SAP database server as described in "Configure the Tivoli Storage Manager client options" on page 54).

3. In Windows Explorer, navigate to the directory where the installation package is located.
4. Invoke the Data Protection for SAP executable and follow the instructions of the installation dialog.
5. Perform these tasks if the Oracle RMAN interface was selected during the installation process:
   a. Set the Data Protection for SAP password for Tivoli Storage Manager as described in "7. Determine the Tivoli Storage Manager password method" on page 61.
   b. Customize the SAP backup profile `init<SID>.sap` to use RMAN by adding this text:

      ```
      backup_dev_type=rman_util
      rman_parms="ENV=(XINT_PROFILE=<path>/init<SID>.utl,
      PROLE_PORT=<portnumber>,&BR_INFO)"
      ```

      Locate the appropriate *ProLE* port number in the `<drive>:\WINNT\system32\drivers\etc\services` file. Look for port name tdpr3ora64.
   c. Restart the Oracle service: `OracleService<SID>`.
6. View the summary at the end of the installation dialog. The summary displays the Data Protection for SAP installation path where the installation log file (`log.txt`) is located.

The following modifications are performed on your system during installation:

- The ProLE service background process is created.
- An entry required for internal communication is created in `%WINDIR%\system32\drivers\etc\services`.

These files are installed in the Data Protection for SAP installation directory:

```
backint.exe
prole.exe
createinfo.exe
orasbt.dll
backfm.exe
backup.cmd
server_a.opt
server_b.opt
inclexcl.list
schedule.sample
dsm.opt
README.txt
README_TSMERP<version><language>.html
TIPHINTS
agent.lic (Only after installation from disc or disc image. This file is not
present in the packages available on the FTP server.)
```

The `_uninst` folder is also created, which contains additional files.

These Data Protection for SAP configuration files are installed in the SAP directory:

```
initSID.bki
initSID.utl
agent.lic (Only after installation from disc or disc image. Not present in the
Web package.)
```

Enable ProLE to access configuration files on a remote share

When Windows is started as a regular service, it operates (by default) under the ID of the local system account with Administrator privileges. However, a session opened on a remote system will not have credentials or permissions. Microsoft knowledge base article 132679 provides information about this situation:

`http://support.microsoft.com/kb/132679`

This situation prevents the ProLE service from accessing files that reside on a remote share. This is true even when the share is mapped to a local drive letter or is accessed as a UNC notation (\\server\path\filename). Data Protection for *SAP*® for Oracle version 5.4 (or later) accepts UNC notation for the profile and infile (passed through the backint command line) but not for all the files specified within the profile. These files will be opened by ProLE, which by default has no permission to access remote shares, as explained above.

Perform these tasks to enable ProLE to access such files on a remote share:

1. Map the share where the configuration files reside to a local drive letter.
2. Modify the profile (.utl) to refer to the path names on the mapped drive.
3. Modify the ProLE service so that it runs as an account with permissions to access the mapped drive (and not as a local system account). Note that this might have other implications when using a regular account. For example, when the password for this account expires or is changed, the service will no longer be able to start.
4. Restart the ProLE service to activate the changes.

Uninstalling the Old Version of Data Protection for *SAP*® for Oracle under UNIX or Linux

Perform these tasks to uninstall a previous version of Data Protection for SAP:

1. Log in on the SAP® database server machine as root user .
2. Make sure that the DISPLAY variable is set correctly as the uninstall procedure requires a graphical X-Window.
3. Make sure the previous version of Data Protection for *SAP*® for Oracle is not running.
4. Launch the uninstall executable file and follow the instructions of the uninstall procedure. The uninstall executable file is located in one of the following directories:
   - AIX 64-bit:
     `/usr/tivoli/tsm/tdp_r3/ora64/_uninst/uninstaller.bin`
   - Other UNIX 64-bit or Linux 64-bit:
     `/opt/tivoli/tsm/tdp_r3/ora64/_unist/uninstaller.bin`

Uninstalling the Old Version of Data Protection for *SAP®* for Oracle under Windows

Perform these tasks to uninstall a previous version of Data Protection for *SAP®* for Oracle on a Windows NT®, Windows 2000, or Windows 2003 machine:

1. Log on as user with administrator authority on the SAP® database server machine.
2. Ensure that the previous version of Data Protection for SAP is not running.
3. Select **Start → Settings → Control** panel.
4. Click on **Add/Remove Programs**.
5. Select the old version of **Data Protection for SAP** and click on **Remove**.
6. Follow the instructions of the uninstall procedure.

Installing the Administration Assistant function for Data Protection for *SAP®* V6.1

The Administration Assistant function for Data Protection for *SAP®* is a Web-browser based graphical interface that provides customization, simulation, and analysis of SAP® database backup, restore, and configuration operations. Information needed to install the Administration Assistant function for Data Protection for *SAP®* V6.1 is provided.

Perform these tasks to install the Administration Assistant function for Data Protection for *SAP®*.

Prerequisites for Installing the Administration Assistant function for Data Protection for *SAP®*

Prerequisites: Server-Level Components

The following products must be installed before setting up the Administration Assistant function for Data Protection for *SAP®* server-level components:

- Java Runtime Environment (JRE) or Java Development Kit (JDK)
- Java Beans Activation Framework (JAF)
- Java Mail
- IBM DB2 data server (optional DBMS for Administration Assistant database). If you elect to use DB2, make sure DB2 is running. In addition, UNIX and Linux systems require that a dedicated system user (for which the DB2 instance should be installed) be created.
- For software, hardware, and maintenance levels required by the current version of the Administration Assistant, refer to the Data Protection for *SAP®* for Oracle release notes.
- TCP/IP must be ready for communication before starting up the Administration Assistant server-level components.

Prerequisites: Client Components

These requirements must be met before starting the Administration Assistant function for Data Protection for *SAP®* client:

- A fully Java-capable Web browser with Java plugin. The applet loaded from the Administration Assistant server must be granted these permissions:

– Permission to establish a connection to the Administration Assistant server through RMI. For example:

```
permission java.net.SocketPermission "<Server component hostname>:1024-", "connect";
```

– Permission to switch to a different language. For example:

```
permission java.util.PropertyPermission "user.language", "write";
```

- In order to view report graphics, a browser that supports Scalable Vector Graphics (SVG), like Adobe SVG Viewer, must be available.
- (UNIX or Linux): An X Window system is required for the Administration Assistant client.
- A minimum screen resolution of 1024x768 pixels (1280x1024 or higher is recommended).
- For software and maintenance levels required by the current version of the Administration Assistant, refer to the Data Protection for SAP release notes.
- TCP/IP must be ready for communication before starting up the Administration Assistant server-level components.

Prerequisites: Scheduling Client

These requirements must be met when selecting the scheduling client:

- A TCP/IP connection can be established to the Administration Assistant Server component.
- A Java VM is available.
- In order to view report graphics, a browser that supports Scalable Vector Graphics (SVG), like Adobe SVG Viewer, must be available.

Installation Planning for Server-Level Components

See Table 15 on page 148 for a list of planning requirements in table form. This information is also available in the `planning_sheet_aa` (UNIX or Linux) and `planning_sheet_aa.txt`. (Windows) files in the Data Protection for SAP installation directory.

Installing the Administration Assistant function for Data Protection for *SAP®* Server-Level Components

Initial installations must be performed from the installation disc or disc image. Refer to the `README.1ST` file in the root path of the disc or disc image for the most current information. The Administration Assistant installation packages reside on each of the Data Protection for *SAP®* for Oracle discs or disc images, and can be downloaded from the IBM FTP server. The Administration Assistant installation package is a single, platform-independent .jar file with this name convention:

```
<version>-TIV-TSMERPAABASE-MULTI.jar
```

When upgrading from an earlier version of the Administration Assistant function for Data Protection for *SAP®*, the latest version is available for download from the IBM FTP server. Additional upgrade information is available in “Upgrade the Administration Assistant function for Data Protection for *SAP®* V6.1” on page 36.

A setup assistant is included in the Administration Assistant package that helps guide the installation process in English or multi-language version. Be aware of the considerations before attempting to install the Administration Assistant:

- System administrator privileges are required to install the Administration Assistant.
- If a multi-host installation (which distributes the server-level components over two or more hosts) is to be performed, copy the package file to each target host. Then perform a custom installation so that components are selected for that host.
- The CLASSPATH environment variable is not required. However, if this variable is set, you must specify the directory in which the package file resides.
- After installation, in order to switch the language (specified during installation), the Administration Assistant must be uninstalled and install again with the preferred language.

Specify this command to start the installation:

```
java -jar <package file name>
```

After the first component is installed, an overview panel displays the installation status and records user entries.

During installation, the following modifications are made to your system automatically:

- All necessary paths (installation, history, OnDoc, log paths) are created. Corresponding files are copied into the installation and OnDoc directories.
- These Administration Assistant startup files are created and added to the installation directory:

Component	UNIX or Linux	Windows
Server	sadma.sh	sadma.cmd
Database Agent	sdba.sh	sdba.cmd

- The configuration file `assist.cfg`, containing all relevant configuration parameters specified during the installation, is created and added to the installation directory.
- The configuration file `dbagent.cfg` containing all relevant configuration parameters specified during installation of the Database Agent component is created and added to the installation directory.
- On Windows systems, a service is installed and automatically started. This service starts `AAStart.exe` and `java.exe`.
- On UNIX or Linux systems, a new `/etc/init.d` entry is created for each Administration Assistant server-level component and the components are started automatically. Note that an administrator must create appropriate run level entries for these components in order for automatic start and stop features to function:

Component	Entry in /etc/init.d
Server	adminAssistant, with parameters start, stop, and status
Database Agent	databaseAgent, with parameters start, stop, and status

Component	Entry in /etc/init.d
Database (Derby) (optional, as alternative to DB2)	apacheDerby, with parameters start and stop
Database (DB2) (optional, as alternative to Derby)	Not applicable

For an installation using IBM DB2:

- On Windows systems, the database tables are created and no other changes are made.
- On UNIX and Linux systems, a DB2 instance for the specified user ($USERNAME) is created. These changes are also made to the system:
  - An entry in /etc/services is added:

```
$USERNAME   $PORT/tcp   # used for Data Protection for SAP - Administration Assistant with DB2 support
```

  - Changes to the created DB2 instance:
    - Set DB2 profile registry variable: `DB2COMM=tcpip`
    - Set DB2 database manager parameter: `SVCENAME=$USERNAME`
    - Set DB2 database manager parameter: `SPM_NAME=NULL`

For an installation using secure communication:

- A keystore is created on request.
- An X.509 v1 self-signed certificate containing a key pair with the hostname as an alias is created in the keystore on request.
- The server's self-signed certificate is imported into the truststore on request.
- The server's self-signed certificate is exported to a certificate file on request.
- A Certificate Signing Request is created if desired.

Consider these items before uninstalling the Administration Assistant server-level components:

- The Administration Assistant client component is not physically installed. It operates as a Java applet when the URL of the host running the Server component is called. No action needs to be taken at the client level when uninstalling the Administration Assistant server-level components.
- The public key infrastructure will not be modified when uninstalling the Administration Assistant components, even if it was originally set up during its installation process.

To uninstall the Administration Assistant server-level components, change to the uninstall directory (in the Administration Assistant installation directory) on each system on which one of the components was installed and issue this following command:

```
java -jar uninstall.jar
```

The command files open an uninstall assistant which guides you through the process.

Chapter 4. Upgrading to Data Protection for *SAP®* for Oracle for V6.1

Information needed to upgrade to Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for *SAP®* for Oracle V6.1 is provided.

Perform these tasks to upgrade to Data Protection for *SAP®* for Oracle V6.1.

Upgrade the Data Protection for *SAP®* for Oracle V6.1 base product

Note: The format of the configuration file (.bki) was changed with version 5.4. The software accepts the previous format and converts it automatically.

If it is necessary to use a version earlier than 5.4, the old format can be recovered by overwriting the new file with the empty file (provided with the previous version). the file must then be initialized by setting the Tivoli Storage Manager password. However, the information about the current backup number will be lost. As a result, more backup versions must be retained for a longer period of time than is specified by the MAX_VERSIONS parameter.

Perform these tasks to upgrade Data Protection for SAP from an earlier version:

1. Verify that the Data Protection for *SAP®* for Oracle package is complete. The installation packages are provided on a disc, disc image (downloadable from Passport Advantage), or the IBM FTP server. See the release notes file in the Tivoli Information Center for the most current release information.
2. Data that was backed up with Tivoli Data Protection for R/3 Version 2.7 must be restored with Tivoli Data Protection for R/3 Version 3.1 or 3.2. Data that was backed up with Tivoli Data Protection for R/3 Version 3.1 or 3.2 or Data Protection for SAP Version 3.3 can be restored with Data Protection for SAP Version 3.3 (or later).
3. Make sure that the requirements for the new version of Data Protection for SAP are met as described in “Prerequisites” on page 24.
4. Make sure planning information is available as described in “Prerequisites” on page 24.
5. A full backup of the SAP® database should be performed before upgrading to the new version.
6. Uninstall the old version as described in “Uninstalling the Old Version of Data Protection for *SAP®* for Oracle under UNIX or Linux” on page 30 or “Uninstalling the Old Version of Data Protection for *SAP®* for Oracle under Windows” on page 31.
7. Install the new version of Data Protection for SAP as described in “Prerequisites” on page 24.
8. Verify the installation as described in “Verify the installation” on page 39.
9. A full backup should be performed after upgrading to the new version.
10. Following an upgrade and subsequent RMAN setup on Windows, start (or restart) service `OracleService<SID>` in order to activate the new Data Protection for SAP environment.

Upgrade the Administration Assistant function for Data Protection for *SAP®* V6.1

Perform these tasks to upgrade the Administration Assistant function for Data Protection for *SAP®* server to a new version:

1. Verify that the Administration Assistant package is complete. The Administration Assistant is provided on each of the Data Protection for SAP installation discs or disc images, or downloaded from the IBM FTP server.
2. Verify that the new Administration Assistant requirements are met as described in "Prerequisites for Installing the Administration Assistant function for Data Protection for *SAP®*" on page 31. Note that the Data Protection for *SAP®* for Oracle release notes contain the latest requirement information.
3. Review planning information as described in "Prerequisites for Installing the Administration Assistant function for Data Protection for *SAP®*" on page 31.
4. If you plan to migrate existing data to the new version, perform the tasks described in "Migrate Administration Assistant function for Data Protection for *SAP®* data from a previous release."
5. Uninstall the old version of the Administration Assistant as described in "Installing the Administration Assistant function for Data Protection for *SAP®* Server-Level Components" on page 32.
6. Install the new version of the Administration Assistant server-level components as described in "Installing the Administration Assistant function for Data Protection for *SAP®* Server-Level Components" on page 32.
7. Perform the configuration tasks beginning with "1. Prepare a secure connection" on page 45.
8. Set up the Administration Assistant client as described in "2. Configure the Administration Assistant function for Data Protection for *SAP®* Client" on page 47.
9. Verify the installation as described in "3. Verify the Administration Assistant function for Data Protection for *SAP®* installation" on page 47.

Note: It is possible to use the Administration Assistant in conjunction with supported Data Protection for SAP versions prior to version 5.4, provided the Administration Assistant is installed on a single host.

Migrate Administration Assistant function for Data Protection for *SAP®* data from a previous release

Note: The following procedure must be performed before uninstalling the Administration Assistant and installing the new version. In addition, Data Protection for *SAP®* for Oracle does not provide support for transferring data from an installation of the Administration Assistant prior to version 5.4. If desired, the report function can be used to capture data from the prior version before the new version is installed.

Migrating Database Data

Information on transferring data from the database of a previous version of the product.

Note: It is recommended that you make a backup of the current Administration Assistant function for Data Protection for *SAP*® database before starting the migration process.

1. **From Administration Assistant function for Data Protection for *SAP*® 5.4**
   a. The export tool is provided on each Data Protection for *SAP*® for Oracle installation disc (or disc image) in the migration directory. This directory contains:
      - aaDerbyAdaption.jar
      - prepareExport.sql c.
      - export.cmd (for use with Windows systems)
      - export.sh and export ksh (for use with UNIX/Linux systems)

      Copy these files from the installation disc (or disc image) for the new version of the Administration Assistant to your system.
   b. If you are using Apache Derby, get information on how to connect to the Apache Derby database. These settings are provided in file assist.cfg and are listed below:
      - Location of your previous installation of the Administration Assistant
      - Username to connect to the Apache Derby database
      - Password to connect to the Apache Derby database
      - Port to connect to the Apache Derby database
      - Hostname of your system
      - Name of the database
      - Path to file aaDerbyAdaption.jar
      - Directory where the data will be exported
   c. Start the export script. You will be guided through the export process.
2. **From Administration Assistant function for Data Protection for *SAP*® v5.5 or higher:**
   a. To export data from a running Apache Derby database, first get information on how to connect to the database. These settings are provided in file assist.cfg.
   b. Change to the utils directory and start the export script by typing the following:
      - For Apache Derby:
        – On Windows systems:export.cmd
        – On UNIX/Linux systems:export.sh (or export.ksh)
      - For DB2 data server:

        On Windows systems:export.cmd <database> <user> <export directory>

        On UNIX/Linux systems:export.sh (or export.ksh) <database> <user> <export directory>

   As a result, the export directory contains several *.aa files.

   During the installation process, you will be asked if you want to import old data. Within this dialog you can enter the export directory you selected during the export.

Migrating Styles and Report Templates

Information on using existing styles and templates from a previous version of the product.

If you would like to reuse your styles and reports, save these directories from the installation directory to another directory.

Note: During the installation of the Administration Assistant function for Data Protection for *SAP®*, all data in the installation directory will be removed.

After the installation process, you can copy these directories back to the installation directory of the Administration Assistant.

Chapter 5. Configuring Data Protection for *SAP®* for Oracle

Instructions about how to configure Data Protection for *SAP®* for Oracle are provided.

Data Protection for *SAP®* for Oracle requires certain configuration tasks to be performed for these applications:

- Data Protection for SAP base product
- Administration Assistant
- Oracle RMAN and related files
- HACMP
- Distributed File System
- Tivoli Storage Manager backup-archive client
- Tivoli Storage Manager server

Configuration tasks for the Data Protection for *SAP®* for Oracle base product

Instructions about how to configure the Data Protection for *SAP®* for Oracle base product are provided.

Data Protection for *SAP®* for Oracle requires certain configuration tasks to be performed before performing a back up operation.

Verification tasks

Data Protection for *SAP®* for Oracle requires these verification tasks to be performed as part of the product configuration.

Verify the installation

Preparing for the Verification for Initial and Upgrade Installations: Make sure the following considerations are met before verifying the Data Protection for *SAP®* for Oracle installation:

- The SAP® Backup profile is configured properly. This profile can be found on UNIX or Linux systems in the path `$ORACLE_HOME/dbs` and on Windows systems in the path `%ORACLE_HOME%\database`. This configuration refers to the following keywords within that profile:

  `backup_type`
  Identifies the default type of the database backup. This parameter is only used by BRBACKUP (default is `offline`).

  `backup_dev_type`
  Determines the backup medium that will be used (default is tape). In order to use the backint interface, this parameter must be set either to 'util_file' or 'util_file_online'. For RMAN, this parameter is set to 'rman_util'

  `util_par_file`
  This parameter specifies the location of the parameter file. This file is required in order to perform a backup operation with an external backup program.

rman_parms
When backup_dev_type is set to "rman_util", this parameter defines various parameters required for RMAN operations.

Available values for the backup_dev_type and backup_type keywords.

Table 6. SAP Backup Profile Parameter Combinations

Operation	backup_dev_type	backup_type
Offline backup	util_file	offline
Online backup	util_file	online
Online backup with individual tablespace locking	util_file_online	online
Online backup via RMAN	rman_util	online

The SAP Backup profile parameter must be set or changed as follows in order to perform online backups with individual tablespace that lock with Data Protection for SAP:

```
backup_type      = online
backup_dev_type  = util_file_online
util_par_file    = <ORACLE_HOME>/dbs/init<SID>.utl
```

Performing the Verification for Initial and Upgrade Installations: Perform a tablespace backup using BR*Tools and then start a full online or offline backup using BRBACKUP:

```
brbackup -c -t online
brbackup -c -t offline
```

A complete restore or recovery of the entire SAP database is also recommended (using BR*Tools). However, a complete offline backup (using BRBACKUP) should be performed first. Step by step scenarios for backup and restore/recovery procedures of an SAP Oracle database using Data Protection for SAP can be found in the IBM Redbooks publication *R/3 Data Management Techniques Using Tivoli Storage Manager, SG24–5743*. IBM Redbooks can be found at http://www.redbooks.ibm.com. For backup tests, the BR*Tools utilities BRBACKUP and BRARCHIVE should be used. For restore or recovery test, only BRRECOVER should be used.

Verify the RMAN Setup on UNIX and Linux

In the following description you have to replace the directory name ora<bit> in the installation path. Depending on the version of Data Protection for *SAP*® for Oracle you have installed, you must replace it with ora64 for the 64–bit version of Data Protection for SAP.

Perform these tasks verify that RMAN is set up correctly on the UNIX or Linux system:

1. Make sure that Oracle is linked to the correct library: /usr/lib/libobk.*<ext>* / usr/tivoli/tsm/tdp_r3/ora<bit>/libtdp_r3.*<ext>* This link is not required in a distributed file system. See "Setting up Data Protection for *SAP*® for Oracle with RMAN in a Distributed File System in an Adaptive Computing Environment" on page 51.

2. Remove the library specified in /$ORACLE_HOME/rdbms/lib/libobk.<*ext*>. If running a 64–bit Oracle 8.x database system, also check in /$ORACLE_HOME/rdbms/lib64/.
3. The shared library must have the same bit level as the installed Oracle Server. For example, Oracle server 64-bit running on AIX 5.2 64-bit requires Data Protection for SAP 64-bit.
4. Examine the sbtio.log located in the directory specified in the user_dump_dest keyword within the Oracle profile init<SID>.ora. This file is usually located at oracle/SID/saptrace/usertrace/sbtio.log.
5. Check the log file sbtio.log for lines starting with BKI. The first message for each RMAN session is:BKI7060I: Data Protection for SAP<version and build number> session: process ID If you cannot find any such message in the file, the library is not correctly linked with Oracle.
6. Examine the dsierror.log located in the directory specified with the environment variable DSMI_LOG or in the file denoted by keyword ERRORlogname in the first stanza of file dsm.sys.
7. To get a Tivoli Storage Manager API trace file, set the following entries in the client system options file dsm.sys: tracefile /<path>/<trace file> traceflags api api_detail config policy The additional soft link might help: ln -s /usr/tivoli/tsm/tdp_r3/ora<bit>/libtdp_r3.<*ext*> /usr/lib/ libtdp_r3.<*ext*>.1

See "RMAN problem resolution" on page 113 if problems or errors were encountered.

Verify the RMAN Setup on Windows

Perform these tasks to verify that the RMAN interface is setup correctly:

1. After an operation using RMAN, examine the sbtio.log located in the directory specified in the user_dump_dest keyword within the Oracle profile init<SID>.ora.. If the sbtio.log file does not exist or there is no line that begins with the letters 'BKI' within an existing sbtio.log, perform these tasks:
   a. Check if the shared library file orasbt.dll was found and loaded by Oracle.
   b. Put the shared library file orasbt.dll into the directory %ORACLE_HOME%\bin. This is the directory where oracle.exe resides.
   c. Stop the service OracleService<SID> and restart it.
2. Examine the dsierror.log located in the directory specified with the environment variable DSMI_LOG.
3. To create a Tivoli Storage Manager API trace file, set the following entries in the client options file: tracefile <drive>:\<path>\<trace file> traceflags api

See "RMAN problem resolution" on page 113 for additional assistance.

Profile tasks

Data Protection for *SAP*® for Oracle requires these tasks to be performed in the Data Protection for SAP profile as part of the product configuration.

Set the SERVER statement in the Data Protection for *SAP*® for Oracle profile

The SERVER statement is specified in the Data Protection for *SAP*® for Oracle profile and there are corresponding keywords in the Tivoli Storage Manager client option file. Depending on the choice of password handling, some parameters are ignored. The corresponding sections in the Data Protection for SAP profile and the Tivoli Storage Manager client option file are established using the logical server name. This logical server name is defined by the keywords SERVER or SERVERNAME. The logical server names are also used by the "View TSM Server Utilization" function of the Administration Assistant. This function generates a separate entry for each logical server name found in the system landscape. Identical logical server names are considered to represent the same server.

Table 7. SERVER Statement and Appropriate Profile and Option File Settings.

Configuration possibilities	**Data Protection for SAP profile init<SID>.utl**	**Tivoli Storage Manager client option file dsm.sys or <server>.opt** [2]
single path; no password or manual password	SERVER <server> ADSMNODE <node>[1]	SERVERNAME <server> TCPSERVERADDRESS <address> NODENAME must not be specified
single path; automatic password by Tivoli Storage Manager	SERVER <server> ADSMNODE must not be specified	SERVERNAME <server> NODENAME <node> TCPSERVERADDRESS <address>
several paths/servers; no password or manual password	SERVER <server 1> ADSMNODE <node 1> • • • SERVER <server n> ADSMNODE <node n>	SERVERNAME <server 1> NODENAME must not be specified TCPSERVERADDRESS <address 1> • • • SERVERNAME <server n> NODENAME must not be specified TCPSERVERADDRESS <address n>
several paths/servers; automatic password by Tivoli Storage Manager[3]	SERVER <server 1> ADSMNODE must not be specified • • • SERVER <server n> ADSMNODE must not be specified	SERVERNAME <server 1> NODENAME <node 1> TCPSERVERADDRESS <address 1> • • • SERVERNAME <server n> NODENAME <node n> TCPSERVERADDRESS <address n>
several paths/servers; automatic password by Tivoli Storage Manager with Tivoli Storage Manager API 5.2 (or later) [4]	SERVER <server> ADSMNODE must not be specified TCP_ADDRESS <address 1> • • • SERVER <server n> ADSMNODE must not be specified TCP_ADDRESS <address n>	SERVERNAME <server NODENAME <node> TCPSERVERADDRESS <address>

Notes:

[1] If ADSMNODE is not specified, the host name is used.

[2] On UNIX and Linux, `dsm.sys` is the single client option file for all Tivoli Storage Manager servers. On Windows, there is a separate client option file `<server>.opt` for each Tivoli Storage Manager server.

[3] If two different physical machines have the same Tivoli Storage Manager node name or if multiple paths are defined on one node using several server stanzas, `passwordaccess generate` may only work for the first stanza that is used after password expiration. During the first client-server contact, the user is prompted for the same password for each server stanza separately, and a copy of the password is stored for each stanza. When the password expires, a new password is generated for the stanza that connects the first client-server contact. All subsequent attempts to connect through other server stanzas fail because there is no logical link between their copies of the old password and the updated copy generated by the first stanza used after password expiration. To avoid this situation, update the passwords before they expire. When the passwords have already expired, perform these tasks to update the password:

1. Run dsmadmc and update the password on the server.
2. Run `dsmc -servername=stanza1` and use the new password to generate a proper entry.
3. Run `dsmc -servername=stanza2` and use the new password to generate the proper entry.

[4] If you are using Tivoli Storage Manager API 5.2 (or later), you can use the TCP_ADDRESS parameter in the Data Protection for SAP profile. This parameter eliminates the need to set multiple stanzas in the Tivoli Storage Manager client option file for multiple paths and eliminates the problem when updating the password (see [3]).

Example of SERVER statement with alternate paths:

This example assumes that the Tivoli Storage Manager server is configured with two tape drives and two LAN connections. A backup is typically performed through network path 1 (SERVER statement 1). If network path 1 is unavailable, the backup is performed using network path 2 (SERVER statement 2). If path 1 is active, Data Protection for *SAP*® for Oracle begins the two sessions as defined in the SERVER statement for path 1. Since MAX_SESSIONS also specifies 2, no more sessions are started. If path 1 is inactive, Data Protection for SAP starts 2 sessions on path 2. Since MAX_SESSIONS specifies 2, the backup is performed using path 2.

This is an example of the Data Protection for SAP profile used in this alternate path configuration:

```
MAX_SESSIONS     2        # 2 tape drives
.
.
SERVER     server_a      # via network path 1
  ADSMNODE          C21
  SESSIONS          2
  PASSWORDREQUIRED  YES
  BRBACKUPMGTCLASS  mdb
  BRARCHIVEMGTCLASS mlog1 mlog2
# USE_AT            0 1 2 3 4 5 6

SERVER     server_b      # via network path 2
  ADSMNODE          C21
  SESSIONS          2
  PASSWORDREQUIRED  YES
  BRBACKUPMGTCLASS  mdb
  BRARCHIVEMGTCLASS mlog1 mlog2
# USE_AT            0 1 2 3 4 5 6
```

Note that even if the logical names server_a and server_b actually point to the same Tivoli Storage Manager server, the Administration Assistant still considers them to be two different servers.

Example of SERVER statement with parallel servers:

This example assumes the following configuration:

- Two Tivoli Storage Manager servers (each with two tape drives) with connections through two network paths:
  - server_a uses TCP/IP address xxx.xxx.xxx.xxx
  - server_b uses TCP/IP address yyy.yyy.yyy.yyy
- An SAP® database server connected to two networks.
- Daily backups are performed on both systems.

This is an example of the Data Protection for *SAP*® for Oracle profile used in this parallel configuration:

```
MAX_SESSIONS     4        # 4 tape drives
.
.
SERVER     server_a      # via network path 1
  ADSMNODE          C21
  SESSIONS          2
  PASSWORDREQUIRED  YES
  BRBACKUPMGTCLASS  MDB
  BRARCHIVEMGTCLASS MLOG1 MLOG2 MLOG3 MLOG4
# USE_AT            1 2 3 4 5 6 7


SERVER     server_b      # via network path 2  ADSMNODE          C21
  SESSIONS          2
  PASSWORDREQUIRED  YES
  BRBACKUPMGTCLASS  MDB
  BRARCHIVEMGTCLASS MLOG1 MLOG2 MLOG3 MLOG4
# USE_AT            1 2 3 4 5 6 7
```

Example of SERVER statement with alternate servers:

This example assumes the following configuration:

- Two Tivoli Storage Manager servers:
  - server_a uses TCP/IP address xxx.xxx.xxx.xxx and uses four tape drives (MAX_SESSIONS 4)
  - server_b uses TCP/IP address yyy.yyy.yyy.yyy and uses four tape drives (MAX_SESSIONS 4)
- An SAP® database server connected to this FDDI network.
- Normal backups are performed with server a, which is local to the SAP database server.
- A disaster recovery backup is stored on remote server b every Friday.

This is an example of the Data Protection for *SAP*® for Oracle profile used in this disaster recovery configuration:

```
MAX_SESSIONS     4        # 4 tape drives
.
.
SERVER     server_a      # via network path 1
  ADSMNODE          C21
  SESSIONS          4
  PASSWORDREQUIRED  YES
  BRBACKUPMGTCLASS  MDB
  BRARCHIVEMGTCLASS MLOG1 MLOG2 MLOG3 MLOG4
  USE_AT            1 2 3 4


SERVER     server_b      # via network path 2
  ADSMNODE          C21
  SESSIONS          4
  PASSWORDREQUIRED  YES
  BRBACKUPMGTCLASS  MDB
  BRARCHIVEMGTCLASS MLOG1 MLOG2 MLOG3 MLOG4
  USE_AT            5    # for Disaster Recovery
```

Administration Assistant function for Data Protection for *SAP*® tasks

Data Protection for *SAP*® for Oracle requires these Administration Assistant function for Data Protection for *SAP*® tasks to be performed as part of the product configuration.

1. Prepare a secure connection

By default, the Administration Assistant function for Data Protection for *SAP*® is set up to accept unsecure (HTTP) client requests. If the Administration Assistant was set up for secure (HTTPS) connection during installation, then proceed to the next step.

The secure communication between the Administration Assistant Server component and its clients is realized with the Secure Socket Layer (SSL) protocol. This protocol requires that both the server and client be integrated in a public key infrastructure (PKI). The Server component requires these settings:

- An HTTPS port to listen on for HTTPS connect requests.
- A keystore containing a key pair it uses to identify itself to the clients and when connecting internally to the RMI registry. The server hostname is used as an

alias for this key pair. Since the keystore contains the server private key, precautions must be taken that prevent access by unauthorized persons.

- A truststore containing trusted certificates that allow verifying the server's signature. If the server certificate was digitally signed by an official certificate authority whose root certificate is available in the truststore by default, there is nothing to be done. If however, the server identifies itself with a self-signed certificate, this certificate must be imported into the truststore as well.
- Be sure to remove this trusted certificate from the truststore as soon as the officially signed server certificate is available and employed. A setup using self-signed certificates is not recommended for production environments.
- Both the keystore and truststore can be modified with your keystore management tool. This tool varies by platform and provider.

Perform these tasks to set up the Administration Assistant Server component for secure communication:

1. Remove the keyword nonsecure from the Server configuration file (assist.cfg).
2. Specify the appropriate HTTPS port number in the Server configuration file:

   ```
   httpsport=<https port number>
   ```

   The default HTTPS port number is 443.
3. Add the keystore, keystore password, and truststore to the appropriate Java call. The Java calls are shown in **bold** text:

   ```
   -Djavax.net.ssl.keyStore=<keystore>
   -Djavax.net.ssl.keyStorePassword=<password for keystore>
   -Djavax.net.ssl.trustStore=<truststore>
   ```

   - (UNIX and Linux): add the parameters to `sadma.sh`
   - (Windows): add the parameters to `sadmt.cmd` and to the registry. The Windows registry key is:

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\...
     ...AdminAssistant\Parameters\AppParameters
     ```

   If you do not specify one or more of these parameters, the defaults of your Java virtual machine will be used.
4. Make sure the required certificates are contained in the keystore and trust store.
5. Restart the Administration Assistant Server component.

When changing the Administration Assistant server from nonsecure to secure mode using a self-signed certificate, remember to also prepare the Administration Assistant clients as described in "2. Configure the Administration Assistant function for Data Protection for *SAP*® Client" on page 47 and "4. Configure a scheduling client to create reports" on page 48.

2. Configure the Administration Assistant function for Data Protection for *SAP®* Client

The Administration Assistant function for Data Protection for *SAP®* client invokes a Java applet when connecting to the Administration Assistant function for Data Protection for *SAP®* Server component. Make sure these requirements are met when setting up the Administration Assistant client:

- Make sure all Administration Assistant Client prerequisites are met as described in "Prerequisites for Installing the Administration Assistant function for Data Protection for *SAP®*" on page 31.
- The browser must be enabled to accept cookies.
- Advertisements and pop-up panels must not be blocked unless `index.html` is used in the address.
- A secure connection requires that the client Java plugin must be able to verify the certificate presented by the Administration Assistant Server component. In a production environment, this is typically performed at the server level as the server certificate is signed by an official certificate authority whose root certificate is contained in the plugin truststore. If the server identifies itself with a self-signed certificate, this certificate must be imported into the plugin truststore. If you did not use the using the Java Plugin Control Panel to replace the plugin truststore, the file `cacerts` (located in the Java security path) is used as the truststore. The file is modified with the keystore management tool. This tool varies by platform and provider. For example, the Sun Microsystems **keytool** is modified with this command:

```
keytool -import -alias <Server component hostname> -file <cert_file>
-keystore <trustore>
```

- Be sure to remove the self-signed trusted certificate from the truststore as soon as the officially signed server certificate is available and activated. A setup with self-signed certificates is not recommended for production environments.

3. Verify the Administration Assistant function for Data Protection for *SAP®* installation

Perform this task to verify the installation of the Administration Assistant function for Data Protection for *SAP®*. Make sure to use the ADMIN userid (with password 'admin') for the initial login:

- (Nonsecure connection): If the Server component was started with the keyword nonsecure in the Server configuration file, connect to the Administration Assistant Server component from a client machine with this command:

```
http://<Server component host name>:<http port>
```

  Optionally, you can make the connection without opening a new browser window by issuing this command:

```
http://<Server component host name>:<http port>/index.html
```

- (Secure connection): If the Server component was started with the keyword secure in the Server configuration file, connect to the Administration Assistant Server component from a client machine with this command:

```
https://<Server component host name>:<https port>
```

Optionally, you can make the connection without opening a new browser window by issuing this command:

```
https://<Server component host name>:<https port>/index.html
```

Use the client function *Administer Users* to change the default password immediately after establishing a connection. As soon as an instance of Data Protection for *SAP*® for Oracle connects to your Administration Assistant Server component, the instance will be displayed in the list of Data Protection for SAP servers. For details on how to set up your instance of Data Protection for SAP to connect to a specific Server component, refer to "Specifying a new Administration Assistant function for Data Protection for *SAP*®" on page 75.

4. Configure a scheduling client to create reports

A scheduling client server must be set up in order to create reports with templates. Perform these tasks to set up a scheduling client server:

1. Select a system that meets the requirements as described in "Prerequisites for Installing the Administration Assistant function for Data Protection for *SAP*®" on page 31.
2. Copy files `Admt.jar` and `NLS.jar` from the installation directory of the Administration Assistant Server component to the scheduling client system. Before generating a report, make sure that these files are specified in the CLASSPATH and that the JVM is included in the PATH. See "Sample Shell Script for Scheduling a Report from a UNIX Scheduling Client" on page 142 or "Sample Command File for Scheduling a Report from a Windows Scheduling Client" on page 143for a sample script.
3. In case the Administration Assistant Server component is started in secure mode, set up a public key infrastructure between the scheduling client and the Server component. In a production environment, this is typically performed at the server level as the server certificate is signed by an official certificate authority whose root certificate is contained in the plugin truststore. If the server identifies itself with a self-signed certificate, this certificate must be imported into the plugin truststore. If you did not use the Java Plugin Control Panel to replace the plugin truststore, the file `cacerts` (located in the Java security path) is used as the truststore. The file is modified with the keystore management tool. This tool varies by platform and provider. For example, the Sun Microsystems **keytool** is modified with this command: `keytool -import -alias <Server component hostname> -file <cert_file> -keystore <trustore>`

Defining thresholds

You can define limits (or thresholds) for various states pertaining to the Administration Assistant function for Data Protection for *SAP*® environment. The threshold status is shown in the ″Monitor Backup States″ and ″Backup State - Detailed View″ panels. These are predefined threshold types:

- Backup duration (in minutes or hours)
- Backup size (in MB or GB)
- Throughput rate (in GB per hour or MB per second)
- Time since the last complete backup (in hours or days)
- Size of all log file backups since the last complete backup (in MB or GB)
- Recovery point objective (maximum time permitted since the last backup, in minutes or hours)

When a threshold is exceeded, this is reported in the ″Threshold Status″ column of the ″Monitor Backup States″ panel, and an e-mail describing the exception in more detail is sent to any e-mail addresses defined for the threshold. A *lifetime* parameter associated with each threshold defines the length of time between e-mail notifications, provided the threshold remains in alert status. The Administration Assistant Online Help provides information about threshold definitions.

Distributed file system tasks

Data Protection for *SAP*® for Oracle requires these tasks to be performed to configure Data Protection for SAP in a distributed file system.

Configuring Data Protection for *SAP*® for Oracle in a Distributed File System

This set up task is not required if the following conditions exist:

- All SAP® systems to are statically assigned to specific hosts. For example, the instances are not moved between hosts.
- The root user is granted read/write access permission to the distributed file system.

If these conditions exist, the standard installation process can be used as described in “Required installation tasks” on page 23.

For a single SID located on a host, Data Protection for SAP sets the ProLE service to run with the ora<SID> user ID instead of root. Perform these tasks to set up the ProLE service to run with the ora<SID> user ID:

1. Enable root access to the distributed file system.
2. Install Data Protection for SAP using the procedure described in “Required installation tasks” on page 23.
3. Replace the following entry in the `/etc/inittab` file:

   ```
   po64:345:respawn:/usr/tivoli/tsm/tdp_r3/ora64/prole -p <profile>
   ```

   with this entry:

   ```
   po64:345:respawn:su - ora<SID> -c /usr/tivoli/tsm/tdp_r3/ora64/prole -p <profile>
   ```

   <SID> must be the actual SID.
4. Issue the following command:

   ```
   init q
   ```

5. Disable root access to the distributed file system.

For multiple SIDs on a host system, run the ProLE service by root with permanent read/write permission to the distributed file system.

Configuring Data Protection for *SAP®* for Oracle in a Distributed File System in an Adaptive Computing Environment

Certain setup tasks must be performed when Data Protection for *SAP®* for Oracle is used in an Adaptive Computing Environment. Since the Adaptive Computing Environment currently does not allow more than one SID per host, the root user does not require additional permissions for the distributed file system. Perform these tasks to prepare installation in the distributed file system:

1. Log in as root user and perform a regular installation of Data Protection for SAP on one of the systems participating in the distributed file system. During the installation procedure, make sure the configuration files and links to the Data Protection for SAP executables reside in a directory that is not located in the distributed file system. These files will not be used and can be deleted after installation.
2. After installation completes successfully, copy the contents of the installation directory to a temporary directory in the distributed file system. For example:

   ```
   mkdir /san/SanFS/tivoli/tdp_r3
   cp -r /usr/tivoli/tsm/tdp_r3/ora64 /san/SanFS/tivoli/tdp_r3
   ```

3. Each of the SAP® environments can now be set up to use Data Protection for SAP for backup and recovery. In the Adaptive Computing Environment, Data Protection for SAP backup and recovery tasks can be performed from the same host for all participating SIDs. For each SID, log in as the database instance owner and run the `'SanFSsetupSID.sh'` script from the installation path in the distributed file system. For example:

   ```
   /san/sanFS/tivoli/tdp_r3/ora64/SanFSsetupSID.sh
   ```

   The following information must be provided to the script:

   a. The SID for the SAP system to be backed up.
   b. If the Data Protection for SAP executable files reside in a location other than the default directory, specify that path when running the script.
   c. The path for the Data Protection for SAP profile and configuration file (`init<SID>.utl`, `init<SID>.bki`).
   d. To connect to an Administration Assistant server, specify the hostname or IP address and server port for the Administration Assistant server.
4. The script `SanFSsetupSID.sh` creates scripts `prepareTDPSAP_<SID>.sh`. On each host, log in as root user and run the `prepareTDPSAP_<SID>.sh` script with the appropriate <SID>. If this script is placed in the distributed file system, make sure the root users have the appropriate permissions to run it.
5. Whenever a SID is moved to a different host, the `'prepareTDPSAP_<SID>.sh'` script must be run by the root user of the new host.

Setting up Data Protection for *SAP®* for Oracle with RMAN in a Distributed File System in an Adaptive Computing Environment

The `SanFSsetupSID.sh` script does not create the link `/usr/lib/libobk.a` to the Data Protection for *SAP®* for Oracle shared library. Therefore, when configuring Oracle to use the Data Protection for SAP shared library (as described in "Verify the RMAN Setup on UNIX and Linux" on page 40), specify the full path and name of the library located in the directory residing in the distributed file system. Add this directory to the library path environment of the database instance owner. Do not link Oracle with the library in `/usr/lib`. This prevents the database from failing to start if the instance is moved to a different host.

HACMP tasks

Data Protection for *SAP®* for Oracle requires these tasks to be performed to use Data Protection for SAP in a High Availability Cluster Multi-Processing environment.

Configuring Data Protection for *SAP®* for Oracle as an HACMP Application

A prerequisite for installation is a correct setup of the Tivoli Storage Manager client. The installation steps for the Tivoli Storage Manager Backup/Archive Client for AIX can be found in the documentation *Tivoli Storage Manager Installing the Clients*.

Data Protection for *SAP®* for Oracle must be defined as an application to HACMP. Although the *HACMP for AIX Installation Guide*should be reviewed for detailed directions, a high-level summary is provided here. Note that Data Protection for SAP must be in a resource group having a cascading or rotating takeover relationship. It does not support a concurrent access resource group. Perform these tasks to configure Data Protection for SAP an application for HACMP:

1. Enter this command start HACMP for AIX system management:

   ```
   smit hacmp
   ```

2. Select Cluster Configuration > Cluster Resources > Define Application Servers > Add an Application Server.
3. Enter field values as follows:

   Server Name
   Enter an ASCII text string that identifies the server (for example, tdpclientgrpA). You use this name to refer to the application server when you define it as a resource during node configuration. The server name can include alphabetic and numeric characters and underscores. Do not use more than 31 characters.

   Start Script
   Enter the full pathname of the script that starts the server (for example, /usr/sbin/cluster/events/utils/start_tdpr3.sh). This script is called by the cluster event scripts. This script must be in the same location on each cluster node that might start the server.

   Stop Script
   Enter the full pathname of the script that stops the server (for example, /usr/sbin/cluster/events/utils/stop_tdpr3.sh). This script is called by the cluster event scripts. This script must be in the same location on each cluster node that might stop the server.
4. Press Enter to add this information to the HACMP for AIX ODM.

5. Press F10 after the command completes to leave SMIT and return to the command line.

Refer also to the *HACMP for AIX Planning Guide V4.4* for further information about selecting the HACMP node topology and takeover relationships.

Adding Data Protection for *SAP*® for Oracle to an HACMP Resource Group:

A final step in enabling Data Protection for *SAP*® for Oracle for HACMP failover is to define it to a cluster resource group. Although the *HACMP for AIX Installation Guide*should be reviewed for detailed directions, a high-level summary is provided here. Perform these tasks to define the resources that will be part of a resource group:

1. From the Cluster Resources SMIT screen, select the Change/Show Resources/Attributes for a Resource Group option and press Enter. SMIT displays a picklist of defined resource groups.
2. Pick the desired resource group.
3. Press Enter and SMIT displays the Configure a Resource Group screen.
4. Enter values that define all the resources you want to add to this resource group.
5. After entering field values, synchronize cluster resources.
6. Press F10 to exit SMIT or F3 to return to previous SMIT screens to perform other configuration tasks or synchronize the changes you just made. To synchronize the cluster definition, go to the Cluster Resources SMIT screen and select the Synchronize Cluster Resources option.

The Tivoli Storage Manager client application should be added to the same resource group that contains the file systems it will back up. The file systems defined in the resource group should also be the ones specified in the domain for this client instance in the client user options file. Note that both JFS and NFS file systems can be defined as cluster resources, although NFS supports only 2 node clusters in a cascading takeover relationship.

HACMP stop script example:

This section illustrates a stop script in an HACMP environment.

Depending on the installation environment, the sample stop script may need to ensure that any backup or restore operation in progress can be stopped. This means that any processes launched by brbackup or brarchive for this client instance (that may be accessing the shared file system) must also be stopped to free resources. This may have already been accomplished by the HACMP script that stops the SAP® systems. It may also not be desirable in certain installations and should be revised.

The stop script is used in the following situations:

- HACMP is stopped.
- A failover occurs due to a failure of one component of the resource groups. The other members are stopped so that the entire group can be restarted on the target node in the failover.
- A fallback occurs and the resource group is stopped on the node currently hosting it to allow transfer back to the node re-entering the cluster.

The stop script will be called by HACMP as the root user.

Note: This script is not in its final form. It should be considered pseudo code that indicates the functions it will perform.

```
#!/bin/ksh
# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #
#    This sample script is provided for use with                                        #
Data Protection for SAP in an HACMP     #
#    environment                                                                        #
#    It should be reviewed and customized to meet your specific environment             #
#                                                                                       #
#                                                                                       #
#    Name: stop_tdpr3.sh                                                                #
#                                                                                       #
#    Function: A sample shell script to update the disk information      #
after the SAP instance is unmounted.                                                   #
#                                                                                       #
# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #

if ["$VERBOSE_LOGGING"="high"]
then
    set -x
fi


# Function to update all disk information for Data Protection for SAP
STOP_PROCESSING()

{
# You may want to cancel all backups currently running
# Note that this will generate errors in the current backup logs and it will also
# cancel the connection to the Admin Assistant.
# *** Note that if you are using Data Protecion for Snapshot Devices for SAP,
# this may leave your FlashCopy device  in an
# inconsistent state.
# kill –9 `cat /var/tdp_r3/prole.pid`


# This stops any running backup or archive process.
STOP_PROCESSING


Exit 0
```

Configuration tasks for Tivoli Storage Manager

Instructions about how to configure the Tivoli Storage manager client and server for Data Protection for *SAP*® for Oracle operation are provided.

Data Protection for *SAP*® for Oracle requires certain configuration tasks to be performed for the Tivoli Storage Manager backup-archive client and server.

Tivoli Storage Manager client tasks

Data Protection for *SAP*® for Oracle requires these tasks to be performed for the Tivoli Storage Manager client as part of the product configuration.

Configure the Tivoli Storage Manager client options

The Tivoli Storage Manager clients must be configured after the Tivoli Storage Manager server is configured. These clients include the *backup-archive client* for the file system backups and the *Application Programming Interface (API) client* for interface programs. The API client allows users to enhance existing applications with backup, archive, restore, and retrieve services. An installed and confirmed API client is a prerequisite for Data Protection for *SAP*® for Oracle.

The clients must be installed on all nodes that will interface with the Tivoli Storage Manager server. In an SAP® system landscape, this means that the backup/archive client must be installed on every machine scheduled for a file system backup, such as SAP application servers and the SAP database server. The Tivoli Storage Manager API client only needs to be installed on the SAP database server machine to enable backup and restore operations of the SAP database using Data Protection for SAP. The Administration Assistant uses the logical Tivoli Storage Manager server names in its ″View TSM Server Utilization″ function. Identical logical names are considered to represent the same Tivoli Storage Manager server, but different entries are generated for each logical server name found in the system landscape. Therefore, use identical logical server names when pointing to the same Tivoli Storage Manager server throughout the system landscape and use different logical server names when different Tivoli Storage Manager servers are addressed.

Set Tivoli Storage Manager client options on UNIX or Linux:

Tivoli Storage Manager clients on UNIX or Linux are configured by setting options in the `dsm.opt` and `dsm.sys` files. The `include/exclude` file is also used to define which files are included or excluded during backup, archive, or hierarchical storage processing. Examples of an `include/exclude` file for UNIX or Linux can be found in “Include/Exclude List Sample (UNIX and Linux)” on page 144. Perform these tasks to configure the Tivoli Storage Manager backup/archive clients to operate in an SAP® environment:

1. Install the Tivoli Storage Manager client software on the SAP database server machine.
2. Edit the client system options file `dsm.sys` and set these values as appropriate for your installation:

```
Servername        server_a
TCPPort           1500
TCPServeraddress  xxx.xxx.xxx.xxx or servername
InclExcl          /usr/tivoli/tsm/client/ba/bin/inclexcl.list
Compression       OFF
```

3. Specify `TCPServeraddress 127.0.0.1` or loopback if the server and client are on the same machine. This improves TCP/IP communication speed.
4. Specify `InclExcl` if you want Tivoli Storage Manager to include or exclude the files listed in `inclexcl.list`. This is optional. You may want to exclude all database files that are processed by the BR*Tools.
5. Throughput improves when tape drives attached to the Tivoli Storage Manager server provide hardware compression. However, combining hardware compression and Tivoli Storage Manager client software compression (`Compression ON`) is not recommended. It might be necessary to experiment with Tivoli Storage Manager client software compression settings to determine its impact in your environment. Tivoli Storage Manager client software compression generally improves performance only when network throughput is low.

6. Edit the client user options file `dsm.opt` and set these values as appropriate for your installation:

```
LANGUAGE     AMENG   (this is the default value)
NUMBERFormat 1       (this is the default value)
TAPEPROMPT   NO
TIMEFORMAT   1       (this is the default value)
```

When the Tivoli Storage Manager API client is installed on a UNIX or Linux system, make sure there is a softlink `/usr/lib/libApiDS.<ext>` that points to the `libApiDS.<ext>` file in the Tivoli Storage Manager API installation directory (`/usr/tivoli/tsm/client/api/bin`). See "Required installation tasks" on page 23 for a detailed description of the meaning of the <*ext*>.

TSM provides two features that allow specifying the location of the TSM API Client error log: the environment variable DSMI_LOG and the TSM system client option ERRORLOGName in dsm.sys. DSMI_LOG specifies a directory to which a file named dsierror.log will be written, while ERRORLOGName sets a path and user-defined file name.

In order to achieve conclusive logical linking of the environment, configuration and log files in your SAP backup/archive system, we recommend using the TSM system client option ERRORLOGName rather than the environment variable DSMI_LOG. The main advantages are:

- As opposed to DSMI_LOG, ERRORLOGName allows including the SID in the file name. This can speed up problem determination by simplifying identification of the correct error log file and matching its name with the active user client options file name, which should also contain the SID and be stored in environment variable DSMI_CONFIG. This is especially useful on machines with several SIDs.
- The suggested configuration prepares the system for TSM API Client tracing for both backint and RMAN operation. For more information, see "Verify the RMAN Setup on UNIX and Linux" on page 40.

The following is the suggested setup for Data Protection for SAP for Oracle 64-bit on AIX:

1. For each "SERVER <servername>" section in the profile init<SID>.utl, create a corresponding "SErvername <servername>" stanza in the system client options file /usr/tivoli/tsm/client/api/bin64/dsm.sys, where <SID> designates the Oracle System ID as returned by "echo $ORACLE_SID". One SID may use several "SErvername <servername>" stanzas, but we do not recommend the use of a "SErvername <servername" stanza by several SIDs.
2. In all "SErvername <servername>" stanzas belonging to the same SID, add option "ERRORLOGName /<writeable_path>/dsierror_<SID>.log". Write permission problems can usually be avoided by specifying a directory below $ORACLE_HOME as <writeable_path>.
3. Create one user options file for each Oracle SID with the filename /usr/tivoli/tsm/client/api/bin64/dsm_<SID>.opt containing option "SErvername <servername>". <servername> should point to the stanza in /usr/tivoli/tsm/client/api/bin64/dsm.sys that is designated by the first "SERVER <servername>" section in init<SID>.utl. Add variable DSMI_CONFIG=/usr/tivoli/tsm/client/api/bin64/dsm_<SID>.opt to the environment of the user who is running the SAP backups, usually ora<SID> or <SID>adm, or both in case of doubt.

4. Add variable DSMI_CONFIG=/usr/tivoli/tsm/client/api/bin64/dsm_<SID>.opt to the rman_parms option in init<SID>.sap. The following should appear on one line:

```
rman_parms="ENV=(XINT_PROFILE=<path>/init<SID>.utl, PROLE_PORT=<portnumber>,
           &BR_INFO, DSMI_CONFIG=/usr/tivoli/tsm/client/api/bin64/dsm_<SID>.opt)"
```

With this recommended setup, you obtain the following logical interlinking:

- environment variable DSMI_CONFIG is exported from the login shell as well as from rman_parms in init<SID*!ENT!*.sap
- environment variable DSMI_CONFIG points to client user options file /usr/tivoli/tsm/client/api/bin64/dsm_<SID*!ENT!*.opt
- client user option ″SERVER <servername*!ENT!*″ in dsm_<SID*!ENT!*.opt points to the ″SERVER <servername*!ENT!*″ stanza in /usr/tivoli/tsm/client/api/bin64/dsm.sys
- the ″SERVER <servername*!ENT!*″ stanza contains the option ″ERRORLOGName /<writeable_path*!ENT!*/dsierror_<SID*!ENT!*.log″

If the variable DSMI_LOG already exists in your environment from an earlier setup, its will be overridden by dsm.sys option ERRORLOGName as configured above. However, in order to avoid confusion, make sure the DSMI_LOG path is identical to the path in ERRORLOGName. Alternatively, you can remove DSMI_LOG completely from your environment.

Set Tivoli Storage Manager client options on Windows:

Tivoli Storage Manager clients on Windows are configured by setting options in the file `<server_a>.opt` (where `server_a` is the logical server name in the `initSID.utl` file). The `include/exclude` file is also used to define which files are included or excluded during backup, archive, or hierarchical storage processing. Examples of an `include/exclude` file for Windows can be found in “Include/Exclude List Sample (Windows)” on page 145. Perform these tasks to configure the Tivoli Storage Manager backup/archive clients to operate in an SAP® environment:

1. Install the Tivoli Storage Manager client software on the SAP database server machine.
2. For each logical Tivoli Storage Manager server, a corresponding client option file is required. In this example, the file name must be `server_a.opt` since `server_a` is the logical server name:

```
TCPPort           1500
TCPServeraddress  xxx.xxx.xxx.xxx
InclExcl          c:\tivoli\tsm\baclient\inclexcl.list
Compression       OFF
```

   In addition, the environment variable `DSMI_CONFIG` must specify the corresponding client options file (for example `c:\tivoli\tsm\api\server_a.opt`).
3. Specify `TCPServeraddress 127.0.0.1` or loopback if the server and client are on the same machine. This improves TCP/IP communication speed.
4. Specify `InclExcl` if you want Tivoli Storage Manager to include or exclude the files listed in `inclexcl.list`. This is optional. You may want to exclude all database files that are processed by the BR*Tools.

5. Throughput improves when tape drives attached to the Tivoli Storage Manager server provide hardware compression. However, combining hardware compression and Tivoli Storage Manager client software compression (`Compression ON`) is not recommended. It might be necessary to experiment with Tivoli Storage Manager client software compression settings to determine its impact in your environment. Tivoli Storage Manager client software compression generally improves performance only when network throughput is low.

A Tivoli Storage Manager error log (required for each client) can be specified for each process regardless of the number of Tivoli Storage Manager client option files `<server>.opt` involved. The Tivoli Storage Manager error log is determined by these rules:

1. The Tivoli Storage Manager Client log is written to the file specified by the DSMI_LOG environment variable.
2. If the DSMI_LOG environment variable is absent or is not writeable, the Tivoli Storage Manager client log is written to the file specified with keyword `ERRORlogname` in the client system options file `dsm.opt`.
3. If there is no `ERRORlogname` in `dsm.opt` or if it is not writeable, the Tivoli Storage Manager client log is written to file `dsierror.log` in the local path.

It is recommended to set up the Tivoli Storage Manager client so that different processes write to separate error logs. Therefore, the error log path should be defined in the DSMI_LOG environment variable if the client options files are shared among processes.

Tivoli Storage Manager server tasks

Data Protection for *SAP*® for Oracle requires these tasks to be performed for the Tivoli Storage Manager server as part of the product configuration.

Configure the Tivoli Storage Manager server

Tasks required to set up the Tivoli Storage Manager server, general server configurations, and specific server configurations (such as setup of storage devices) are provided. Although the task examples use Tivoli Storage Manager commands, these tasks can also be performed using the Tivoli Storage Manager Web client GUI.

Consider these performance-related guidelines before installing the Tivoli Storage Manager server:

Tivoli Storage Manager server host machine
The Tivoli Storage Manager server should be installed on an exclusive machine. The tasks presented in this section avoid concurrent processes and disk I/O access with other applications. A single Tivoli Storage Manager server is sufficient for a single SAP® system landscape. If the Tivoli Storage Manager server will be used to back up and restore other clients, consider installing the server on a large machine or using several Tivoli Storage Manager servers.

Network topology
Network topologies such as Ethernet, Token Ring, FDDI, and Fast Ethernet work well with the Tivoli Storage Manager server. Fast network topology such as FDDI or Fast Ethernet should be used to prevent bottlenecks during backup and restore operations. The Tivoli Storage Manager server supports multiple network adapters. This support increases server

throughput by providing multiple connections to the same network or by providing several physically distinct networks for the same server.

RS/6000® SP™ environment.
An RS/6000 SP node can be used for a Tivoli Storage Manager server. The use of a High Performance Switch network can improve backup and performance.

These steps are considered complete once the Tivoli Storage Manager server is successfully installed:

- Recovery log volume has been allocated and initialized.
- Recovery log mirror volume has been allocated and initialized.
- Database volume has been allocated and initialized.
- Database mirror volume has been allocated and initialized.
- Additional labeled volumes for the backup and archive storage pools have been allocated and initialized (disks, tapes or combinations).
- Licenses have been registered.
- The Tivoli Storage Manager server has been started.

The latest code fixes for Tivoli Storage Manager can be found at:
`ftp://index.storsys.ibm.com/tivoli-storage-management/maintenance`

1. Specify a Tivoli Storage Manager server:

Perform these tasks to add a Tivoli Storage Manager server:

1. Add a new server statement to the Data Protection for *SAP*® for Oracle profile.
2. Adapt the Tivoli Storage Manager options files as described in "8. Verify the Tivoli Storage Manager server name" on page 65.
3. Set and save the Tivoli Storage Manager password for the new server as described in "Set the Tivoli Storage Manager password" on page 62.

2. Specify a storage device:

A storage device defines a device class which handles the type of media, such as tape libraries or jukeboxes. The default device class defined for disks is `DISK` and is considered sufficient. Verify that these items are established within the Tivoli Storage Manager server after installation:

- Query the defined library:

```
q library
```

- Query the defined drives:

```
q drive
```

- Query the defined device class:

```
q devclass
```

3. Define a storage pool:

A storage pool is a named collection of storage volumes that are associated with one device class. Each storage pool represents a collection of volumes that are the same media type. The storage pool setup defines the storage hierarchy for the appropriate environment. In an SAP® environment, these data types can be backed up:

- SAP system data
- SAP database data (data files, online and offline redo log, control files)

To separate this data within the Tivoli Storage Manager server, define appropriate storage pools for each of these data collections. Log on as the Tivoli Storage Manager Administrator using the *Admin Command Line* or the *Web Admin* and run these commands to define storage pools:

1. Define a storage pool for the SAP system data: `define stgpool sap_incr <device_class_name> maxscr=5`
2. Define a storage pool for the data files : `define stgpool sap_db <device_class_name> maxscr=20`
3. Define a storage pool for the first copy of offline redo log files : `define stgpool sap_log1 <device_class_name> maxscr=3`
4. It is strongly recommended that you back up the offline redo log files twice on two different Tivoli Storage Manager volumes. For this purpose, you have to define an additional storage pool for the second copy of offline redo log files: `define stgpool sap_log2 <device_class_name> maxscr=3`

When a library tape device is associated, the maximum number of *scratch volumes* (labeled volumes which are empty or contain no valid data) that this storage pool will be allowed to use (parameter `maxscr`) must be defined. The maximum number of scratch tapes depends on the size of the database, the capacity of the tapes, the number of scratch volumes available, and how many versions of the backup must be retained. Replace these values with appropriate estimates.

4. Define a policy:

Tivoli Storage Manager policies specify how files are backed up, archived, migrated from client node storage, and also how they are managed in server storage. A policy definition includes the definition of a *policy domain*, a *policy set*, *management classes*, and *copy groups*. After setting definitions, a default policy set must be assigned, validated, and activated. For the policy definition, log on as a Tivoli Storage Manager Administrator using the *Admin Command Line* or the *Web Admin* and run these commands:

1. Define a policy domain and policy set:

```
define domain sap_c21
define policyset sap_c21 p_c21
```

2. Define a management class for file system backups, data files, offline redo logs and copies of offlineredo logs:

```
define mgmtclass sap_c21 p_c21 mdefault
define mgmtclass sap_c21 p_c21 mdb
define mgmtclass sap_c21 p_c21 mlog1
define mgmtclass sap_c21 p_c21 mlog2
```

If you are planning to use this Tivoli Storage Manager server with multiple SAP® systems, use a set of different management classes for each system.

3. Define a copy group:

```
define copygroup sap_c21 p_c21 mdefault type=backup destination=sap_incr
define copygroup sap_c21 p_c21 mdefault type=archive destination=archivepool
define copygroup sap_c21 p_c21 mdb type=archive destination=sap_db retver=nolimit
define copygroup sap_c21 p_c21 mlog1 type=archive destination=sap_log1 retver=nolimit
define copygroup sap_c21 p_c21 mlog2 type=archive destination=sap_log2 retver=nolimit
```

   Data Protection for *SAP*® for Oracle uses its own *version control* mechanism for managing SAP database backups by backing up all data to only those management classes for which an archive copy group has been defined (parameter `type` set to `archive`). In addition, to prevent backed up files within Tivoli Storage Manager server storage from being deleted because of their expiration date (Tivoli Storage Manager deletes expired files), the copy group parameter `retver` (specifies the number of days a file is to be kept) should be set to unlimited (`9999` or `nolimit`).

4. Assign the default management class:

```
assign defmgmtclass sap_c21 p_c21 mdefault
```

5. Validate and activate the policy set:

```
validate policyset sap_c21 p_c21
activate policyset sap_c21 p_c21
```

5. Register a node:

The Tivoli Storage Manager server views its registered clients, application clients, host servers, and source servers as nodes. To register a node, log on as the Tivoli Storage Manager administrator using the *Admin Command Line* or the *Web Admin* and run this command:

```
register node C21 passwd domain=sap_c21 maxnummp=8
```

When using two or more tape drives, the `maxnummp` parameter settings can affect the nodes. It defines the maximum number of mount points that one node can use. The default value is *1*. If one node should use more than one mount point, the parameter must be set to the desired number of mount points. This parameter should not be set higher than the total number of drives available on the Tivoli Storage Manager server.

6. Set the IdleTimeOut parameter:

For simulations of network transfer and media rates, the Tivoli Storage Manager server must be configured so that sessions do not time out during simulation. This is achieved by setting the parameter IdleTimeOut to a value higher than the time required for sending the largest table space file to Tivoli Storage Manager. For example:

```
setopt IdleTimeOut 60
```

7. Determine the Tivoli Storage Manager password method:

There are three methods of password handling:

No password required
No authentication is performed on the Tivoli Storage Manager server. Each user connected to the backup server can access Tivoli Storage Manager data without a password. This method is only recommended if adequate security measures are established. For example, no password might be acceptable when the Tivoli Storage Manager server is only used for SAP®, no other clients are registered, and authentication and authorization is performed at the operating system level.

Manual password handling
A password is required for each connection to the Tivoli Storage Manager server. In this method, Data Protection for *SAP®* for Oracle stores the encrypted password in its configuration files. As long as the password does not expire and is not changed on the Tivoli Storage Manager server, Data Protection for SAP automatically uses the stored password when connecting to Tivoli Storage Manager. This method provides password security and can be set up easily. Whenever the password expires or is changed, the new password must be set with this command:

(UNIX or Linux):

```
backint -p <full path to UTL file>/init<SID>.utl -f password
```

(Windows):

```
backint -p <full path to UTL file>\init<SID>.utl -f password
```

On Windows, the path can also be specified in UNC notation (for example: `-p \\SERVER_A\dpsap\init<SID>.utl`. However, the password updates need to be synchronized on the Tivoli Storage Manager server with the `update node` command. These steps must also be repeated whenever the Tivoli Storage Manager password expires. Therefore, this method is only recommended during installation or testing, and a long password expiration period should be specified. manual password handling is not recommended for production operations.

If setting the password is to be automated (such as in a script), enter this information on the command line:

```
backint -p <full path>/init<SID>.utl
   -f password  serverA:nodeA:passwordA serverB:nodeB:passwordB
```

where 'passwordA' is the password for Tivoli Storage Manager node 'nodeA' on Tivoli Storage Manager server 'serverA'.

Note:

1. The interactive password prompt is omitted only if the passwords for *all* server stanzas in the`.utl` file are specified.
2. There is a potential security risk involved in recording Tivoli Storage Manager passwords in a script.

Automatic password handling

A password is required for each connection to the Tivoli Storage Manager server. After the first connection, the password is managed by Tivoli Storage Manager. The Tivoli Storage Manager client stores the current password locally. When the password expires, the password is changed and stored automatically. If you are planning to use Oracle RMAN and schedule your backups or restores from a system user different from the database owner, you need to grant access permissions to your data files on disk for this user. You need to specify the Tivoli Storage Manager password currently in effect before you start using Data Protection for SAP in order to connect to the server for the first time and whenever the password is changed manually on the Tivoli Storage Manager server (command `update node`). You do this with the command:

(UNIX or Linux):

```
backint -p <full path to UTL file>/init<SID>.utl -f password
```

(Windows):

```
backint -p <full path to UTL file>\init<SID>.utl -f password
```

On Windows, the path can also be specified in UNC notation (for example: `-p \\SERVER_A\dpsap\init<SID>.utl`This method is recommended for an automated production environment.

Set the Tivoli Storage Manager password:

Data Protection for *SAP*® for Oracle should be installed after the Tivoli Storage Manager installation has been completed. Tivoli Storage Manager provides different password methods to protect data. Data Protection for SAP must use the same method as specified within Tivoli Storage Manager. The default password method during Data Protection for SAP installation is PASSWORDACCESS prompt. The default parameters for Data Protection for SAP are set according to this default value. If a different password method is set within Tivoli Storage Manager, refer to "7. Determine the Tivoli Storage Manager password method" on page 61 in order to adjust the Data Protection for SAP parameters.

Provide Data Protection for *SAP*® for Oracle with the password for the Tivoli Storage Manager node by performing these steps in the shell:

1. Log in as the Oracle user.
2. Enter the following command for Windows:

   ```
   backint -p <full path to UTL file>\init<SID>.utl -f password
   ```

   On Windows, the path can also be specified in UNC notation (for example: `-p \\SERVER_A\dpsap\init<SID>.utl`
3. Enter the following command for UNIX or Linux:

   ```
   backint -p <full path to UTL file>/init<SID>.utl -f password
   ```

4. Enter the password when prompted. On HP-UX, the password is limited to 8 characters. Make sure that the Tivoli Storage Manager password for HP-UX clients does not exceed this limit.

Password Configuration Matrix (UNIX or Linux):

Once the preferred method of password handling is determined, review these steps for direction as to how to set the keywords and parameters in the various profiles. Detailed information regarding password handling methods is available in "7. Determine the Tivoli Storage Manager password method" on page 61.

After you have selected the suitable password handling method, follow this configuration matrix to set the keywords and parameters accordingly. Proceed as indicated by the step number.

Table 8. Password Handling for UNIX or Linux

Step	Profile/Action	Parameter	Password		
			No	**Manual**	**Set by Tivoli Storage Manager**
1	Tivoli Storage Manager admin	AUTHENTICATION EXPIRATION PERIOD (see note 1)	OFF, n.a.	ON <n days> (see note 2)	ON <n days>
2	dsm.sys	PASSWORDACCESS PASSWORDDIR (see note 5) NODENAME	n.a. n.a. n.a.	PROMPT,n.a., n.a.	GENERATE <path> <nodename>
3	Tivoli Storage Manager admin	UPDATE NODE (see notes 1, 6)	n.a.	<password>	<password>
4	Data Protection for *SAP*® for Oracle profile (init<SID>.utl)	For each SERVER statement specify:PASSWORDREQUIRED ADSMNODE	NO <nodename>	YES <nodename>	NO (see note 4)
5	Data Protection for SAP command line	Specify in each SERVER statement: `backint -p init<SID>.utl -f password`	n.a.	<password> (see notes 3,7,9)	<password> (see notes 3,7,9)

Note:

1. See appropriate Tivoli Storage Manager documentation.
2. If you are using manual password generation during testing, make sure that the expiration period is set to an appropriate period of time.
3. This password must be the one that is effective on the Tivoli Storage Manager server for the node.
4. ADSMNODE must not be set when PASSWORDACCESS generate is set.
5. The users `<SID>adm` and `ora<SID>` must have read and write permission for the `path` specified in the `PASSWORDDIR` option in the Tivoli Storage Manager client options file.
6. This step is only necessary if the password is expired (manual handling only) or needs to be changed on the Tivoli Storage Manager server.
7. A password must be entered for each server statement in the Data Protection for SAP profile.
8. (No longer applicable.)

9. When using Oracle RMAN with PASSWORDACCESS GENERATE, backups must always be started with the same user ID provided in step 5 (setting of passwords).

Password Configuration Matrix (Windows):

Once the preferred method of password handling is determined, review these steps for direction as to how to set the keywords and parameters in the various profiles. Detailed information regarding password handling methods is available in "7. Determine the Tivoli Storage Manager password method" on page 61.

After you have selected the suitable password handling method, follow this configuration matrix to set the keywords and parameters accordingly. Proceed as indicated by the step number.

Table 9. Password Handling for Windows

Step	Profile/Action	Parameter	Password		
			No	**Manual**	**Set by Tivoli Storage Manager**
1	Tivoli Storage Manager admin	AUTHENTICATION EXPIRATION PERIOD(see note 1)	OFF, n.a.	ON <n days> (see note 2)	ON <n days>
2	<server>.opt	PASSWORDACCESS PASSWORDDIR (see note 5) NODENAME	n.a.n.a. n.a.	PROMPT,n.a., n.a.	GENERATE <path> <nodename>
3	Tivoli Storage Manager admin	UPDATE NODE (see notes 1,6)	n.a.	<password>	<password>
4	Data Protection for *SAP*® for Oracle profile `init<SID>.utl`	For each SERVER statement specify: PASSWORDREQUIRED ADSMNODE	NO <nodename>	YES <nodename>	NO (see note 4)
5	Data Protection for SAP command line	Specify in each SERVER statement: `backint -p init<SID>.utl -f password`	n.a.	<password> (see note 1)	<password>

Note:

1. See Tivoli Storage Manager documentation.
2. If you are using manual password generation during testing, make sure that the expiration period is set to an appropriate period of time.
3. For an initial setup, this password must be the same password specified when the node was registered to Tivoli Storage Manager. The password must be changed first on the Tivoli Storage Manager server and then on Data Protection for SAP.
4. ADSMNODE must not be set when PASSWORDACCESS generate is set.
5. The users `<SID>adm` and `sapservice<SID>` must have read and write permission for the `path` specified in the `PASSWORDDIR` option in the Tivoli Storage Manager client options file.
6. This step is only necessary if the password is expired (manual handling only) or needs to be changed on the Tivoli Storage Manager server.

7. A password must be entered for each server statement in the Data Protection for SAP profile.

8. Verify the Tivoli Storage Manager server name:

Review the Tivoli Storage Manager client options files to make sure that the server name matches the name specified in the server statement of the `init<SID>.utl` file. review that other parameters are set correctly. These depend on the password method selected. (See "7. Determine the Tivoli Storage Manager password method" on page 61).

On UNIX or Linux, define the Tivoli Storage Manager server in the Tivoli Storage Manager client system options file (`dsm.sys`). The server stanza specified in `dsm.sys` must match the entry in `init<SID>.utl`.

On Windows, you must define a client options file `<servername>.opt`. This file must be in the directory that contains `dsm.opt`. The value of `<servername>` is the server name specified in `init<SID>.utl`.

Chapter 6. Protecting SAP® data with Data Protection for *SAP®* for Oracle V6.1

Information needed to back up, restore, and clone your SAP® data is provided.

Review the information carefully before performing a backup or restore operation.

Backing up SAP® data

Instructions about how to back up your SAP® data is provided.

Perform the tasks required for your operating system.

Implementing the Strategy by Scheduling Automated Backup Runs

Scheduling (or automating) backup and archive operations helps ensure that the data is backed up regularly at a specified time. These products provide scheduled operations:

SAP® scheduler
The SAP® Computer Center Management System (CCMS) provides a scheduler for database administration and backup planning on a single database server. The scheduler can be started from the SAP GUI command line (transaction code `db13`) or with the SAP GUI menu function Tools -> CCMS -> DB administration -> DBA scheduling.

Scheduler (Windows) or Crontab (UNIX or Linux)
Automating backups at the database server level is available using either the Schedule Services feature (on Windows) or the `crontab` command (for UNIX or Linux). See "UNIX or Linux Crontab Example" on page 120 for more information.

Tivoli Storage Manager scheduler
Tivoli Storage Manager also provides a scheduler function for all of its clients. As a result, automation can be performed for multiple database servers. The Tivoli Storage Manager administrative client GUI provides a user-friendly wizard for defining schedules. Information on how to define Tivoli Storage Manager schedules can be found in the *Tivoli Storage Manager Administrator's Reference* manual.

IBM Tivoli Workload Scheduler
The IBM Tivoli Workload Scheduler provides event-driven automation, monitoring, and job control for both local and remote systems. More information can be found at http://www.ibm.com/software/tivoli/products/scheduler/.

Sample Backup Strategy for Daily Backup Processing

This figure illustrates the sequence of backup operations to consider for a daily backup schedule.

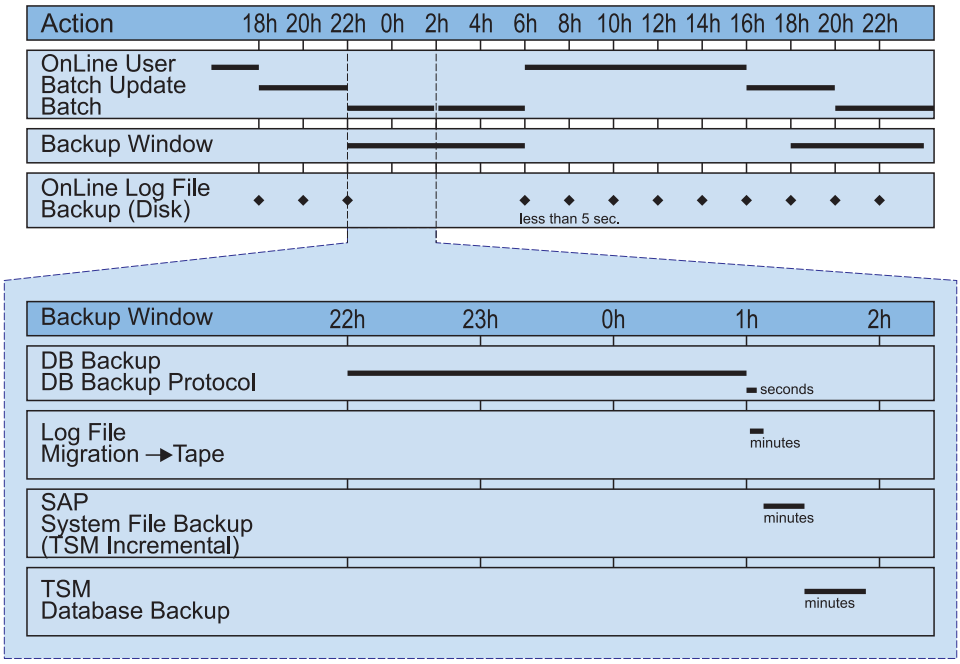


Figure 9. Production Backup Example

The automated backup example (shown in Figure 3) displays these common tasks:

- A full database backup (offline or without application load) performed each night.
- Offline redo logs are backed up to disk during online hours. This has the advantage of eliminating the need for extra tape mounts for relatively small files.
- The Tivoli Storage Manager server migrates archived log files from disk to tape after the full database backup.
- SAP system files are backed up incrementally with the Tivoli Storage Manager backup-archive client.
- The last backup in the daily cycle is the backup of the Tivoli Storage Manager database. This should always be performed.

Backups can be performed to disk storage as well as to tape media. The Tivoli Storage Manager server manages the data regardless of the storage media. However, backing up the SAP database directly to tape is the preferred media.

Windows Scheduling Example

On Windows systems, the schedule service must be running in order to start automated backup jobs. Issue this command to start the schedule service:

```
net start schedule
```

Use the `at` command to schedule jobs when the schedule service is running. This command launches the batch file `backup.cmd`. In this example, the command runs the schedule every Friday at 8:00 p.m.:

```
at 20:00 /every:f cmd /c <drive>:\oracle\SID\sapscripts\backup.cmd
```

Schedule Batch Sample

```
@echo off
rem ------------------------------------------------------------------------
rem file name: schedule.sample
rem ------------------------------------------------------------------------
rem Task:
rem Submits backup/archive commands at regularly scheduled intervals
rem using two simple batch files containing SAP backup/archive commands.
rem ------------------------------------------------------------------------
rem ***** NOTE ***** NOTE ***** NOTE *****
rem
rem This file is intended only as a model and should be
rem carefully tailored to the needs of the specific site.
rem
rem ***** NOTE ***** NOTE ***** NOTE *****
rem ------------------------------------------------------------------------
rem For a full reference of the AT command please see the Windows NT
rem help.
rem ------------------------------------------------------------------------
rem
rem For the following examples, the system ID of the ORACLE database
rem is assumed to be "C21".
rem
rem ------------------------------------------------------------------------
rem Full database backup, scheduled every Friday at 8:00 p.m.
rem
at 20:00 /every:f cmd /c c:\oracle\C21\sapscripts\backup\backup.cmd
rem
rem ------------------------------------------------------------------------
rem Save redo logs, scheduled twice a day at 11:30 a.m. and at 5:30 p.m.
rem Monday through Friday
rem
at 11:30 /every:m,t,w,th,f cmd /c c:\oracle\C21\sapscripts\backup\archive.cmd
rem --------------------- end of schedule.sample -----------------------
```

Full Offline Backup Batch File Sample

```
@echo off
rem Full Offline Backup batch file:
rem ------------------------------------------------------------------------
rem file name: backup.cmd
rem ------------------------------------------------------------------------
rem Sample BRBACKUP batch file
rem ------------------------------------------------------------------------
rem Task:
rem Invokes the SAP utility BRBACKUP in order to perform a full offline
rem backup of all tablespaces using Data Protection for SAP (R)
rem ------------------------------------------------------------------------
rem ***** NOTE ***** NOTE ***** NOTE *****
rem
rem This script is intended only as a model and should be
rem carefully tailored to the needs of the specific site.
rem
rem ***** NOTE ***** NOTE ***** NOTE *****
rem ------------------------------------------------------------------------
rem
rem For the following examples, the system ID of the ORACLE database
rem is assumed to be "C21".
rem
rem ------------------------------------------------------------------------
rem
rem First, let's do a full offline backup of the ORACLE database. This
rem includes at least files located in the following file systems:
rem c:\oracle\C21\sapdata0
rem c:\oracle\C21\sapdata1
rem c:\oracle\C21\sapdata2
```

```
rem c:\oracle\C21\sapdata3
rem c:\oracle\C21\sapdata4
rem
rem Remarks on the parameters of BRBACKUP:
rem
rem -u system/manager ORACLE username/password
rem -c run BRBACKUP in quiet mode
rem -m all backup all tablespaces
rem -t offline perform backup offline
rem
rem The following should be configured within the SAP profile
rem initC21.sap:
rem
rem backup_dev_type = util_file
rem causes BRBACKUP to use the external program
rem Data Protection for SAP (R)
rem util_par_file = %ORACLE_HOME%\database\initC21.utl
rem Data Protection for SAP (R) profile
rem ------------------------------COMMAND----------------------------------
brbackup -u system/manager -c -m all -t offline
```

Full Offline Backup Shell Script Sample

```
#!/bin/ksh
# ----------------------------------------------------------------------------
# backup.ksh:
# Sample BRBACKUP shell script
# ----------------------------------------------------------------------------
# Task:
# Invokes the SAP utility brbackup in order to perform a full offline
# backup of all tablespaces using Data Protection for SAP (R) technology.
# ----------------------------------------------------------------------------
#      *****     NOTE     *****     NOTE     *****     NOTE     *****
#
#          This script is intended only as a model and should be
#          carefully tailored to the needs of the specific site.
#
#      *****     NOTE     *****     NOTE     *****     NOTE     *****
# ----------------------------------------------------------------------------
#
# For the following examples, the system id of the ORACLE database
# is assumed to be 'C11'.
#
# ----------------------------------------------------------------------------
#
# First, lets do a full offline backup of the ORACLE database. This includes
# at least files located in the following filesystems:
#      /oracle/C11/sapdata0
#      /oracle/C11/sapdata1
#      /oracle/C11/sapdata2
#      /oracle/C11/sapdata3
#      /oracle/C11/sapdata4
#
# Remarks on the parameters:
#
# -u system/manager     Oracle username/password
# -c                    run brbackup in quiet mode
# -m all                backup all tablespaces
# -t offline            perform backup offline
#
# The following should be configured within the SAP profile initC11.sap:
#
# backup_dev_type = util_file
#  causes brbackup to use the external program backint
# util_par_file =  initC11.utl
#  Data Protection for SAP profile
```

```
#
# --------------------------------COMMAND----------------------------------
brbackup -u system/manager -c -m all -t offline
```

Restoring SAP® data

Instructions about how to restore your SAP® data is provided.

Perform the tasks required for your operating system.

Data Protection for *SAP®* for Oracle File Manager

The Data Protection for *SAP®* for Oracle File Manager is a supplementary tool that simplifies the Data Protection for SAP inquire, restore, and delete operations. However, users with Oracle database restore and recovery experience and knowledge should use this tool. BR*Tools is the standard tool for restore operations. Consider these important characteristics before using the File Manager:

- The File Manager perform all operations by using the standard functions provided by Data Protection for SAP.
- The interface consists of a split window that is character based. In the left window, all backup IDs found on all Tivoli Storage Manager servers that match the backup ID prefix configured in the Data Protection for SAP profile are displayed. In the right window, all the files belonging to the selected backup ID are displayed. Individual backup IDs or multiple files are available for selection as shown in Figure 11 on page 72).

1. Start the File Manager with the path and name of the Data Protection for SAP profile. The user must be a member of the `dba` group: (UNIX or Linux):

   ```
   backfm -p /oracle/SID/dbs/init<SID>.utl [-o <log file directory>]
   ```

   (Windows):

   ```
   backfm -p <drive>:\orant\database\init<SID>.utl [-o <log file directory>]
   ```

   If the `-o` parameter is specified at startup, the default directory for log files will be changed.
2. The File Manager calls the `backint` executable file to connect to the Tivoli Storage Manager server configured in the Data Protection for SAP profile. If this call fails, the File Manager shows an error message but does not analyze the cause of the error. Use the backint inquire function as described in (“Inquire function” on page 117) to analyze the error.
3. An automatic inquire operation for all backup IDs is performed by the File Manager. Figure 10 on page 72 displays a set of backup IDs located by an inquiry procedure. If you mark the backup ID you are interested in and then press the **Tab** key to move the cursor to the right-hand panel, all file names belonging to the marked backup ID will be displayed as shown in Figure 11 on page 72.

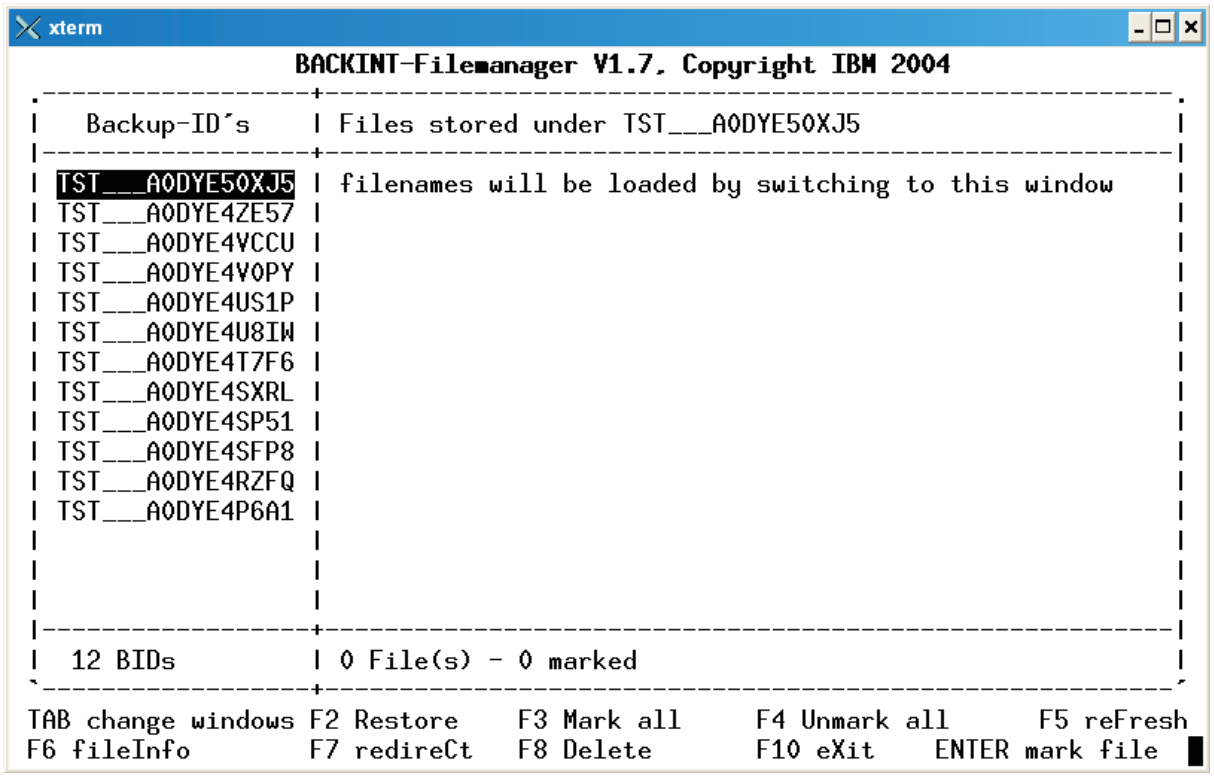


Figure 10. File Manager — Result of an Inquiry Procedure

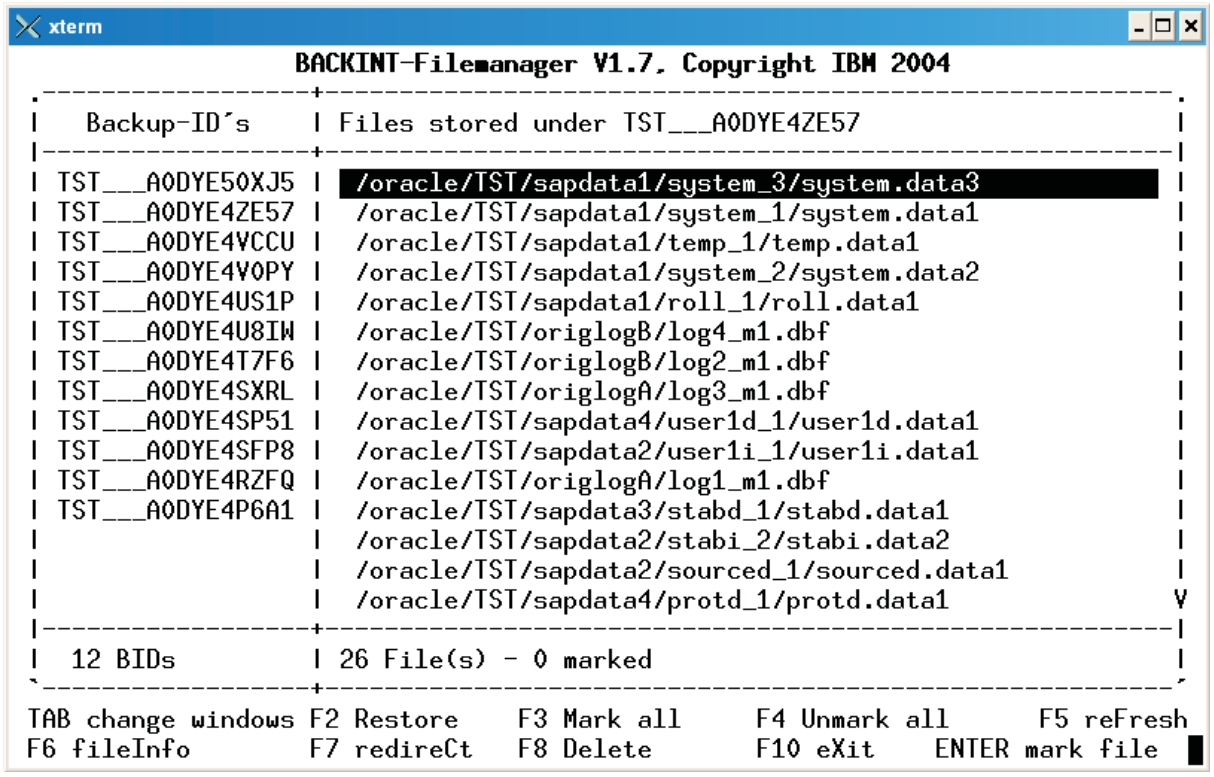


Figure 11. File Manager — Result of an Inquiry Procedure Showing File Names

The following function keys are defined for performing restore or delete operations:

Up, Down, Left, Right - Move cursor
Move the highlighted cursor in the direction indicated on the key.

Tab - Switch window side
Move the cursor between the left and right sides of the window.

F2 - Restore
Restore all marked files. Before the restore actually begins, you can specify a common destination path and you will be asked to confirm the restore process. If you specify a destination path, all marked files will be restored to that directory. Otherwise the files will be restored to the directory from which they were backed up.

For restore operations, the desired files first have to be marked. This can be done either with the **F3** function key to mark all the files that were found or with the **ENTER** key to mark only one desired file. Marked files can be identified by the symbol ″ * ″ in front of the filename. Only the marked files will be restored. For every restore operation, a log file will be created in the following location:

- (UNIX or Linux): $SAPDATA_HOME/sapbackup/backfm_<timestamp>.log
- (Windows): timestamp>.log

F3 - Mark all
All files belonging to the current backup ID will be marked.

F4 - Unmark all
Unmark all files belonging to the current backup ID.

F5 - Refresh
Refresh the list of backup IDs and file names.

F6 - Fileinfo
Opens a separate window to display file information.

For backup IDs, the sequence number is displayed (backup version count, for more information see on page "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122). For files, the Tivoli Storage Manager expiration date and time is displayed.

F7 - Redirected Restore
Restores the selected files to a new location. A new directory structure is created. The new path names are derived from the original paths by replacing the original SID with the target SID. Filenames are not modified. Redirected restore makes cloning of SAP® systems easier. See also "Cloning the SAP® System" on page 81. To clone a database you need to restore the database files to a different directory structure. In the path names of the new directory structure, the Oracle SID is replaced by the new SID. Please note that the file names are left untouched by this function. You first have to mark the files for restore. This can be done either with the **F3** function key to mark all files of a backup ID or with the **ENTER** key to mark only the highlighted file. Marked files can be identified by the symbol ″ * ″ in front of the filename. Press **F7** to start the redirected restore.

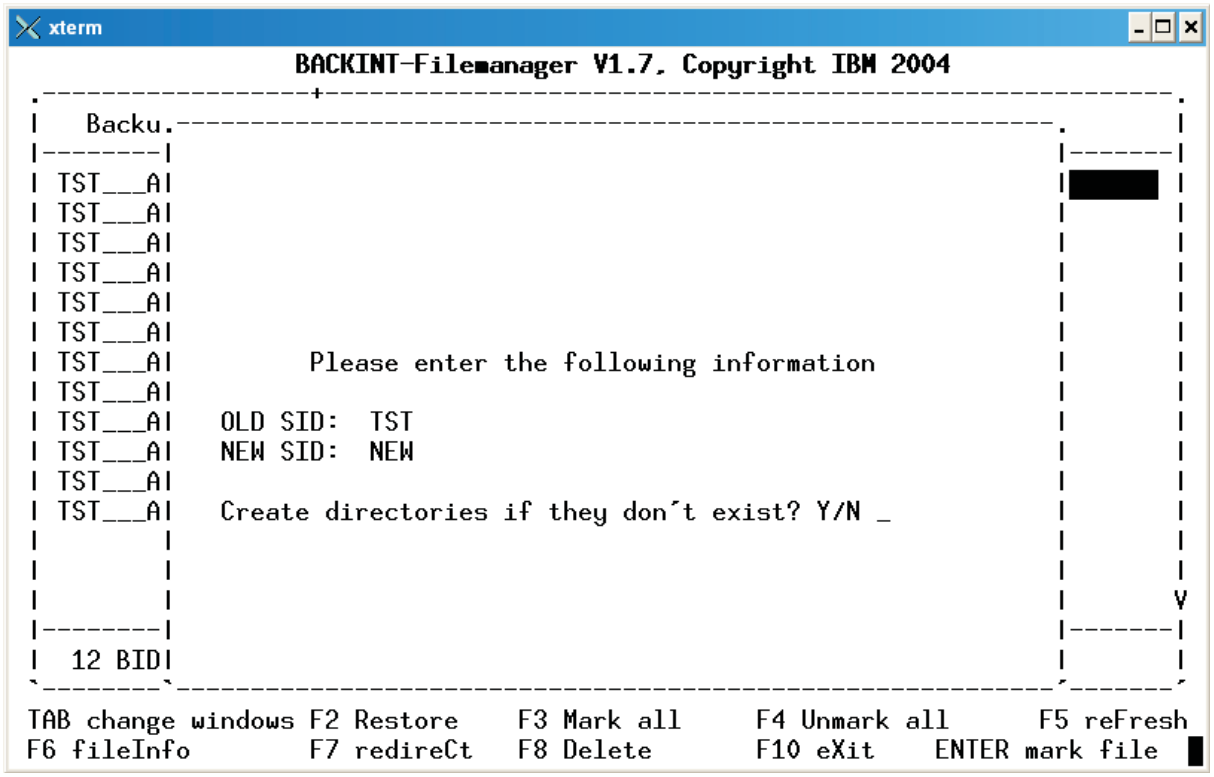


Figure 12. File Manager — Result of a Redirected Restore Procedure

F8 - Delete
Delete the selected backup ID and all corresponding files. The File Manager can delete backup IDs with all included files. It is not possible to delete single files within a backup ID. To delete a backup ID it must be highlighted. After pressing **F8** you have to confirm the deletion operation. The backup ID and all included files are deleted from the Tivoli Storage Manager server.

F10 - Exit
Exit from Data Protection for SAP File Manager

ENTER - Mark/unmark file
Mark or unmark the file below the cursor.

Protecting SAP® data with the Administration Assistant function for Data Protection for *SAP®*

Instructions about how to protect your SAP® data with the Administration Assistant function for Data Protection for *SAP®* is provided.

Perform these tasks in order to protect your SAP® data with the Administration Assistant function for Data Protection for *SAP®*.

Administering User IDs

The Administer users function allows accounts to be created or deleted and user permissions to be granted or revoked. Note that profiles for authorized users need to be created when the Administration Assistant is started for the first time. The online help provides details on creating profiles. For each SID in the system landscape, the following permissions can be granted:

- **Simulate backup/restores**: to initiate simulations
- **Configure groups**: to configure display groups to be used with function ″Monitor backup states″
- **Problem support**: to send support request mail
- **Operations monitoring**: to view backup status information
- **User administration**: to manage user accounts
- **Performance monitoring**: to view performance data
- **Configuration**: to modify the configuration of Data Protection for *SAP*® for Oracle

Additionally, a user can be granted permission to configure parts of the internal logic of the Monitor backup states function.

Specifying a new Administration Assistant function for Data Protection for *SAP*®

If the Administration Assistant function for Data Protection for *SAP*® has not been installed, you can establish a connection when needed by following these instructions.

If you need to specify a new Administration Assistant function for Data Protection for *SAP*® Server component, perform the following steps on the SAP® database server:

(UNIX or Linux)

1. Find the entry for daemon ProLE in `/etc/inittab`. Modify the entry to read as follows:

   ```
   .../prole -p tdpr3ora64 <Server component hostname> <port>
   ```

   where `<Server component hostname>` is the name or IP address of the host running the Administration Assistant Server component and `<port>` is the port the Server component is listening to for connects from Data Protection for *SAP*® for Oracle (default `5126`).
2. Make sure that Data Protection for SAP is not running, and use the `kill` command to stop the ProLE daemon. The ProLE daemon will be restarted automatically with the new parameters.

(Windows)

1. Log in as a user with administrator authority.
2. Enter this command from a command prompt:

   ```
   prole -update -p tdpr3ora64 <Server component hostname> <port>
   ```

where<Server component hostname> is the name or IP address of the host running the Administration Assistant Server component and <port> is the port that the Server component is listening to for connects from Data Protection for SAP (default 5126).

Generating Reports Using Report Templates

Once report templates are available, the Administration Assistant function for Data Protection for *SAP*® reports can be started automatically at given points in time using a preferred scheduler. The scheduler must call the scheduler interface Sched_Main which can be started from a scheduling client as described in "4. Configure a scheduling client to create reports" on page 48.

The scheduling interface is called by using this command syntax:

```
java -cp $CLASSPATH com.ibm.bkit.schedulerIF.Sched_Main <Server component hostname>...
... <RMI registry port> <template name> <userid> <password>...
... directory=<local directory> log=<log path>
```

- <Server component hostname>: The name or IP address of the host running the Administration Assistant Server component.
- <RMI registry port>: The number of the RMI registry port of the Administration Assistant Server component as defined in its configuration file (*assist.cfg*). The default value is 1099.
- <template name>: The name of the appropriate report template to be used. It must be available in the user template path in the Administration Assistant Server component.
- <userid>: The Administration Assistant account of the template owner.
- <password>: The password associated with <userid>.
- <local directory>: The local path in the system of the scheduling client where the requested reports are to be stored. If the local directory is not specified, the reports are not stored in the local file system. In order to access the report, the administrator needs file system access to the Administration Assistant server where the report is kept for 24 hours.
- <log path>: The local path in the system of the scheduling client where the scheduling client saves its own log files.

Consider creating a command file that sets the correct environment and schedules one (or more reports) on the scheduling client system as described in "4. Configure a scheduling client to create reports" on page 48. If a large number of clients try to connect to the Administration Assistant server simultaneously, some of them may not immediately connect. In this case, the scheduling client waits for a random time between 15 and 45 seconds before another attempt is made. After the second unsuccessful attempt, the scheduling client creates an error log and exits.

Requesting a Report from the Administration Assistant function for Data Protection for *SAP*® Client

A report is requested by selecting the Create Report button on the Monitor Backup States, Backup State - Detailed View, View Performance Data (History Mode), and Available Simulation Results panels of the Administration Assistant function for Data Protection for *SAP*® graphical user interface. Reports requested from the Backup State - Detailed View, View Performance Data (History Mode), and Available Simulation Results panels always pertain to the single SID currently displayed on the panel. Reports requested from the Monitor Backup States panel

contain information on all SIDs displayed on the panel. Selections made in the table of systems do not have an impact on the report created. However, active filters or the activation of a display group is reflected in the report. A time interval can be specified in the report. Backup operations are included in the report if they completed within the specified time interval. Also, some reports can include information about log files.

Starting and Stopping the Administration Assistant function for Data Protection for *SAP®* Manually

You can manually start or stop the Administration Assistant function for Data Protection for *SAP®* by using these command files (located in the installation directory):

- Issue this command to start or stop the Administration Assistant Server component:

  (UNIX and Linux):

  ```
  sadma.sh start|stop <Server component configuration file>
  ```

  (Windows):

  ```
  sadma.cmd start|stop <Server component configuration file>
  ```

- Issue this command to start or stop the Administration Assistant Database Agent:

  (UNIX and Linux):

  ```
  sdba.sh start|stop <Database Agent configuration file>
  ```

  (Windows):

  ```
  sdba.cmd start|stop <Database Agent configuration file>
  ```

- When using the bundled Apache Derby, issue this command to start or stop the Administration Assistant Database component:

  (UNIX and Linux):

  ```
  sdb.sh start|stop
  ```

  (Windows):

  ```
  sdb.cmd start|stop
  ```

- When using the IBM DB2 data server, use the DB2 Control Center or the DB2 command line to start or stop the database. Refer to your IBM DB2 data server documentation for complete instructions.

Important: When the Server or Database Agent components are started, a lock file (`.lockAA` and `.lockDBA`, respectively) is created. If either of these components are terminated or restarted using the delivered scripts, the respective lock file is also deleted. If for some reason the lock file still exists when the component is started, the request will fail with an error message. In this case, first verify that the process is not already active. If it is not active, the lock file must be deleted manually and

the start request reissued.

Changing the Password for the Administration Assistant function for Data Protection for *SAP*® Database User ID

The password for accessing the internal Administration Assistant function for Data Protection for *SAP*® database can be changed using the changeSettings.jar program. This program was added to the installation directory in the `utils` subdirectory:

1. Change to the `utils` directory and issue the command

```
java –cp changeSettings.jar run
```

2. Select the type of database you are using with the Administration Assistant function for Data Protection for *SAP*® (Apache Derby or IBM DB2).
3. Enter the directory containing the encrypted password file (pass.enc).
4. Enter the user ID and the existing password.
5. Enter the new password.
6. For Apache Derby only: To apply the new password to the database, check the box provided. Otherwise, the password file is updated but the database change must then be performed manually.
7. Click Next to complete the change.

Cyclic Procedure for Optimizing your Configuration

The Administration Assistant function for Data Protection for *SAP*® Database User ID provides the ability to analyze performance, modify the configuration, and test the effects of configuration changes without having to modify the production environment.

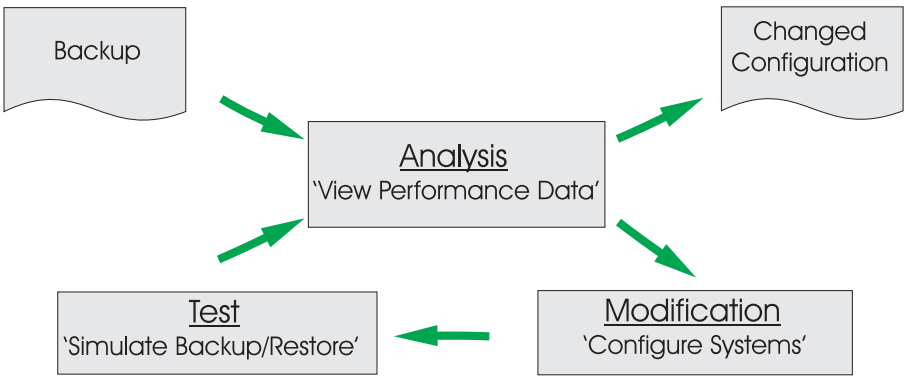


Figure 13. Optimizing your Configuration with the Administration Assistant function for Data Protection for SAP®

The optimization cycle starts with a full backup of the database using the file interface (BRBACKUP). The performance data is analyzed using the View Performance Data function. This function provides insight as to possible Data Protection for *SAP*® for Oracle configuration or infrastructure changes. These changes are temporarily implemented in a test profile with the Configure Systems function. Using the Simulate Backup/Restore function, another backup or restore is simulated to test the configuration changes. The View Performance Data function can then be used to verify whether the changes produced the desired results. This cycle can be implemented multiple times until the desired results are met. Once the configuration changes are confirmed, they can be propagated to the production system. Note that all configuration changes and simulation runs within the cycle

are maintained separately from the production system.

Determining Throughput Rates

Table 10. Summary: How to Determine Throughput Rates

	Disk I/O Rate	**Storage Media Rate**	**Network Throughput Rate**
Simulation Type	No data moved to/from Tivoli Storage Manager	No data moved to/from disk	No data moved to/from disk
Disk Transfer Rate	-	infinite	infinite
Network Transfer Rate	infinite	-	-
Tape Rate	infinite	-	-
RL Compression	off	off	off
Multiplexing	1	1	1
Number of Sessions	1	1	maximum possible number

Determining the Actual Disk I/O Rate

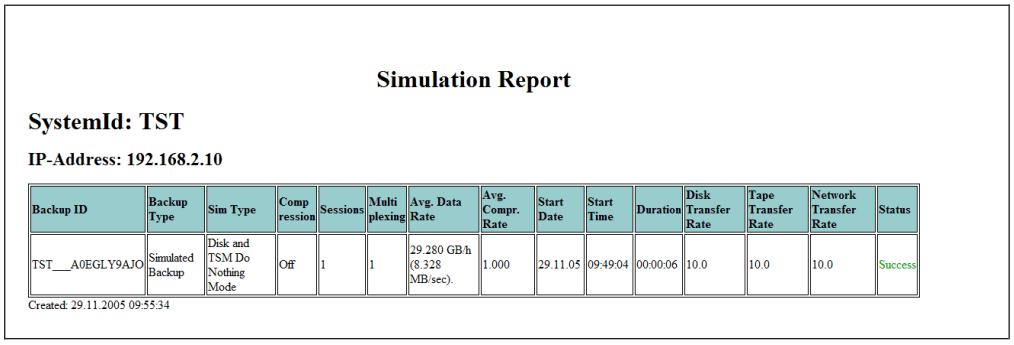
Run a simulated backup of type No data moved to Tivoli Storage Manager in order to determine the actual disk reading rate. Both the Tape Transfer Rate and the Network Transfer Rate must be set to infinite in order to make sure there will not be a network bottleneck. Compression must be turned off and the View Performance Data function should show 100 % disk utilization. The overall throughput you get with this configuration is the rate at which data is read from disk. In order to determine the actual disk writing rate, run a simulated restore of type No data moved from Tivoli Storage Manager. Both the Tape Transfer Rate and the Network Transfer Rate must be set to infinite in order to make sure the system will not create a network bottleneck. Compression must be turned off and the View Performance Data function should show 100 % disk utilization. The overall throughput you get with this configuration is the rate at which data is written to disk. Be aware that an increased disk I/O rate is shown while data is written to the file system cache.

Determining the Actual Network Throughput Rate

Run a simulated backup of type No data moved from disk in order to determine the actual network throughput rate. The Disk Transfer Rate must be set to infinite in order to make sure there will not be a disk bottleneck. Increase the number of sessions to the maximum number possible (for example, the number of available tape drives). To be sure that the limiting factor is not the tape transfer rate, the throughput rate must be less than the media rate as provided in the 'Determining the Actual Throughput Rate of Storage Media' section, multiplied by the number of sessions. The View Performance Data function should show 100% network utilization. The overall throughput provided with this configuration is the network throughput rate.

Reporting on Simulations

An overview of simulation parameters and results for a single SID is contained in the Simulation Report. It is requested from the Available Simulation Results panel and displays a screen capture similar to this panel.



Simulation Report

SystemId: TST

IP-Address: 192.168.2.10

Backup ID	Backup Type	Sim Type	Comp ression	Sessions	Multi plexing	Avg. Data Rate	Avg. Compr. Rate	Start Date	Start Time	Duration	Disk Transfer Rate	Tape Transfer Rate	Network Transfer Rate	Status
TST___A0EGLY9AJO	Simulated Backup	Disk and TSM Do Nothing Mode	Off	1	1	29.280 GB/h (8.328 MB/sec).	1.000	29.11.05	09:49:04	00:00:06	10.0	10.0	10.0	Success

Created: 29.11.2005 09:55:34

Figure 14. Simulation Report

Simulating Backup and Restore

The Administration Assistant function for Data Protection for *SAP*® Simulate Backup/Restore function requires a full backup of the database using the file interface (BRBACKUP). Backups done using the RMAN interface cannot serve as a basis for simulation. Both backups and restores can be simulated. A restore simulation might provide information regarding the duration of the restore operation but it will not affect your production system. When there are two (or more) eligible backups available, the latest one is used as the basis for simulation. Compression should be enabled for the base backup and the COMPR_INFO parameter should specify a valid file in the Data Protection for *SAP*® for Oracle profile. These environment components are available for simulation:

Disk I/O

No data is read from the disk when simulating disk I/O for a backup. Data is generated in memory instead. When simulating disk I/O for a restore, data is consumed and is not written to disk. The disk I/O rate to be used for the simulation is set by the administrator as described in "Determining the Actual Disk I/O Rate" on page 79.

Network transfer and media rates

No data is sent through the network when simulating network transfer and media rates for a backup. The data is consumed instead. When simulating network transfer and media rates for a restore, no data is expected from the network and the data is generated in memory instead. However, a connection to the Tivoli Storage Manager server needs to be maintained during the simulation. Therefore, configure the Tivoli Storage Manager server so that the sessions do not time out as described in "6. Set the IdleTimeOut parameter" on page 60. The network throughput rate and the media rate used for the simulation can be set by the administrator. "Determining the Actual Network Throughput Rate" on page 79 and "Determining the Actual Throughput Rate of Storage Media" on page 81 provide information about determining these rates.

Configuration changes

When simulating configuration changes, performance parameters (in the Data Protection for SAP profile) can be modified to test for the optimum configuration within a given infrastructure. During a backup configuration simulation, data is read from disk and written to a special file space in Tivoli Storage Manager and does not affect production backups. During a

restore configuration simulation, data is retrieved from the Tivoli Storage Manager server and written to disk before they are deleted. See "Performance Options of Data Protection for *SAP*® for Oracle" on page 96 for information about Data Protection for SAP profile parameters that affect data throughput.

Determining the Actual Throughput Rate of Storage Media

Run a simulated backup of type No data moved from disk in order to determine the actual writing rate of a tape. The Disk Transfer Rate must be set to infinite in order to make sure there will not be a disk bottleneck. The number of sessions must be set to one, compression must be turned off, and the View Performance Data function should show 100 % disk utilization. The overall throughput provided with this configuration is the rate at which data is written to the storage media unless the network rate is lower than the media rate. In order to determine the actual reading rate of a tape, run a simulated restore of type No data moved to disk. The Disk Transfer Rate must be set to infinite in order to make sure there will not be a disk bottleneck. The number of sessions must be set to one. In order to exclude a CPU bottleneck, make sure that the View Performance Data function shows 100 % network utilization. The overall throughput provided with this configuration is the rate at which data is read from the storage media unless the network rate is lower than the media rate. Note that the throughput rate might not increase when the number of sessions is increased. In this situation, the network throughput rate is lower than the media rate, and the media rate cannot be determined with the Administration Assistant.

Cloning the SAP® System

This information regarding how to clone an SAP® system should be used to complement the primary SAP documentation *R/3 Homogeneous System Copy* and *R/3 Installation on UNIX / Windows - Oracle Database*. Make sure the SAP documentation is correct for the environment. SAP documentation is available at http://sapnet.sap.com and on the SAP Documentation Guides CD. Additional information about SAP system cloning can be found in the IBM Redbooks publication *SAP R/3 Data Management Techniques Using Tivoli Storage Manager*. The book can be downloaded at http://www.redbooks.ibm.com.

What is Cloning?

SAP system cloning refers to an operation where an exact copy of one source SAP system (original system) is copied to a target SAP system (destination system). The copy is considered an homogeneous system copy when the original system and destination system contain the same SAP release level, operating system, and database version. The copy is considered an heterogeneous system copy when the SAP release level, operating system, and database version are not the same. Detailed information about these two system copy scenarios can be found in SAP Notes 86859 and 86860.

SAP system cloning considered appropriate in these situations:

- Setting up an SAP system landscape (development, quality assurance, and production system).
- After a hardware upgrade is completed.
- Creating multiple SAP test or demonstration systems.

Performing SAP® System Cloning when automatic password handling is used

Although this procedure is provided as a reference, SAP® documentation should be used as the primary instructions when cloning SAP systems. For SAP-specific changes, see also SAP Note 71254. This procedure assumes this environment:

- Two SAP R/3 systems are installed and operating on two different machines.
- Data Protection for *SAP*® for Oracle is installed and operating on both SAP R/3 systems.

This procedure describes the tasks necessary to restore an Oracle SID to a different machine with a different SID. Use the procedure that reflects the password handling method for the environment.

Perform these tasks when automatic password handling (passwordaccess=generate) is used:

1. Make sure that the same nodename and password that are specified in the Tivoli Storage Manager client options file on the source system are specified on the target system.

   Note: Make sure the client uses the password that is stored on the Tivoli Storage Manager server. Although passwords are stored in different locations, the only original password is the one that resides on the Tivoli Storage Manager server.
2. Make a backup copy of the client option file on the target system.
3. Copy the client option file from the source system to the target system.
4. Edit the client option file and add `NODENAME source system` to the server stanza.
5. Reset the Tivoli Storage Manager password for the target system node on the server.
6. As root (UNIX or Linux) or administrator (Windows), set the new password on the client.
7. Make a backup copy of the `init<SID>.utl` file on the target system.
8. Copy the `init<SID>.utl` file from the source system to the target system. Rename the file from `init<SID>.utl` to `init<target_SID>.utl`.
9. Edit the `init<SID>.utl` file on the target system to reflect all the correct file and path names, especially for CONFIGFILE and TRACEFILE.
10. Restore the database under the SAP considerations.
11. After the restore, reset the client option file and `init<SID>.utl` file to their original and set the passwords on the target system.
12. Reset the passwords on the source system.

Detailed information regarding automatic password handling is available on page "7. Determine the Tivoli Storage Manager password method" on page 61.

Performing SAP® System Cloning when manual password handling is used

Although this procedure is provided as a reference, SAP® documentation should be used as the primary instructions when cloning SAP systems. For SAP-specific changes, see also SAP Note 71254. This procedure assumes this environment:

- Two SAP R/3 systems are installed and operating on two different machines.
- Data Protection for *SAP*® for Oracle is installed and operating on both SAP R/3 systems.

This procedure describes the tasks necessary to restore an Oracle SID to a different machine with a different SID. Use the procedure that reflects the password handling method for the environment.

Perform these tasks when manual password handling (passwordaccess=prompt) is used:If you are using `passwordaccess=prompt`, you only need to set the nodename/password in the `init<SID>.utl` file:

1. Create a backup copy of the `init<SID>.utl` file on the target system.
2. Copy the `init<SID>.utl` file from the source system to the target system. Rename the file from `init<SID>.utl` to `init<target_SID>.utl`.
3. Edit the `init<SID>.utl` file on the target system to reflect all the correct file and path names, especially for CONFIGFILE and TRACEFILE.
4. As `<SID>adm` user, set the Data Protection for *SAP*® for Oracle password on the target system: (UNIX or Linux):

   ```
   backint -p /oracle/<SID>/dbs/init<SID>.utl -f password
   ```

   (Windows):

   ```
   backint -p <drive>:\orant\database\init<SID>.utl -f password
   ```

   Issue the password when prompted. On Windows, the profile path can also be specified in UNC notation (for example: `-p \\SERVER_A\ora nt\database\init<SID>.utl`
5. Restore the database according to the SAP recommendation.
6. Reset the `init<SID>.utl` file and the password on the target system.

Detailed information regarding manual password handling is available on page "7. Determine the Tivoli Storage Manager password method" on page 61.

Chapter 7. Performance tuning for Data Protection for *SAP®* for Oracle

Information needed to fine-tune Data Protection for *SAP®* for Oracle performance is provided.

Overview of a balanced system

Descriptions on how to proceed when tuning your system according to your needs is discussed. This is done by employing a combination of functions provided in the Administration Assistant function for Data Protection for *SAP®*.

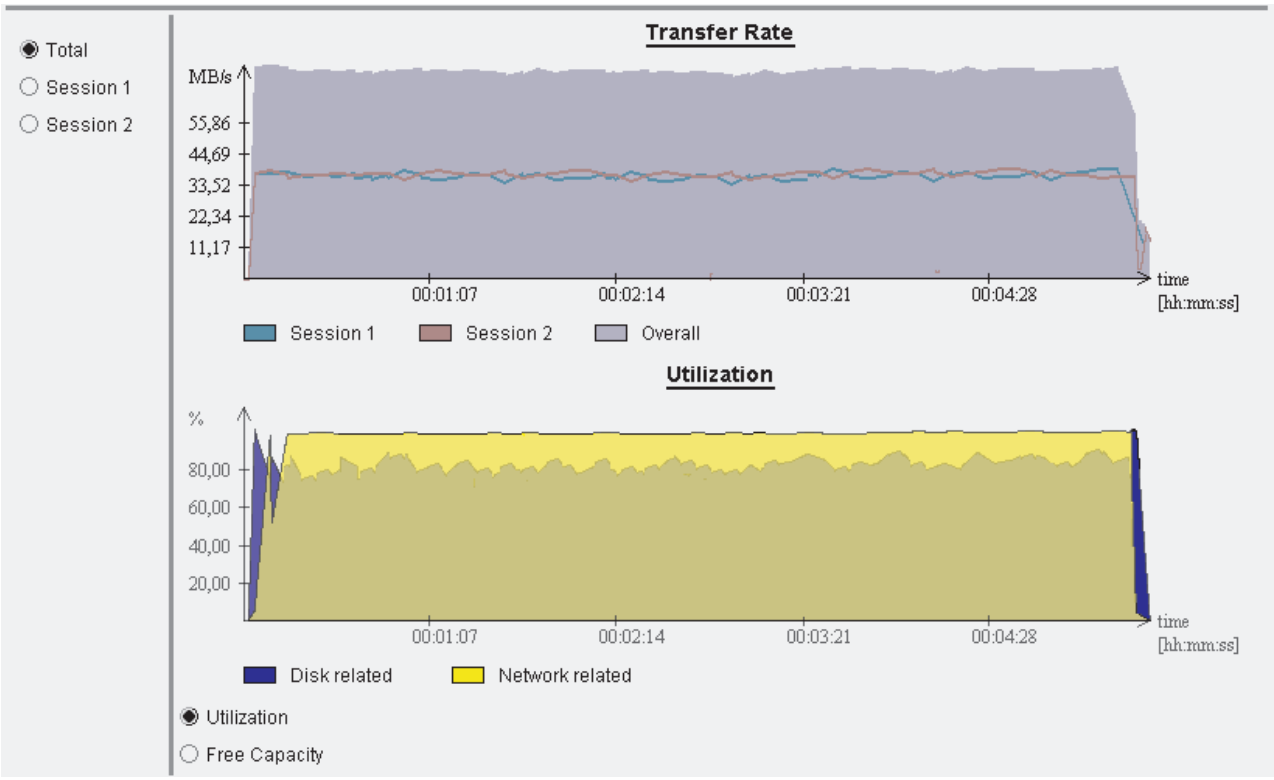


Figure 15. Indicating a Balanced Configuration

A system is considered balanced when the threads on both the disk and the network side are similarly busy throughout the backup and resource utilization is good. In an optimum setup, tapes are maintained in streaming mode. This means that the network is at least as fast as the tape and there is no idle time on the network side. Thus, a slight network bottleneck is desired. Under certain conditions, the degree of imbalance cannot be determined from the graphical presentation. Depending on your system characteristics (system buffering, buffer sizes, etc.), utilization may reduce to almost zero in the graphical presentation although the system is actually balanced. In this case, slight modifications can yield a change of bottleneck without significant throughput changes. However, whether the system is disk or network, tape constraints are always shown correctly. To improve overall throughput, consider adding more resources to create

a balanced system. A balanced system, however, does not necessarily mean that the data throughput cannot be improved further. Adding new resources can still improve the throughput rate.

Example of a disk bottleneck

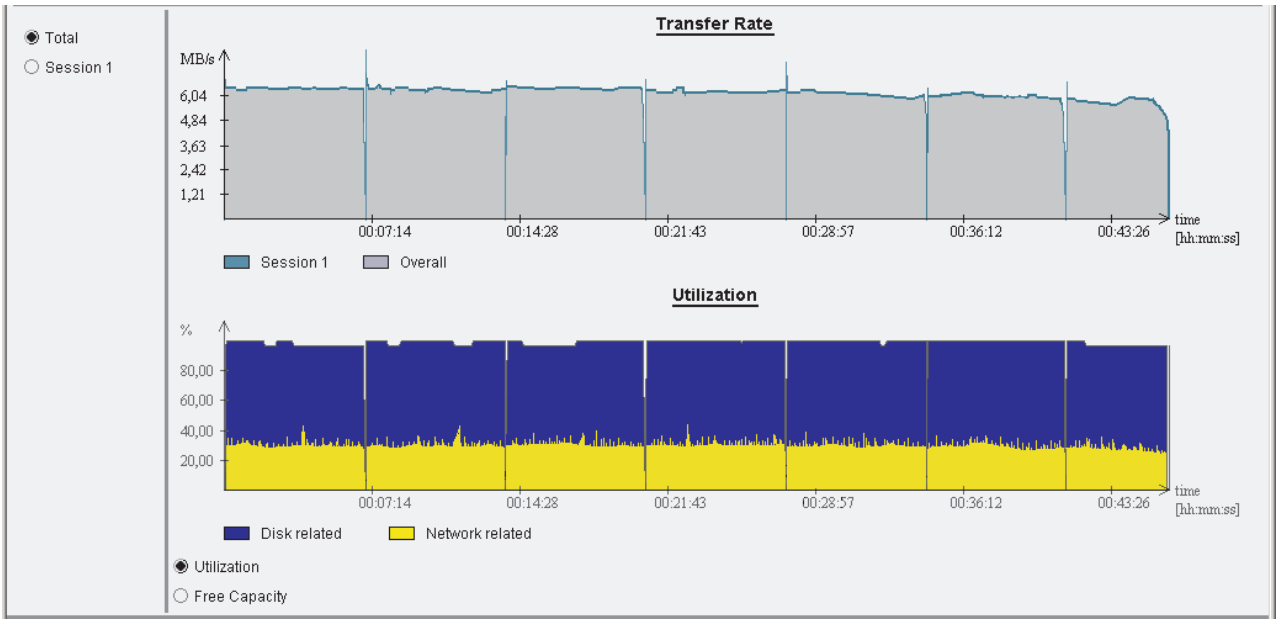


Figure 16. Indicating a Disk Bottleneck

A disk bottleneck occurs when data is processed by the network and Tivoli Storage Manager server faster than the data can be read from disk. As a result, overall throughput is limited by the disk I/O rate and the network thread is idle. Although internal buffering causes network threads to return very quickly, the network utilization might be reduced to almost zero in this situation. Both the network and the storage media are not used to their capacity. When tapes are used, they are not kept in streaming mode when this type of bottleneck occurs. Overall throughput can be improved by increasing multiplexing (which accelerates disk reading) or making sure data compression is not used. By reducing the number of sessions to the Tivoli Storage Manager server and the number of tapes used for the backup while also increasing multiplexing at the same time, resources (such as tape drives) are used more efficiently. See "Cyclic Procedure for Optimizing your Configuration" on page 78 for more information about optimizing your system.

Example of a network or Tivoli Storage Manager bottleneck

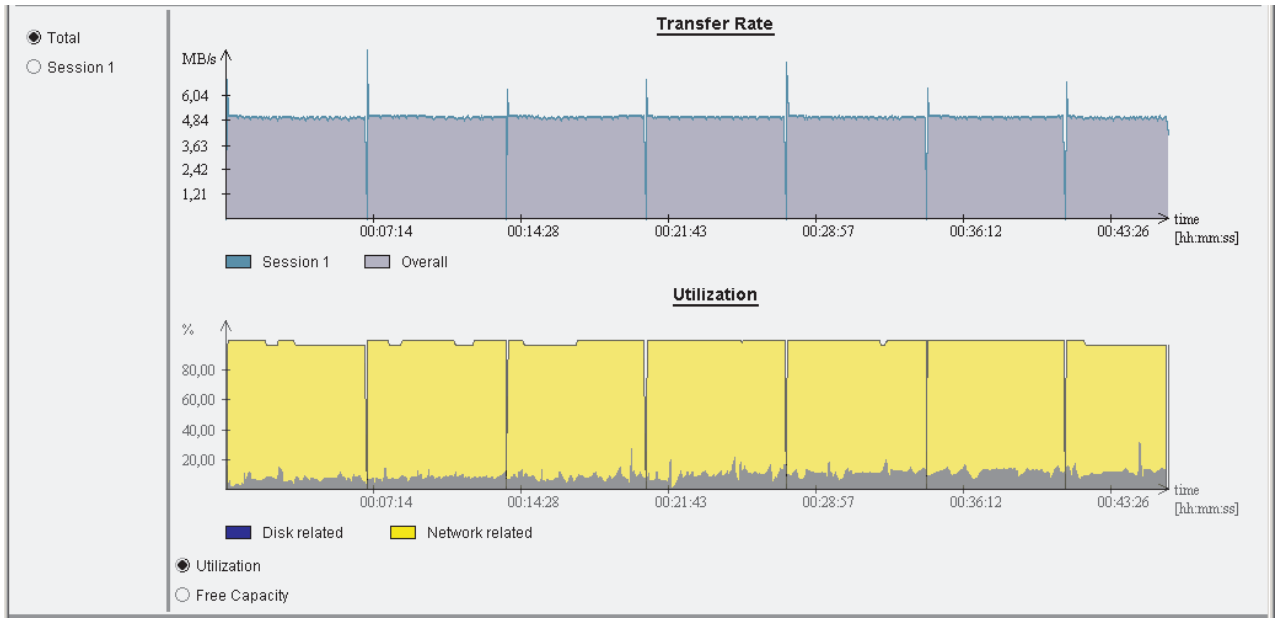


Figure 17. Indicating a Network or Tivoli Storage Manager Bottleneck

A network or Tivoli Storage Manager bottleneck occurs when data is read from the disk faster than the network or Tivoli Storage Manager can process the data. Consequently, throughput is limited either by the network capacity or by the disk or tape storage media rate. In depth analysis is usually required in order to identify the exact cause of the bottleneck. However, some insight is obtained from the Data Protection for *SAP*® for Oracle performance analysis, as described in "Simulating Backup and Restore" on page 80. Overall throughput might be improved by implementing any of these guidelines:

- If the tape is the bottleneck, increase the number of sessions to the Tivoli Storage Manager server.
- Use multiple paths to the Tivoli Storage Manager server or use multiple Tivoli Storage Manager servers.
- Use RL compression in order to reduce the amount of data to be sent to storage.

Also, to better exploit the resources, consider reducing multiplexing so that less data is read simultaneously from the disk. If the database is configured for file-online backup, reducing multiplexing will also reduce the number of redo logs created during the backup. See "Cyclic Procedure for Optimizing your Configuration" on page 78 for more information about optimizing your system.

Viewing performance data

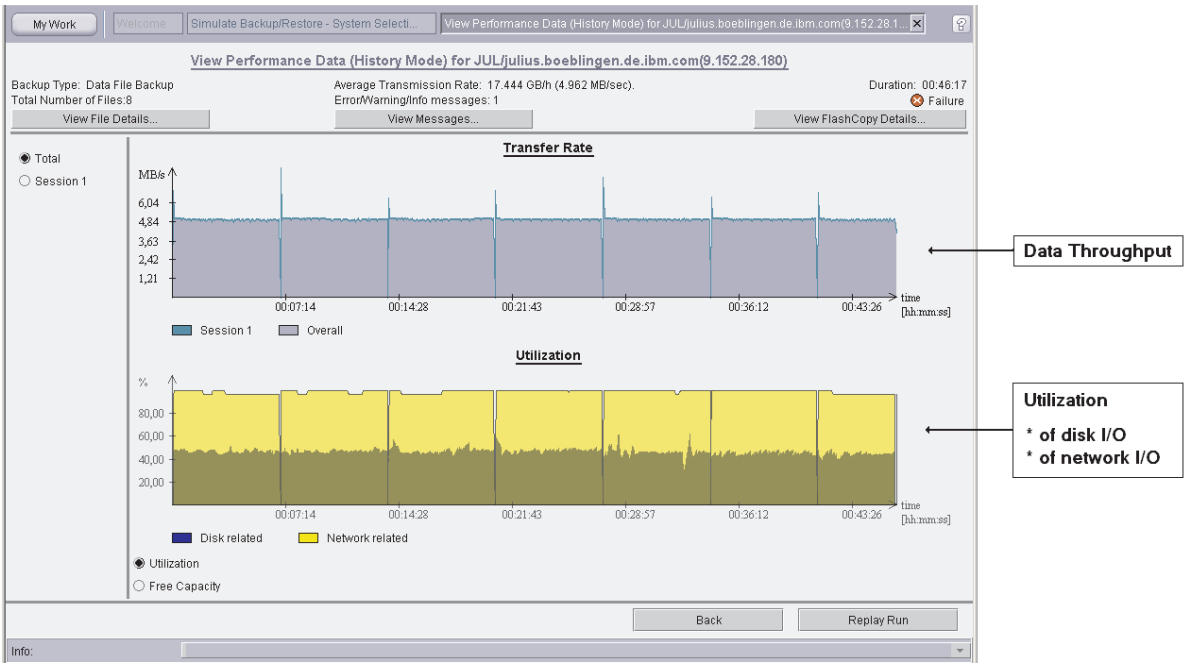


Figure 18. Showing Data Throughput and I/O Utilization

The Administration Assistant View Performance Data function provides a graphical representation of the data throughput rate at any point in time during the backup. Aligned with this representation, the utilization rates of the disk (presented in blue by the Administration Assistant) and network threads (presented in yellow by the Administration Assistant) are displayed. Optionally, the free capacity of these threads can also be displayed. These rates displayed can be displayed for all Tivoli Storage Manager sessions used in the backup or display rate on a per-session basis only. Time intervals that require further analysis are selected for viewing in replay mode as described in "Drilling Down on Special Situations." Data Protection for *SAP*® for Oracle performance sensor results are displayed using the Administration Assistant View Performance Data function. The Administration Assistant collects history data during each backup run for later analysis. In order to find the results, select View Performance Data, then select History Data. In the list of eligible backups, select the backup to be analyzed. Press the Review button to view the performance data summary panel.

Drilling Down on Special Situations

When looking at the diagrams in the View Performance Data function, you might find points in time when throughput or the utilization of a resource decreases significantly. To better understand what happened, you may drill down on these time intervals. In most cases you will find that a session is ending or a shorter file was multiplexed with longer files.

Using reports

After a backup completes, Data Protection for *SAP*® for Oracle creates a report that contains statistical information such as the number of bytes transferred and the effective data throughput. The profile keyword REPORT (on page "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122) can provide additional information on report levels. The Administration Assistant program also provides detailed performance information that assists when optimizing your system. Reports can be provided in XML- or HTML-format for display and printing. Complete report information is available in "Reporting on Data Protection for *SAP*® for Oracle Activities" on page 95.

Performance Analysis

The Administration Assistant provides performance data for all components involved in the data transfer. Graphical representations are provided that help identify problem areas and resource use. Backup and restore simulations are also available. These simulations can test configuration changes or planned restore operations without compromising the production system. Performance optimization is discussed in detail in "Overview of a balanced system" on page 85.

Tracing

Trace information can be recorded in a file to help analyze problems that occur. However, contact your Data Protection for SAP support before attempting to use this function.

Monitoring the Backup Status

Backup status of multiple SAP® database servers is available by using the Administration Assistant. See "Reporting on Backup Status" on page 91 for complete details.

Reporting on the Performance of Backup Operations

The performance data of a single backup are included in the Performance Report. Although data is presented in the same manner as in the View Performance Data (History Mode) panel, the transfer rate and the utilization of adapters for each session are also displayed. The report is requested from the View Performance Data (History Mode) panel.

Performance-Report

TST (gladiator.boeblingen.de.ibm.com)

System Status: success

Type of run: full , data

Start Date	Start Time	Backup Type	Status	Throughput	End Date	End Time
18.11.2005	22:00:33	full	Success	113.11GB/h	18.11.2005	22:51:02

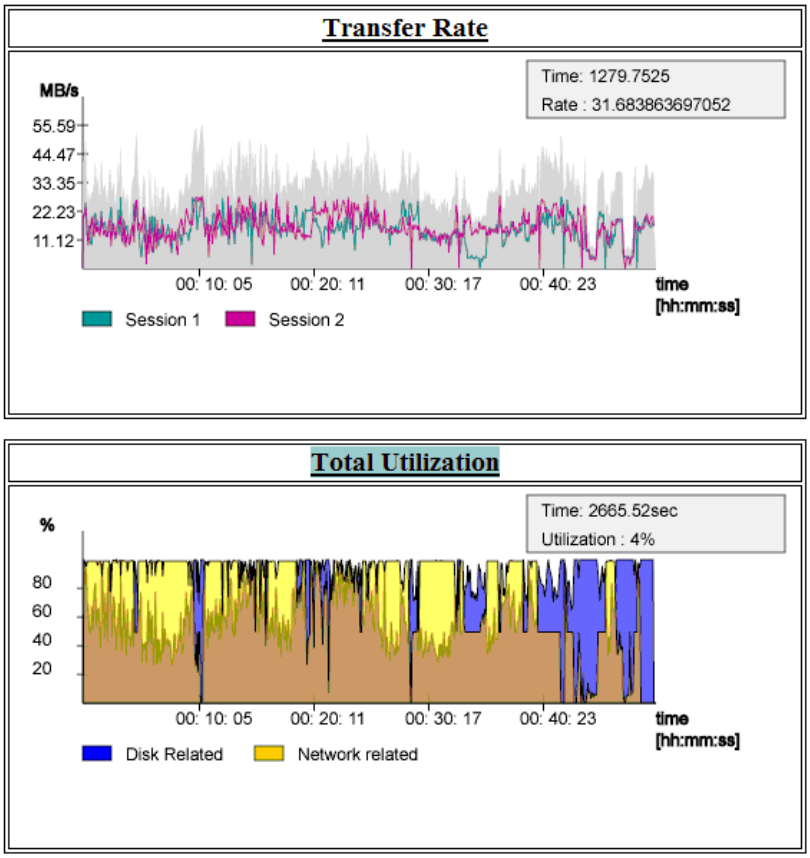


Figure 19. Performance Report - Graphical Presentation Section

Performance-Report

TST (gladiator.boeblingen.de.ibm.com)

System Status: success

Type of run: full , data

Start Date	Start Time	Backup Type	Status	Throughput	End Date	End Time
18.11.2005	22:00:33	full	Success	113.11GB/h	18.11.2005	22:51:02

[...]

Start Time	Filename	Session #	Orig. Filesize	Compr. Rate	Data Rate	Finished At
22:00:22	/oracle/TST/sapdata5/tst_5/tst.data5	2	10485768192 bytes	1.474	55.277GB/h	22:10:58
22:10:58	/oracle/TST/sapdata2/tst_2/tst.data2	2	10485768192 bytes	1.354	60.199GB/h	22:20:42
22:20:42	/oracle/TST/sapdata1/tst_1/tst.data1	2	10485768192 bytes	1.383	68.132GB/h	22:29:18

[...]

Messages

infos: 0 warnings: 0 errors: 0 undefined: 0

Type	Message

Created: 24.11.2005 11:03:06

end of report

Figure 20. Performance Report - Tabular Presentation Section

Reporting on Backup Status

The Administration Assistant function for Data Protection for *SAP*® provides information on the backup status of the monitored SAP® database servers. Administrators access this information by using the Monitor Operations, Monitor Backup Status function. Reports containing status information in tabular form are requested from this panel. The overview information provided in the Monitor Backup States panel is provided in the Status Report.

Status Report

System Status	System ID	Hostname	Conn.Status	DB Type	Date of Backup	Time of Backup	Backup Status	GMT Off.	Group
Success	LUS	lucius.boeblingen.de.ibm.com	offline	oracle	2005.11.23	14:18:16	Success	1	
Failure	TST(0)	radon.boeblingen.de.ibm.com	offline	db2	2005.11.23	18:10:09	Success	1	

Created: 24.11.2005 11:40:10end of report

Figure 21. Status Report

Creating a Report

Consider this information when planning to create a report:

- Reports are requested from the Administration Assistant function for Data Protection for *SAP*® client using the graphical user interface panels that contain the information to be included.
- Reports can also be generated from a scheduling client using a command line interface without any user interaction.
- Each report is produced as an XML file, an HTML file, with possibly one (or more) graphic files in SVG format. The HTML and the SVG files are displayed in the browser.
- All files created can be printed or saved to the local file system using the browser functionality. All reports are temporarily stored for 24 hours on the Administration Assistant server in these subdirectories:

  ```
  <Administration Assistant install dir>/reports/
  <report type>_<time stamp>_<userid>/
  ```

  File system access to the Administration Assistant server is required in order to access reports stored in the report cache.

Reporting on Failed Actions

Information on failed backup operations is provided in the Operations – Failure Report which is accessible from the Monitor Backup States panel. Administrators can choose to include information on failed backups of log files in this report.

Operations-Failure Report

Reported failures between : 2005.11.22 11:41:10 and 2005.11.24 11:40:10

System ID	Hostname	Conn. status	DB Type	Start Date	Start Time	BackupID	Size	Backup Type	Mode	End Date	End Time	Data RC	Control File RC	Catalog File RC
TCT	julius.boeblingen.de.ibm.com	offline	oracle	2005.11.24	06:37:43	A0EGEM5M5X	10987811	full	offline	2005.11.24	06:37:46	2	N/A	N/A
TST(0)	admiral.boeblingen.de.ibm.com	offline	db2	2005.11.23	18:10:09	A0EGDVHN65	110592	restore	restore	2005.11.23	18:10:28	2	N/A	N/A

Created: 24.11.2005 11:41:13

end of report

Figure 22. Operations - Failure Report

Modifying Report Output

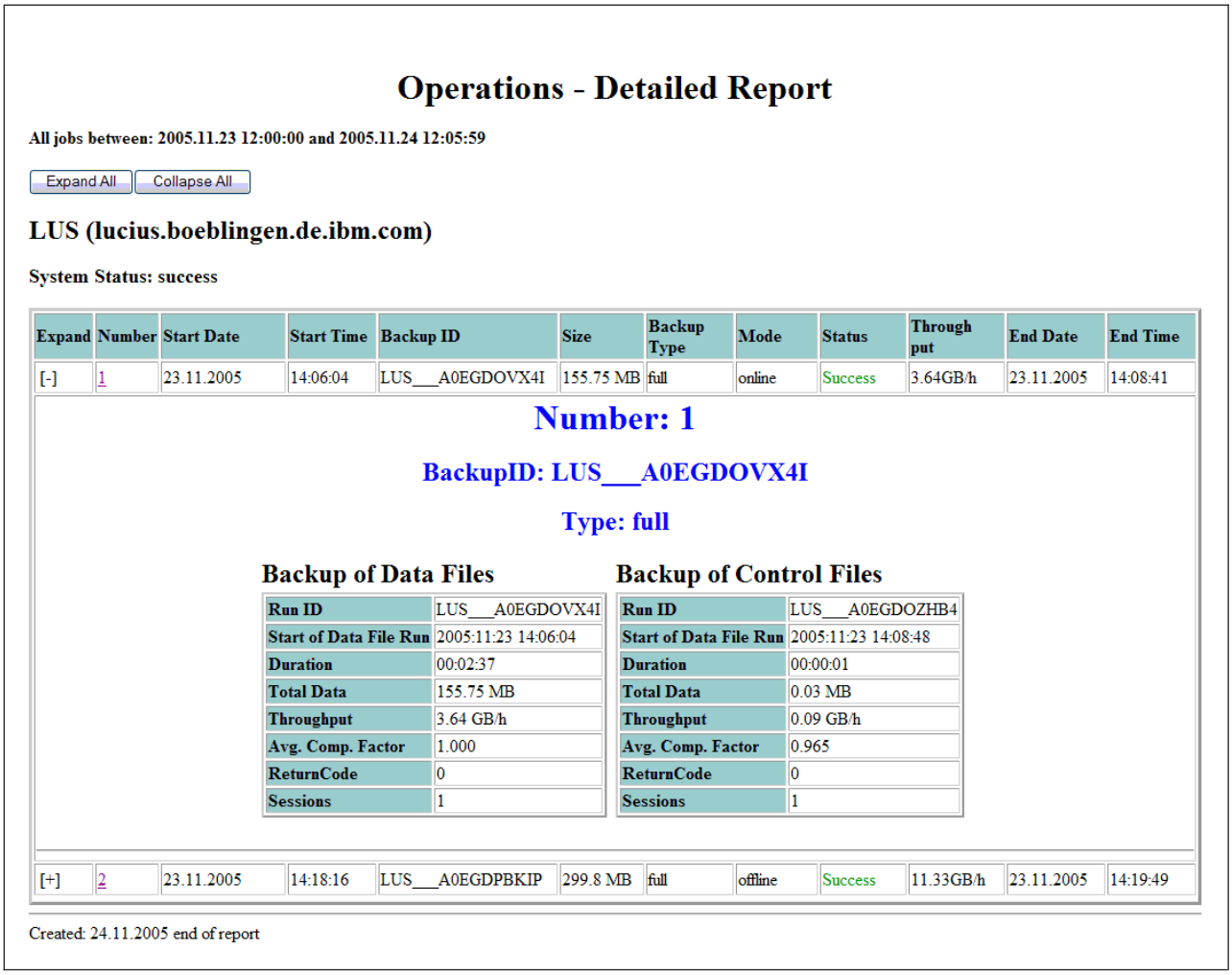
Consider this information when modifying a report:

- All report requests result in the information being written to an XML file. Style sheets (which can be customized) reside with the Administration Assistant function for Data Protection for *SAP*® Server component and are used to generate the information to different types of reports in HTML or SVG format. They determine the appearance and contents of a specific report.
- To generate a report, at least one report-specific style sheet is necessary for the transformation from XML to HTML. If a report contains graphics, each graphic is transformed to an SVG file which requires a separate style sheet. In this scenario, a single report needs a set of style sheets.

- The Administration Assistant provides two types of style sheet file sets. One set is contained in file *Admt.jar* and is used as the default. The second set of style sheets resides on the Administration Assistant server in the `<Admin. Assistant install dir>/styles/` directory.
- Style sheet names must be of the format `<report_name>_<file format>.xsl` where `<file format>` denotes the file type (HTML or SVG) and `<report name>` denotes the name of the file to be created. For example, Picture1_svg.xsl will generate a file named Picture1.svg. Note that the name of the HTML file must always be 'report'.
- The styles directory currently contains four subdirectories (Overview, Detailed, History, Simulation) that specify reports based on different XML data sources as provided in the corresponding Administration Assistant panels Monitor Backup States, Backup State - Detailed View, View Performance Data (History Mode), and Available Simulation Results. The names of these folders are displayed in the list of selectable report types within the Create Report dialogs.
- For every report type, an additional file `config.xml` exists in the styles subdirectory. This file specifies default settings of the Create Reports dialogs. For example, the Operations – Daily Report has a reporting interval of 24 hours. Therefore the end of the time frame does not need to be specified, and the corresponding button will be hidden.
- All style sheets contained either in file `Admt.jar` or in the styles directory are displayed for selection in the Create Report dialogs of the Administration Assistant. Style sheets contained in `Admt.jar` are marked by the addition '(built-in)'.

Reporting on Operations Details

Detailed information on the latest backup operations for a single SID can be obtained with the Operations - Detailed Report requested from the Backup State - Detailed View panel of the Administration Assistant function for Data Protection for *SAP*®. This panel is reached by selecting a single SID in the Monitor Backup States panel.



Operations - Detailed Report

All jobs between: 2005.11.23 12:00:00 and 2005.11.24 12:05:59

Expand All | Collapse All

LUS (lucius.boeblingen.de.ibm.com)

System Status: success

Expand	Number	Start Date	Start Time	Backup ID	Size	Backup Type	Mode	Status	Through put	End Date	End Time
[-]	1	23.11.2005	14:06:04	LUS___A0EGDOVX4I	155.75 MB	full	online	Success	3.64GB/h	23.11.2005	14:08:41

Number: 1

BackupID: LUS___A0EGDOVX4I

Type: full

Backup of Data Files

Run ID	LUS___A0EGDOVX4I
Start of Data File Run	2005:11:23 14:06:04
Duration	00:02:37
Total Data	155.75 MB
Throughput	3.64 GB/h
Avg. Comp. Factor	1.000
ReturnCode	0
Sessions	1

Backup of Control Files

Run ID	LUS___A0EGDOZHB4
Start of Data File Run	2005:11:23 14:08:48
Duration	00:00:01
Total Data	0.03 MB
Throughput	0.09 GB/h
Avg. Comp. Factor	0.965
ReturnCode	0
Sessions	1

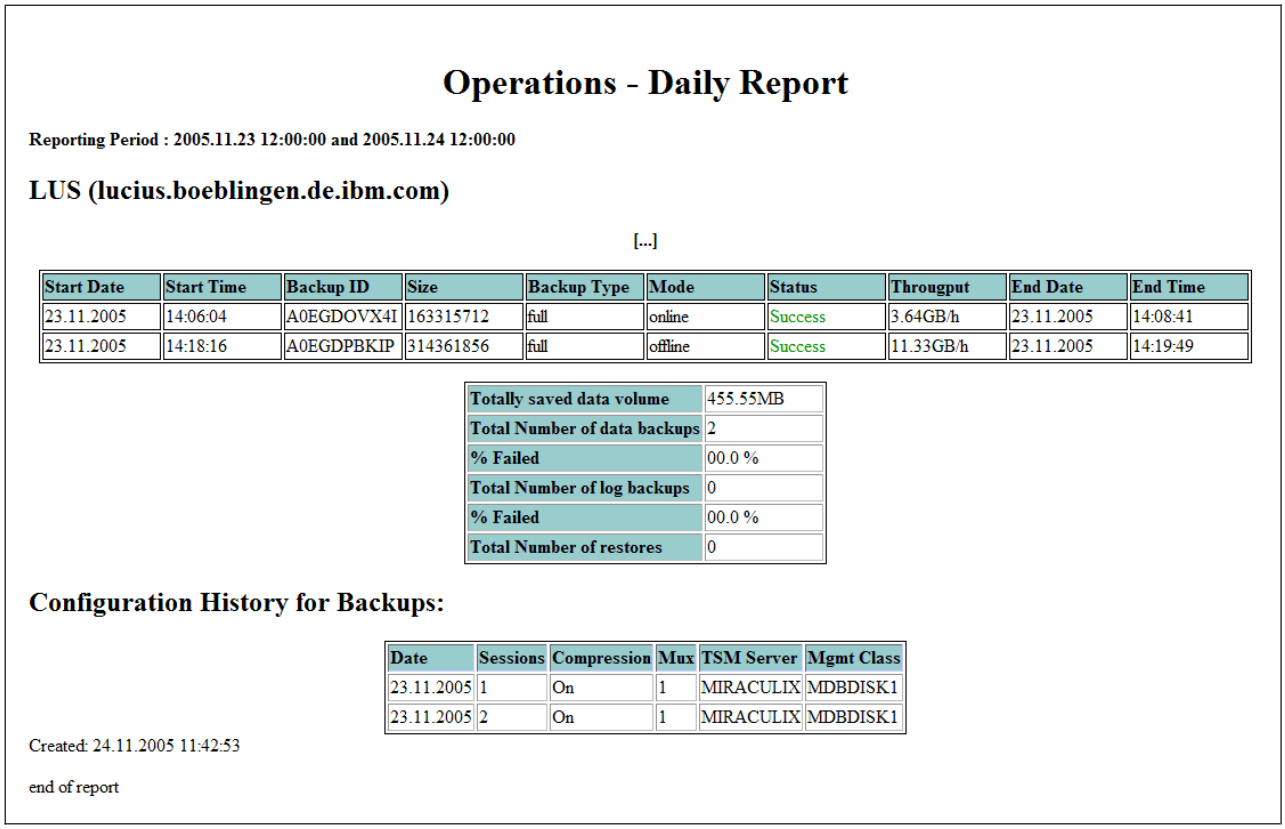
[+]	2	23.11.2005	14:18:16	LUS___A0EGDPBKIP	299.8 MB	full	offline	Success	11.33GB/h	23.11.2005	14:19:49

Created: 24.11.2005 end of report

Figure 23. Operations – Detailed Report

Reporting on Backup Operation Trends

This report type contains general information about the backups of a single SID. Data is represented in graphical and tabular form. A daily report produces a graphic that displays the amount of data saved for a single day. A monthly report produces a graphic that displays the backup duration, amount of data saved, throughput, and log file data for a specified time interval. These reports are requested from the Administration Assistant function for Data Protection for *SAP*® Backup State – Detailed View panel which is accessible by selecting a single SID in the Monitor Backup States panel.



Operations - Daily Report

Reporting Period : 2005.11.23 12:00:00 and 2005.11.24 12:00:00

LUS (lucius.boeblingen.de.ibm.com)

[...]

Start Date	Start Time	Backup ID	Size	Backup Type	Mode	Status	Througput	End Date	End Time
23.11.2005	14:06:04	A0EGDOVX4I	163315712	full	online	Success	3.64GB/h	23.11.2005	14:08:41
23.11.2005	14:18:16	A0EGDPBKIP	314361856	full	offline	Success	11.33GB/h	23.11.2005	14:19:49

Totally saved data volume	455.55MB
Total Number of data backups	2
% Failed	00.0 %
Total Number of log backups	0
% Failed	00.0 %
Total Number of restores	0

Configuration History for Backups:

Date	Sessions	Compression	Mux	TSM Server	Mgmt Class
23.11.2005	1	On	1	MIRACULIX	MDBDISK1
23.11.2005	2	On	1	MIRACULIX	MDBDISK1

Created: 24.11.2005 11:42:53

end of report

Figure 24. Operations Daily Report

Reporting on Data Protection for *SAP®* for Oracle Activities

The Administration Assistant function for Data Protection for *SAP®* obtains, monitors, and administers backup configuration and performance information performed with Data Protection for *SAP®* for Oracle and the corresponding backup status of SAP® database servers. The Administration Assistant Server and Database Agent components collect status, performance, and configuration data from several SAP database servers and retains it for a limited time. Reports can be created in XML or HTML format (or printed) by the Administration Assistant. This is useful when there is no access to the Server component.

Types of Reports

Administration Assistant reports contain the same information that is displayed by the Administration Assistant Monitor Operations, View Performance Data, and Simulate Backup/Restore functions. All information is provided in XML format. In addition, the Administration Assistant provides style sheets used when generating these reports in HTML format:

- Status Report
- Operations - Detailed Report
- Operations - Daily Report
- Operations - Monthly Report
- Operations - Failure Report
- Performance Report
- Simulation Report

All built-in reports are created in English.

Working with Report Templates

A template must be created before a report can be generated without user interaction (for example, using a scheduled script). Templates are created in the same way as reports are requested from the Administration Assistant function for Data Protection for *SAP*® panels. Whenever the Create Report button is used, you are prompted to create a report or use the corresponding template. Each template must be given a unique name which is used when referencing the template. The template is stored in a file with the given name in path `<Administration Assistant install dir>/templates/<userid>/` where `<Administration Assistant install dir>` is the Administration Assistant server installation path. The file extension depends on the type of report requested. A single template can be used to generate reports on several SIDs. Note that a template is owned by the user account that creates it and cannot be accessed from a different account. In order to view, change, or delete owned templates, an administrator can use the Manage templates function in the Administration Assistant View pull-down menu.

Server-related tuning

Alternate Network Paths and Servers

Multiple network paths and multiple backup servers can be used as an alternate instead of in parallel. When the number of available sessions to multiple servers exceeds the number of sessions allowed, Data Protection for *SAP*® for Oracle uses the first sessions it can establish. It continues to use the number of sessions allowed as defined by the MAX_SESSIONS keyword (as described on page "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122). This allows data to be backed up even when a resource (such as a Tivoli Storage Manager server or its network interface) is unavailable. The servers used for the backup must be available in order to restore the data. Note that the days of the week that a server is used can also be specified as described for the USE_AT keyword on page "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122.

Options

Performance Options of Data Protection for *SAP*® for Oracle

These three components have the greatest impact on data transfer rates:

- the type of disks on which the database resides
- the network capabilities accessed by the database host and the Tivoli Storage Manager server
- the type of storage device that contains the backup

Data Protection for *SAP*® for Oracle provides these options to help optimize the data transfer rate for these components.

Parallel (Multiple) Sessions
Data Protection for SAP can back up or restore data to multiple tape drives in parallel. Parallelism is achieved by using more than one session to send data to a backup server. Details are provided in "Multiple Sessions" on page 103.

Multiplexing
Multiplexing simultaneously transfers data from different files through one session (MULTIPLEXING) in order to maximize tape performance. Multiplexing is useful for tape storage since tape drives often have higher

data transfer rates than the disks. Combining multiplexing and parallel sessions can optimize overall backup and restore performance. See the description of the MULTIPLEXING option on page "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122.

Disk Sorting
Data Protection for SAP uses Adaptive File Sequencing during backup processing. This feature sorts database files in sequential order to avoid simultaneously reading files located on the same disk. As a result, to reduce backup processing time is reduced.

Multiple (Parallel) Network Paths and Multiple (Parallel) Servers
Improve performance by configuring Data Protection for SAP to distribute a database backup across two or more Tivoli Storage Manager servers. In addition, you can balance network traffic by providing two (or more) separate network connections between the SAP® database host and the Tivoli Storage Manager server. Detail information regarding these features is available in "Multiple Network Paths" on page 104 and "Multiple Servers" on page 102.

Incremental Backup
Data Protection for SAP supports incremental RMAN backup of a SAP databases. Depending on the system environment, incremental backups might decrease backup processing time.

Individual Tablespace Locking
Data Protection for SAP provides a backup profile parameter (`util_file_online`) that minimizes the number of archived redo logs backed up during online backup operations. This parameter informs the SAP database utilities of the files (and related table spaces) to be backed up. The SAP utilities then switch those table spaces into backup mode. After the files are backed up, the table spaces are released and a new cycle starts. See page "The Data Protection for *SAP*® for Oracle Profile" on page 121 for detailed information.

RL_COMPRESSION
The RL_COMPRESSION profile keyword is compresses a partially filled database. This can result in reduced network traffic and fewer tapes required for backup. See "Compression" on page 98 for complete details.

Adjustments to Data Protection for *SAP*® for Oracle for Improving Performance of Data Transfer

Data Protection for *SAP*® for Oracle is configured (by default) to send uncompressed data to the Tivoli Storage Manager server using a single session.

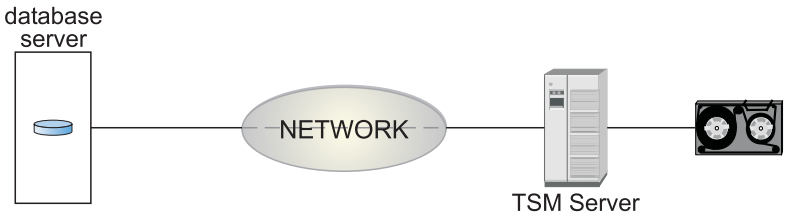


Figure 25. Data Transfer for a Backup / Restore

A single configuration that is best for all environments is not possible or realistic. However, the information provided in this section can help in determining which configuration is best for your environment. The Administration Assistant function

for Data Protection for *SAP*® provides the View Performance Data feature which provides information about performance characteristics and how they change with your configuration. Information about tuning a system with the Administration Assistant is available in "Overview of a balanced system" on page 85.

Buffer Copies

Data Protection for *SAP*® for Oracle uses internal buffers to store and exchange data with Tivoli Storage Manager. When sending data from one component to another, data buffers are copied (by default). Data Protection for SAP can prevent copying the data buffers by sending the original data buffers. This reduces the CPU load of the database server. However, if client compression or client encryption are specified in the Tivoli Storage Manager options file (`dsm.sys` or `dsm.opt` on UNIX or Linux or `<server>.opt` on Windows), the original data buffers are sent. See the description of BUFFCOPY keyword on page "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122 for more information.

Buffer Size

Data Protection for *SAP*® for Oracle allows the size of the internal data buffers to be adjusted. These buffers are used for both reading the disk and sending data to the Tivoli Storage Manager client API. The default values typically produce acceptable performance. It is recommended to optimize the buffer size for disk I/O. For EMC disk subsystems, the best transfer rates have been achieved when the buffer size was set equal to the stripe size. Before increasing the size of internal buffers, however, make sure that sufficient storage is available for the number of buffers specified by Data Protection for SAP. This number correlates to the number of sessions requested. Be aware that number of buffers doubles when compression is specified. See the description of BUFFSIZE keyword on page "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122 for more information.

Compression

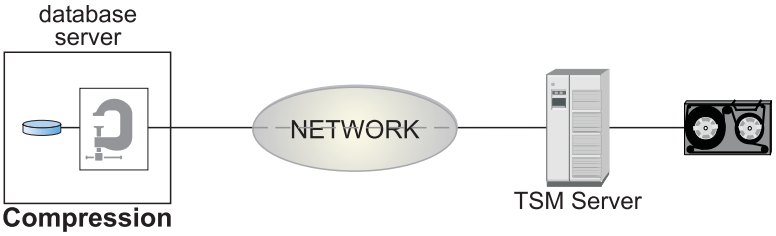


Figure 26. Null Block Compression

Data Protection for *SAP*® for Oracle can decrease the amount of data sent to the Tivoli Storage Manager server by compressing zero-byte blocks. Although compression can increase the CPU load on the database server, it can improve performance in situations when the network is the point of constraint. Compression is most effective with database files that contain large portions of null blocks. See the description of the RL_COMPRESSION keyword on page "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122 for details on how to activate Data Protection for SAP compression.

Automation Options for Data Protection for *SAP®* for Oracle

Administrative productivity can be improved by using these Data Protection for *SAP®* for Oracle automation options.

Selectable Management Classes

Specify different Tivoli Storage Manager management classes for back up data and archive data. It is recommended to configure Data Protection for SAP to back up directly to a tape storage pool and to archive log files to a disk storage pool. Multiple management classes can also be specified to use in conjunction with multiple redo log copies. The profile keywords BRARCHIVEMGTCLASS and BRBACKUPMGTCLASS in "Data Protection for *SAP®* for Oracle profile parameter descriptions" on page 122 provide information about specifying management classes.

Retain Backups by Version

Retaining backups by version limits the number of full backups retained on the Tivoli Storage Manager server. When the number of full backups on the Tivoli Storage Manager server exceeds the value of the MAX_VERSIONS parameter, the oldest versions are deleted. Retaining backups keeps track of all redo log files, database control files, partial and incremental backups, associated with a full backup. All these objects are removed together with the full backup.

Multiple Redo Log Copies

Backing up multiple copies of a log file in a single archive operation helps protect against this data in the event of tape defects or disaster recovery situation. These copies can be located on different physical Tivoli Storage Manager volumes or on different Tivoli Storage Manager servers. When a log file copy is unavailable at restore time, Data Protection for SAP automatically switches to another copy and continues restoring the log file from that copy. The description of the profile keyword REDOLOG_COPIES in "Data Protection for *SAP®* for Oracle profile parameter descriptions" on page 122 provides detailed information about creating and using multiple Redo Log Copies.

Alternate Network Paths and Servers

The availability of backed up data can be improved by configuring Data Protection for SAP to use multiple Tivoli Storage Manager servers or multiple network connections to a single Tivoli Storage Manager server. In this configuration, Data Protection for SAP checks all servers and network connections for availability and then performs the backup even if some resources are unavailable. Policies can also be set that use different Tivoli Storage Manager servers for different days of the week.

Messaging

Policies can be created that enable Data Protection for SAP to send different classes of log messages to the Tivoli Storage Manager server.

Frontend/Backend Processing

Frontend and backend processing calls programs at specified times during backup processing. See the description of the profile keywords BACKEND and

FRONTEND in "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122.

Data transfer

Observations on the Data Protection for *SAP*® for Oracle Data Throughput

Throughput rates differ widely among various environments due to different disk, network bandwidth, server platforms, number of tapes, and configuration settings. The information provided in this section concentrates on selected elements involved in the movement of data. This information should assist in determining how to use existing resources to their maximum efficiency and provide insight as to how throughput can be improved.

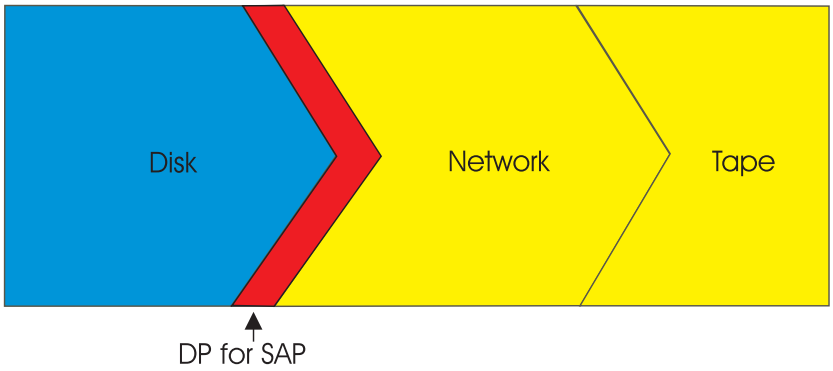


Figure 27. High-level View of the Data Flow During Backup

From a high-level view, the data packages need to send these elements when doing a backup with Data Protection for *SAP*® for Oracle: Data is read from disk, processed by Data Protection for SAP, and sent through the network to tape or disk storage media. If the system is not balanced, the disk I/O, network bandwidth, and storage media rates might create a bottleneck which can cause other resources to remain idle. Overall data throughput is typically measured per file or per entire backup operation. The results are documented as an average throughput rate in a log file. However, identifying bottlenecks based upon log file messages is difficult. To assist in this analysis effort, Data Protection for SAP provides performance sensors that indicate whether there is a bottleneck located either in the elements represented in blue (for disk) or in yellow (for network and tape respectively) in the this graphic. Data Protection for SAP configuration options that can be adjusted to improve performance is described in "Performance Options of Data Protection for *SAP*® for Oracle" on page 96. Additional performance issues are available in "General Performance Considerations" on page 101.

Data Protection for *SAP*® for Oracle Performance Sensors

The method of transferring data packages is based how upon how Tivoli Storage Manager, is configured. In a standard configuration, the data packages are sent from the Tivoli Storage Manager API Client through the network to the backup server. In an environment configured for LAN-free operations, the data packages are processed by the Tivoli Storage Manager API Client and the Tivoli Storage Manager Storage Agent.

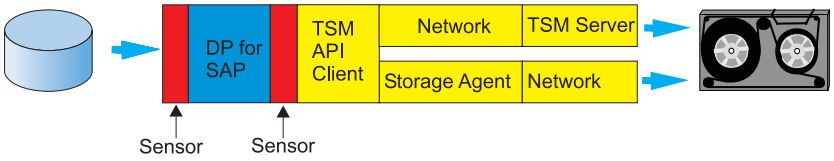


Figure 28. Performance Optimizing by Using Sensors

Data Protection for *SAP*® for Oracle uses sensors that observe incoming and outgoing data streams. They measure throughput and the idle time of the I/O threads in comparison to the duration of the backup. This provides a way to determine whether the streams of incoming and outgoing Data Protection for SAP data are balanced. Be aware that once a backup operation begins, the buffers need to be filled before the effects of a bottleneck are viewable.

General Performance Considerations

Figure 29 on page 102 provides a high level overview of these three main components involved during a Data Protection for *SAP*® for Oracle data transfer:

- The SAP® database server.
- The network.
- The Tivoli Storage Manager server which is also referred to as a backup server.

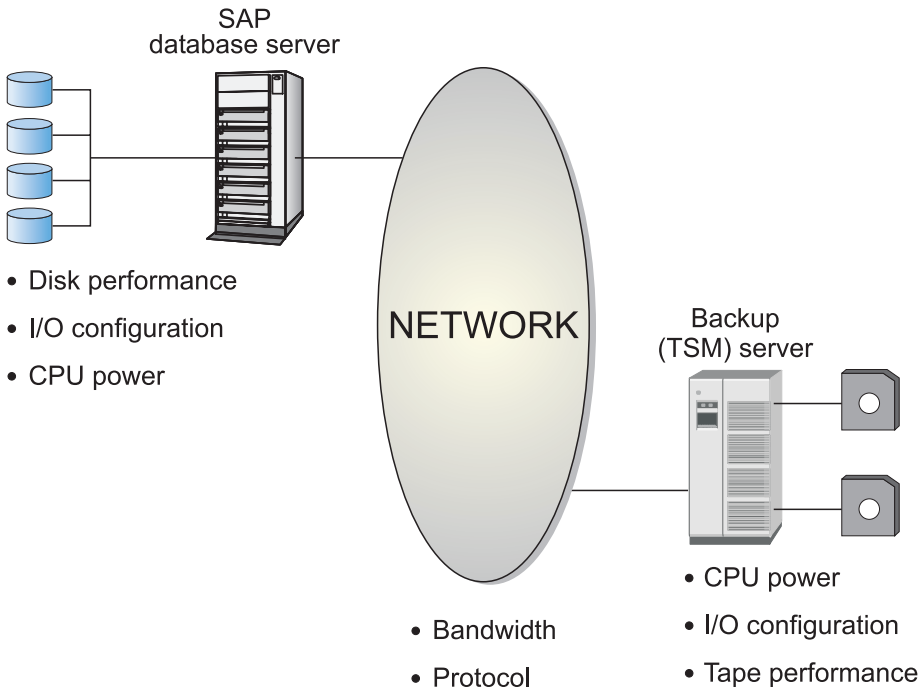


Figure 29. Data Protection for SAP Data Transfer

A continuous stream of data is generated among these components during a backup or restore operation. The weakest component in this stream decreases the overall data transfer rate. The guidelines provided are based on experience gathered from many installations and should be considered when designing a backup/restore infrastructure that will be efficient.

Multiple Servers

Data Protection for *SAP*® for Oracle supports multiple servers which can distribute backup data among two (or more) backup servers. This feature helps eliminate constraints that are frequently encountered among backup servers.

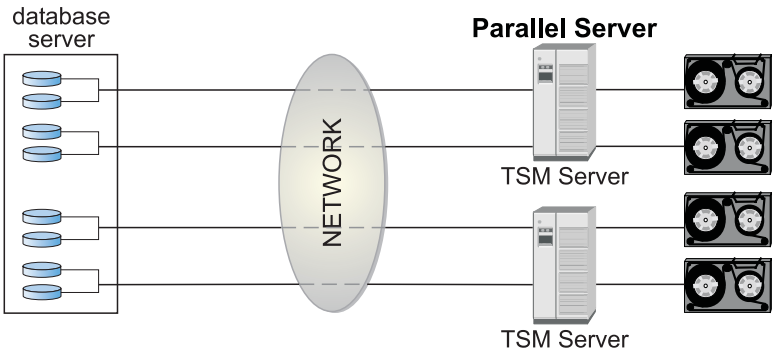


Figure 30. Multiple Servers

A server statement must be entered in the Data Protection for SAP profile for each adapter of the backup server as described for the SERVER keyword in "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122. The value of the MAX_SESSIONS keyword is not greater than the sum of all SESSION values specified for the SERVER statements used concurrently.

When RMAN is used, the number of SESSIONS configured for each SERVER must be greater than or equal to the number of sessions configured for the MAX_SESSIONS keyword specified during restore operations. This prevents RMAN from requesting a number of objects (in parallel from the same server) that exceeds the number of sessions that are available for that server. Detailed information regarding parallel servers is available in "Alternate or parallel backup paths and backup servers" on page 17.

Multiple Sessions

Data Protection for *SAP*® for Oracle allows use of multiple tape drives simultaneously in order to increase the transfer rate to or from the Tivoli Storage Manager server.

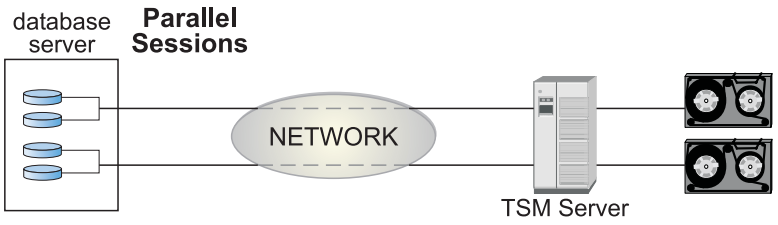


Figure 31. Parallel (Multiple) Sessions

The keywords MAX_SESSIONS, MAX_BACK_SESSIONS, MAX_ARCH_SESSIONS and MAX_RESTORE_SESSIONS are used for defining the number of parallel sessions to be established with the Tivoli Storage Manager server for database backup, archive (backup of log files) and restore. For a detailed description of how to use these keywords,see page "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122. When performing a database backup, the data is typically written directly to tape drives on the Tivoli Storage Manager server. The parameter specified in the MAX_SESSIONS keyword must match the number of tape drives used simultaneously. These must be available to the management class defined as BRBACKUPMGTCLASS in the Data Protection for SAP profile as described on page "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122.

When setting up the Tivoli Storage Manager server, make sure not to activate collocation in the (tape) storage pool defined for the management class chosen as BRBACKUPMGTCLASS. In addition, make sure as many tape drives for this management class are available as the number of sessions defined in MAX_SESSIONS as multiple access to the same tape might slow down data transfer.

When running BRARCHIVE for log file backups, either disk or tape storage pools can be utilized. These must be available to the management class defined as BRARCHIVEMGTCLASS in the Data Protection for SAP profile. If you are using tape pools as (primary) pools for this management class, these considerations for database backups also apply to disk storage pools:

- Several sessions of one BRARCHIVE operation can utilize one or two independent disk storage pool(s).
- Several sessions of BRARCHIVE operations of different databases can simultaneously utilize one or two independent disk storage pool(s).

The number of storage pools required depends on the number of backup copies requested for a log file. See keyword REDOLOG_COPIES in "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122. BRARCHIVE details

are available in "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122.

Multiplexing

Multiplexing is using parallel access to data on the database server. This is recommended when using a tape drive during database backup operations on the backup server.

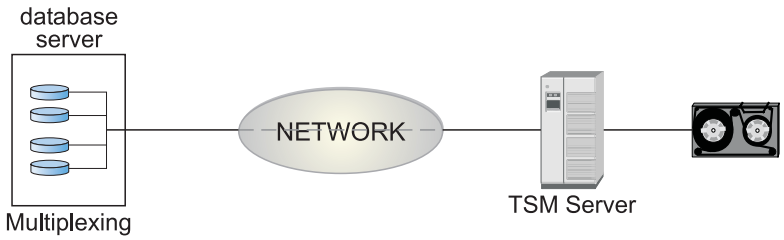


Figure 32. Multiplexing

The value of keyword MULTIPLEXING defines the number of files read in parallel within a single session. Appropriate MULTIPLEXING values are expected in the range of 1 to 4. The best value for your environment depends on the I/O rate of your disks, the location of your data on the disks, the network capacity, the throughput rate of the storage media, and the compression setting. If the MULTIPLEXING value is too high, a thread management overhead may be occur that might offset any performance gain. details regarding this keyword is available on page "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122.

Multiple Network Paths

Data Protection for *SAP*® for Oracle allows you to use multiple network connections (paths) for data transfer between the database server and the backup server.

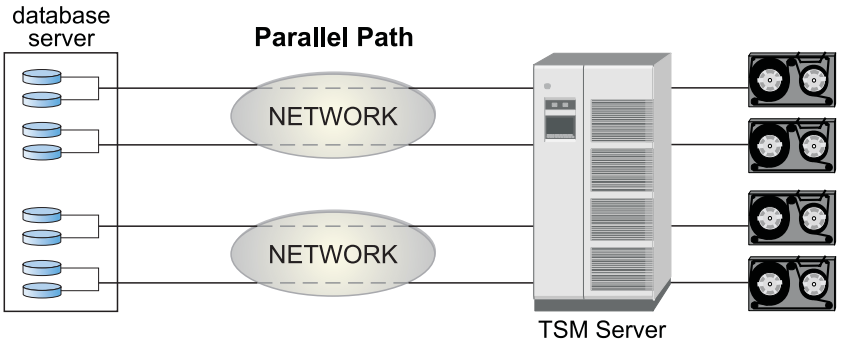


Figure 33. Parallel (Multiple) Paths

Parallel paths can be used to eliminate network points of constraint. For each additional path, additional network adapters are required on both the production and the backup server. A server statement must be entered in the Data Protection for SAP profile for each adapter of the backup server as described for the SERVER keyword on page "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122. The value of the MAX_SESSIONS keyword is not greater than the sum of all SESSION values specified for the SERVER statements

used concurrently. Detailed information regarding setting up multiple parallel network paths is described in detail in “Alternate or parallel backup paths and backup servers” on page 17.

Storage space

Disk Sorting

Data Protection for *SAP*® for Oracle uses Adaptive File Sequencing which attempts to read operations from disks that are truly parallel. For example, when MULTIPLEXING set to 5 and MAX_SESSIONS is set to 3, Data Protection for SAP backs up fifteen files to three tapes. Due to disk sorting, the fifteen files are selected from different disks whenever possible. However, some storage subsystems only provide the information required for disk sorting to users with administrator authority. In such a situation, the administrator can perform a manual sort file to retrieve the locations of the files. See the description of the SORT_FILE keyword on page “Data Protection for *SAP*® for Oracle profile parameter descriptions” on page 122 for more information.

The information required for sorting is determined by the UNIX or Linux createinfo program. Beginning with Data Protection for SAP version 5.4, createinfo is no longer run automatically on UNIX or Linux. due to the wide use of storage subsystems. If performance suffers or you want to retain the previous functionality (because of directly attached disks), this can be achieved by starting the 'prole' process with the 'c' option:

1. As user root, modify the entry in /etc/inittab (add '-c'). For example:

   ```
   .../tivoli/Tivoli Storage Manager/tdp_r3/ora/prole -p tdpr3ora -c ....
   ```

2. Activate the change with 'init q'.

This simplifies, or even eliminates the need for, the start/stop scripts for HACMP™ takeover.

Chapter 8. Troubleshooting Data Protection for *SAP®* for Oracle

Information on how to resolve errors that might occur during Data Protection for *SAP®* for Oracle operations is provided.

Troubleshooting Data Protection for *SAP®* for Oracle common problems

Information on how to resolve errors that might occur during Data Protection for *SAP®* operations is provided.

Random problems

If a problem occurs inconsistently, try to determine what the difference is when the problem occurs, if any. Compare the log files of the application in question (`brbackup / brrestore log`, `sbtio.log`, Tivoli Storage Manager server activity log, etc.) to find out the differences between successful and unsuccessful operations. Look for one of these patterns when the problem occurs:

- The problem always occurs at the same time. If this is true, view the appropriate log files to determine review if there are any scheduled processes occurring simultaneously such as virus checker, automatic updates, or batch jobs.
- The problem always occurs after another operation is performed or the same operation is performed.
- The problem occurs when another application or process is performed in parallel.

Reproducible (repeatable) problems

When encountering a problem that occurs during an operation that has previously performed successfully, consider these possible causes:

- The Data Protection for *SAP®* for Oracle setup changed.
- One (or more) of the Oracle, SAP, Tivoli Storage Manager, operating system, network, or hardware components changed.
- Patches or updates to one (or more) of the components were applied.
- Changes originated by the system have occurred such as these:
  - Check if the disks are running full with the UNIX or Linux® `df` command.
  - If network performance has decreased, check if additional hosts, additional applications, or defects in software or hardware occurred. Compare operation runs in the Administration Assistant Performance Monitor `history view` or compare the `brbackup / brrestore log files`.
  - If Tivoli Storage Manager server processing has decreased, check if additional clients or additional operations were added. Information is also available in the Tivoli Storage Manager server activity log.

When none of these possible causes has occurred, view the last modified time stamp of the configuration files (`init<SID>.utl`, `init<SID>.sap`, `dsm.sys`, `dsm.opt`, `/etc/services`, `/etc/inittab`, ...). This UNIX or Linux command lists all files in the `/etc` directory which have been modified during the previous five days:

```
find /etc -type f -ctime 5 -print
```

If you are able to identify changes made to the system, roll them back one at a time and try to reproduce the problem. This method frequently reveals which change or set of changes caused the problem.

Internet Protocol version 6 (IPv6) support

Data Protection for *SAP*® for Oracle supports both IPv4 and IPv6 for internal communication in that it will run in IPv4, IPv6, and mixed environments on AIX and Linux. However, these products do not exploit new IPv6 functionality. In a mixed environment, the communication depends on the adapter network settings. There is no option to enforce the use of a specific protocol other than by network configuration. Specifically, the ProLE or acsd service will listen for both IPv4 and IPv6 connection requests if the system is configured accordingly. Connection requests to ProLE are made for the addresses returned by the system for the respective port on the local host. Connection requests to other machines such as the Administration Assistant function for Data Protection for *SAP*® are made for the addresses specified by the user. IPv6 addresses are supported when TCP/IP addresses are specified in a command line or in a profile parameter such as TCP_ADDRESS. However, when the IP address and port are specified in the `<IPv4 address>:<service or port>` format, then the format needs to be changed to `<service or port>@<IP address>` if the IP address is specified in the IPv6 notation. In the case of a dotted decimal IPv4 address, the traditional format can still be used.

The specification of IPv6 addresses assumes that Data Protection for SAP is used in an environment in which IPv6 is supported by all hardware and software components involved and has been adequately tested in this environment.

Understanding the setup

Review these considerations to better understand the installation setup on UNIX or Linux systems:

- Make sure all files are installed as described in "Prerequisites" on page 24.
- Make sure an entry similar to this example is defined in the `/etc/inittab` file:

```
po64:2:respawn:/usr/tivoli/tsm/tdp_r3/ora64/prole
-p tdpr3ora64 <Server component hostname> 5126
```

The purpose of this entry is to start a daemon process for ProLE. This process listens on the Data Protection for *SAP*® for Oracle 64-bit port `tdpr3ora64` for backint and RMAN connections and sends performance-related information to the Administration Assistant Server component. The port can have a different name; however, the name must match the name in the /etc/services file as shown in this example `/etc/services` file:

```
tdpr3ora64      57323/tcp
```

These lines are added to the /etc/services file by the installer. The <Server component hostname> specifies the name or IP address of the host on which the Administration Assistant Server component is running. 5126 is the default port to which the Server component listens. These Server arguments are only needed when using the Administration Assistant.

- Make sure the Data Protection for SAP configuration file init<SID>.utl is located in the $ORACLE_HOME/dbs directory.
- When using the BR*Tools, modify the init<SID>.sap file by setting `backup_dev_type = util_file` and variable `util_par_file` to the fully qualified path and file name of init<SID>.utl.

See Figure 34 for an overview of the configuration files on a UNIX or Linux system.

Review these considerations to better understand the installation setup on Windows systems:

- Make sure all files are installed as described in "Prerequisites" on page 24.
- Verify that service `ProLE Service` is running and set to `automatic` startup. If this service is not running, Data Protection for SAP does not function properly.
- The installer adds lines to the %SYSTEMROOT%\system32\drivers\etc\services file similar to these:

```
tdpr3ora64      57323/tcp
```

  `tdpr3ora64` is the Data Protection for SAP 64-bit port. This port name is also needed for the init<SID>.sap file when RMAN is configured.
- Make sure the Data Protection for SAP configuration file init<SID>.utl is located in the %ORACLE_HOME%\database directory.
- When using the BR*Tools, modify the init<SID>.sap file by setting backup_dev_type = util_file and variable util_par_file to the fully qualified path and file name of init<SID>.utl.

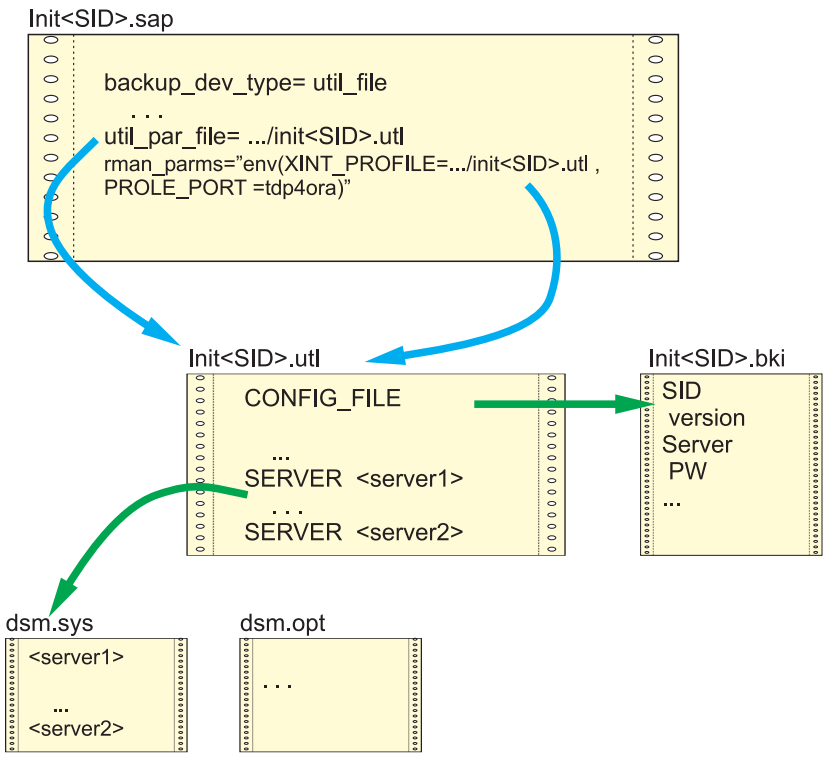


Figure 34. SAP and Data Protection for SAP configuration files on UNIX or Linux

On UNIX or Linux systems, the names of the Tivoli Storage Manager servers specified in init<SID>.utl must match the names in the dsm.sys file. If the Tivoli Storage Manager API or Tivoli Storage Manager Backup Archive Client were installed into their default locations, then the DSMI_* variables do not need to be set. If the variables are set, however, make sure they specify the correct directories and files. The user ID that runs the backups must have the correct permissions to access all of files and directories specified by these variables. Also verify that write permissions exist for the init<SID>.bki file as this is the only file to which Data Protection for SAP writes persistent information.

On Windows systems, the dsm.opt file is used instead of the dsm.sys file. However, the content of this file is not relevant to Data Protection for SAP. The directory that contains the dsm.opt file must also contain a <server>.opt file for each server specified in the init<SID>.utl file. The environment variable DSMI_CONFIG must specify an option file within this directory. DSMI_CONFIG should specify the dsm.opt file in this directory. The DSMI_DIR environment variable must also specify the directory where the dscamen.txt file resides. This is typically the c:\Program Files\Tivoli\tsm\api directory.

Providing information to IBM or Tivoli support

Provide this information when contacting IBM or Tivoli support:

- The Data Protection for *SAP*® for Oracle version.
- The operating system level (including 32- or 64-bit) and patches that were applied.
- The Oracle version (including 32- or 64-bit)
- The Tivoli Storage Manager server version.
- The Tivoli Storage Manager server operating system level.
- Data Protection for SAP configuration file (initSID.utl)including Tivoli Storage Manager client configuration files (dsm.sys, dsm.opt)
- Data Protection for SAP profile (`initSID.utl`)
- BR*Tools output for the operation in question (`brarchive`, `brrestore`)
- The change history of the system components (if the process worked previously).

Additional information might also be requested from the service representative.

Troubleshooting Data Protection for *SAP*® for Oracle problems

Information on how to resolve errors that might occur during Data Protection for *SAP*® for Oracle operations is provided.

Location of log files

Text displayed on the screen during `brbackup`, `brrestore`, and SAP® Tools operations are typically written to a log file. Oracle also writes internal operations in the alert log and core files that reside in the directory specified in the Oracle control files, for example $SAPDATA_HOME/saptrace/background/ alert_<SID>.log. Information about how to locate these log files is available in "How to find files containing message output (log files)" on page 155.

Messages

During BR*Tools processing, logs that contain all issued messages are written to paths /oracle/<SID>/sapbackup (for BRBACKUP) or /oracle/<SID>/saparch (for BRARCHIVE). The message prefix indicates the issuing components. Refer to the documentation for the component that issued the message for detailed information. However, the following prefixes are used when employing BR*Tools with Data Protection for *SAP*® for Oracle:

*Table 11. Prefixes when using BR*Tools*

Prefix	Issuing Component
ANS / ANR	Tivoli Storage Manager
BKI	Data Protection for SAP
BR	BR*Tools
ORA	Oracle database kernel
RMAN	RMAN

File Manager

The most important requirement for File Manager is that Data Protection for *SAP*® for Oracle is set up correctly. This is especially true in regard to the backint executable file, as this file must be able to connect to the Tivoli Storage Manager server without errors. If this call fails, the File Manager displays an error message but does not analyze the reason for the failure. To analyze the error, invoke backint manually with the inquire function and check the output for error messages.

BACKINT problem resolution

Figure 35 on page 112 displays how to isolate the problem once the settings performed by the installer are verified. Make sure the BACKINT interface is working correctly before examing the RMAN interface.

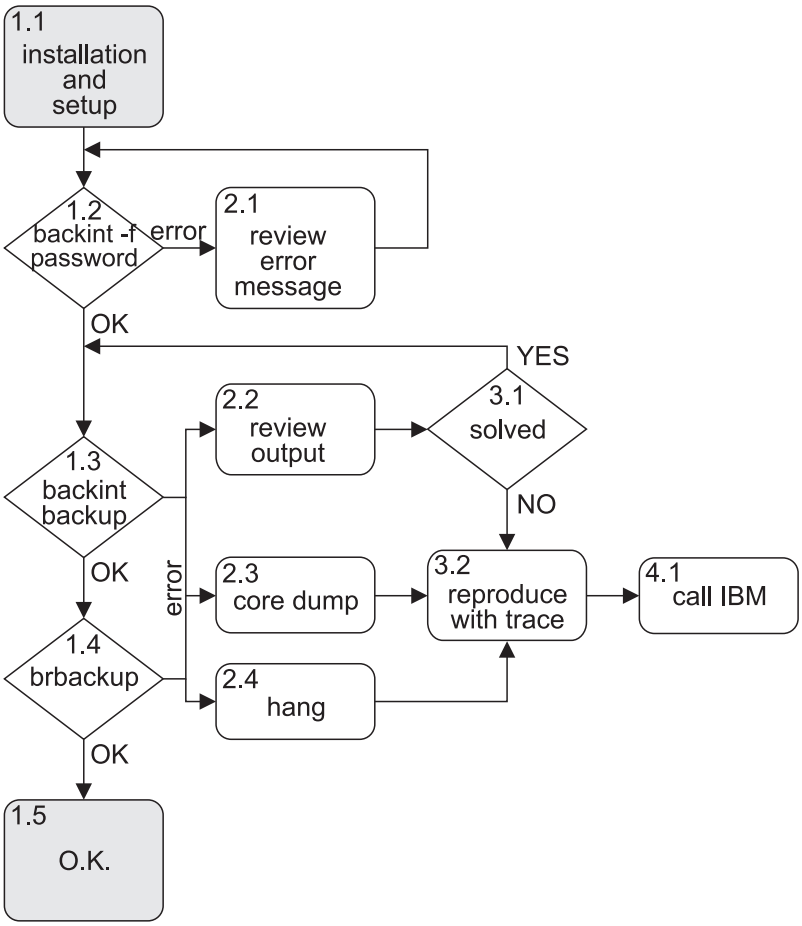


Figure 35. Problem Isolation for Backint

After installation is completed (Step 1.1) and manual password handling is specified, set the password (Step 1.2) as described in "Set the Tivoli Storage Manager password" on page 62. When the operation completes successfully, the informational messages `BKI0051I: Password successfully verified for node <NODENAME> on server <SERVERNAME>` and `BKI0024I: Return code is: 0.` display for each server configured within the init<SID>.utl file. An error message displays when a problem occurred. The Administration Assistant can also be used. The Configurator feature loads the configuration of the node on which problems are encountered and allows the Administration Assistant to check the configuration.

These errors are frequently encountered at Step 1.2:

`BKI2001E: Socket error while connecting to ProLE at <IP-Address>:<PORT>: Connection refused`

On Windows, verify that the ProLE Service is running by viewing the Computer Management Services screen or issue this command:

```
net start
```

A list of all running services displays. On UNIX or Linux, verify that the background daemon is running by issuing this command:

```
ps -ef | grep prole
```

Check the entry in /etc/services (UNIX or Linux) and %SYSTEMROOT%\system32\drivers\etc\services (Windows). Compare the port number from the error message with the port number within /etc/services. Also check the entry in /etc/inittab (UNIX or Linux). If another port was set using the option -p<PORT>, check this as well. If all of this will not help, start the ProLE from another shell on UNIX or Linux with this command:

```
prole -p <PORT>
```

Issue this command on Windows:

```
prole -console -p <PORT>
```

Attempt to start backint again.

BKI5001E: Tivoli Storage Manager Error: Server not found in configuration file
On UNIX or Linux, the Tivoli Storage Manager server defined in the init<SID>.utl file does not match the server specified in the dsm.sys file. On Windows, the <server>.opt file might be missing.

BKI5001E: Tivoli Storage Manager Error: ANS1353E (RC53) Session rejected: Unknown or incorrect ID entered
This message can display when the node in the server stanza of the UTL file is not valid on the server.

HANG If backint hangs after the password is entered, the server IP address specified in the UNIX or Linux dsm.sys file might be incorrect.

When Step 1.2 (setting the password) is successful, proceed to Step 1.3 and perform a backup using backint to verify the settings are correct as described in "Backup function" on page 116. When the backup completes successfully, the message `#SAVED<BID><FILENAME>` displays for each saved file and `BKI0024I: Return code is: 0` also displays. If an error message displays, view the error description in "Data Protection for *SAP*® (Oracle) Messages" on page 155 for information regarding how to resolve it. At this point, the primary Data Protection for *SAP*® for Oracle setup is almost complete. The BR*Tools and Oracle (when using RMAN) must also be configured correctly. Proceed to Step 1.3 and start `brbackup` as described in "Verify the installation" on page 39.

RMAN problem resolution

The following graphic (Figure 36 on page 114) will help you to isolate problems that occur when using RMAN.

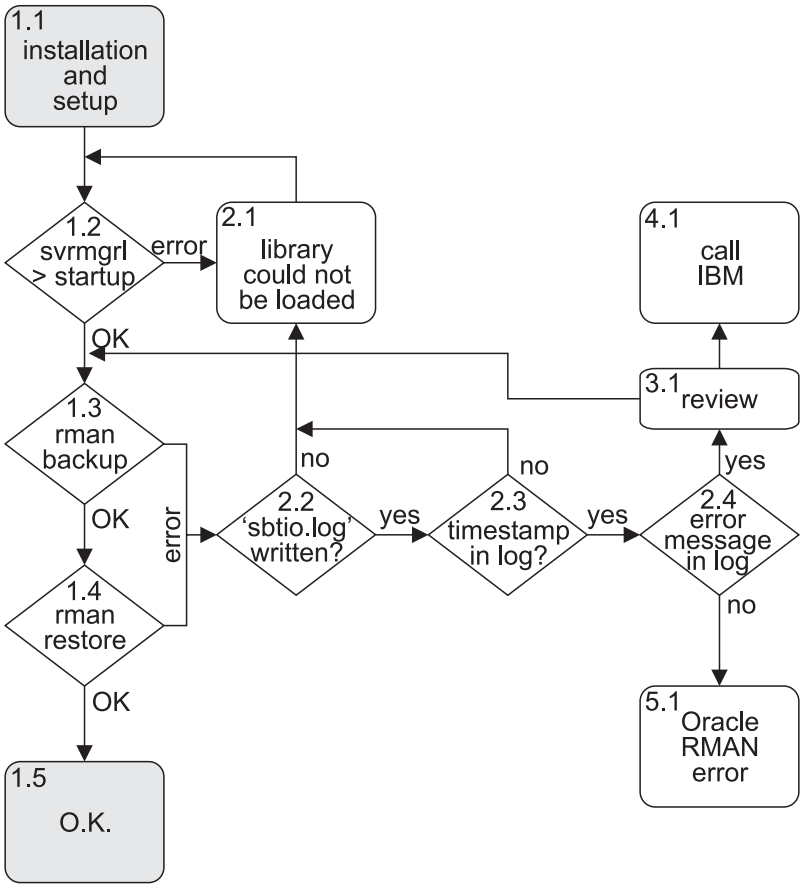


Figure 36. Problem Isolation for RMAN

After Data Protection for *SAP*® for Oracle and Oracle are configured to work together (Step 1.1 in Figure 36), attempt to start Oracle using the server manager `svrmgrl` (on UNIX or Linux) or `svrmgr30` (on Windows) with Oracle 8.x. Use SQL Plus (sqlplus) with Oracle 9.x. When an error occurs while using RMAN, always view the sbtio.log file first. This file is located in the directory specified by the `user_dump_dest` keyword in the Oracle init<SID>.ora profile (located at $ORACLE_HOME/saptrace/usertrace/sbtio.log by default). If the sbtio.log file does not exist (Step 2.2), then either Oracle was unable to load the shared library that contains the RMAN connector for Data Protection for SAP or an error was encountered before the Data Protection for SAP library was called. In both cases, an Oracle error message should exist in the brbackup log file that begins with ORA-, PLS-, or RMAN-. Try to resolve this problem using the Oracle and SAP® documentation. If the sbtio.log file exists, search for a message beginning with `BKI`*`XXXXY`* where *`XXXX`* is a four digit number and *`Y`* is the letter I, W, or E. When such a message occurs, the RMAN connector for Data Protection for SAP loaded correctly and was called by RMAN. This should be the first message for every new session in Step 2.3:

```
BKI7060I: Data Protection for SAP <version and build number> session: 764
```

If this message is not available, Oracle loaded an incorrect library.

Perform these tasks on Windows when an incorrect library is loaded by Oracle:

1. Remove or rename all occurrences of the file orasbt.dll except the one in the Data Protection for SAP installation directory. Then copy this one to %ORACLE_HOME%\bin.
2. Stop the `OracleService<SID>` and restart it.

Several factors must be considered when an incorrect library is loaded by Oracle on UNIX or Linux. For example, the RMAN library `libtdp_r3.<ext>` is not located by the Oracle executable. Oracle suggests to use the SBT_LIBRARY variable to specify the library. However, do not use this variable for a version of Oracle prior to Oracle 9.2. Be aware that Oracle recommends not to issue the `make` command as described in "Required installation tasks" on page 23. However, this recommendation is not applicable for all combinations of operating system and Oracle combinations. As a result, issuing the `make` command on any UNIX or Linux system with Data Protection for SAP is acceptable. When issued correctly, this command can confirm that the library and the Oracle executable are compatible. Also, make sure the library and soft link entered during the command exists and that the soft link is valid:

```
make -f ins_rdbms.mk ioracle LLIBMM=<lib or link>
```

It might be helpful to add the location of the link or library to the LIBPATH environment variable (on AIX) or to the LD_LIBRARY_PATH environment variable (on other UNIX or Linux systems).

On Windows based systems, the location of orasbt.dll must be in the PATH. Also, ensure that you have only one `orasbt.dll` in your system's PATH. It will be helpful as well to review the setup procedure according to "Required installation tasks" on page 23 and the information given in that chapter. Also, check if a core file is written or if Oracle has written a trace within the `saptrace/usertrace` directory.

In (Step 2.4) the file sbtio.log is written and you find an error message starting with BKI see "Data Protection for *SAP*® (Oracle) Messages" on page 155. Using the backint executable file to determine any problems may make it easier because you can see all messages on the screen. Also, you will not disturb Oracle if something goes wrong. If backint is working as expected, return to problem determination with RMAN.

When isolating a problem with Data Protection for SAP and RMAN, you can follow the same steps as in "BACKINT problem resolution" on page 111. There must be a connection established to ProLE and the Tivoli Storage Manager server, and a password must be set (using backint) as well. If some of these steps fail, you will get exactly the same error messages with RMAN as you get with backint. Use "Data Protection for *SAP*® (Oracle) Messages" on page 155 to review these messages.

Manually invoke Data Protection for *SAP*® for Oracle

Information about how to invoke Data Protection for *SAP*® for Oracle from the command line to assist with troubleshooting efforts is provided.

Data Protection for *SAP*® for Oracle is typically invoked by the BR*Tools utilities with a set of appropriate parameters. For troubleshooting purposes, call Data Protection for SAP directly from the command line:

```
backint -?
```

This command displays a list of all possible Data Protection for SAP command line options. It enables you to manually perform data protection operations which can assist with correcting errors. For the C shell, enclose the option string in quotes (`backint '-?'`).

Backup function

Data Protection for *SAP*® for Oracle is typically invoked by the BR*Tools utilities with a set of appropriate parameters. For troubleshooting purposes, call Data Protection for SAP directly from the command line:

```
backint -?
```

This command displays a list of all possible Data Protection for SAP command line options. It enables you to manually perform data protection operations which can assist with correcting errors. For the C shell, enclose the option string in quotes (`backint '-?'`).

The backup function is typically invoked by the SAP® database utilities BRBACKUP and BRARCHIVE. These programs provide an input file (in the case of backup and inquire) to Data Protection for SAP that contain the names and paths of the database files to be processed. For troubleshooting purposes, however, it might be necessary to directly call this Data Protection for SAP function directly in order to back up individual files as shown in these examples. Issue this command on UNIX or Linux systems:

```
backint -p /oracle/SID/dbs/init<SID>.utl -f backup
```

Issue this command on Windows systems:

```
backint -p <drive: or UNC name>\orant\database\init<SID>.utl -f backup
```

The Data Protection for SAP profile `init<SID>.utl` has to be specified with the path and file name statement as shown in the examples. The program prompts you to enter one (or more) file names. Every successful backup operation (collection of one or more files) is allocated its own backup ID within Tivoli Storage Manager. Remember to press CTRL + D (on a UNIX or Linux system) or CTRL + Z (on a Windows system) after the file name to backup has been entered.

Delete function

Data Protection for *SAP*® for Oracle is typically invoked by the BR*Tools utilities with a set of appropriate parameters. For troubleshooting purposes, call Data Protection for SAP directly from the command line:

```
backint -?
```

This command displays a list of all possible Data Protection for SAP command line options. It enables you to manually perform data protection operations which can assist with correcting errors. For the C shell, enclose the option string in quotes (`backint '-?'`).

The delete function is used as part of the Data Protection for SAP version control mechanism and can only be called by Data Protection for SAP or by a user. The

delete function allows you to delete individual files, which might be necessary for recovering from an error. This function can be invoked from the command line as shown in these examples. Issue this command on UNIX or Linux systems:

```
backint -p /oracle/SID/dbs/init<SID>.utl -f delete
```

Issue this command on Windows systems:

```
backint -p <drive: or UNC name>\orant\database\init<SID>.utl -f delete
```

You will be prompted to enter the backup ID and the full file names of the files to be deleted.

Inquire function

Data Protection for *SAP*® for Oracle is typically invoked by the BR*Tools utilities with a set of appropriate parameters. For troubleshooting purposes, call Data Protection for SAP directly from the command line:

```
backint -?
```

This command displays a list of all possible Data Protection for SAP command line options. It enables you to manually perform data protection operations which can assist with correcting errors. For the C shell, enclose the option string in quotes (`backint '-?'`).

The inquire function (typically invoked by BR*Tools and BRRESTORE) is used to query the Tivoli Storage Manager server for backup IDs or files which belong to a particular backup ID. For troubleshooting purposes, however, it might be necessary to invoke this function manually as shown in these examples. Issue this command on UNIX or Linux systems:

```
backint -p /oracle/SID/dbs/init<SID>.utl -f inquire
```

Issue this command on Windows systems:

```
backint -p <drive: or UNC name>\orant\database\init<SID>.utl -f inquire
```

Data Protection for SAP prompts you to enter the inquiry in one of these four formats:

- **#NULL**: Display all backup IDs that have been saved to this point. A typical line of the response could be `#BACKUP JE0___A0DNE9Z74C`. The backup ID in this case is `JE0___A0DNE9Z74C` (`#BACKUP` does not belong to the backup ID). The first six characters are the user defined prefix (see BACKIDPREFIX as described in "Data Protection for *SAP*® for Oracle profile parameter descriptions" on page 122). The next ten characters after this represent a unique ID of the backup.
- **BackupID**: Display all of the files which belong to that backup ID. A typical result could be `##BACKUP JE0___A0DNE9Z74C /oracle/C21/dbs/initC21.utl`.
- **#NULL `filename`**: Display all of the backup IDs corresponding to the specified file. *Filename* requires an input consisting of path and name of the file.

- **BackupID `filename`**: Verify whether a particular file has been saved under a certain backup ID. *Filename* requires an input consisting of path and name of the file.

Restore function

Data Protection for *SAP*® for Oracle is typically invoked by the BR*Tools utilities with a set of appropriate parameters. For troubleshooting purposes, call Data Protection for SAP directly from the command line:

```
backint -?
```

This command displays a list of all possible Data Protection for SAP command line options. It enables you to manually perform data protection operations which can assist with correcting errors. For the C shell, enclose the option string in quotes (`backint '-?'`).

The restore function is typically started by the SAP® database utility BRRESTORE. For troubleshooting purposes, however, it might be necessary to directly call this Data Protection for SAP function directly in order to restore individual files as shown in these examples. Issue this command on UNIX or Linux systems:

```
backint -p /oracle/SID/dbs/init<SID>.utl -f restore
```

Issue this command on Windows systems:

```
backint -p <drive: or UNC name>\orant\database\init<SID>.utl -f restore
```

You will be prompted to enter the backup ID and the full file names of the files to be restored. If the files are to be restored to another directory, it is necessary to specify the path to the input files. If a file is restored directly, any existing file with the same name will be overwritten without warning. Thus, it is recommended that you restore database files directly only in a very controlled manner, when it is absolutely necessary in order to remove an error. In normal operation, a database should never be restored directly because this could corrupt the SAP database.

Chapter 9. Data Protection for *SAP®* for Oracle reference information

Data Protection for *SAP®* for Oracle reference information provided.

Commands used with Data Protection for *SAP®* for Oracle

A list of various commands that are used with Data Protection for *SAP®* for Oracle operations is provided.

Cooperation of Data Protection for *SAP®* for Oracle with BRARCHIVE

BR*Tools are a collection of utilities that simplify Oracle database system administration within an SAP environment. Details regarding setting up and using BR*Tools is available in SAP® documentation such as the *SAP Database Guide: Oracle*.

BRARCHIVE backs up redo logs. To save each redo log to Tivoli Storage Manager, BRARCHIVE calls Data Protection for *SAP®* for Oracle either through the BACKINT interface or through RMAN. BRARCHIVE maintains a list of redo logs to be saved. Redo logs that were successfully saved by Data Protection for SAP may be deleted from the file system immediately by BRARCHIVE. However, BRARCHIVE deletes redo log files only in the order of the list. As a result, if the requested number of backup copies cannot be saved for a redo log, this redo log and all subsequent redo logs are maintained. When BRARCHIVE starts again, these redo logs are saved again even if some were successfully saved earlier. Data Protection for SAP informs BRARCHIVE about the redo logs that were saved successfully to Tivoli Storage Manager. If a problem occurs, Data Protection for SAP makes several attempts to save the redo log. When a redo log cannot be saved to the number of copies requested, Data Protection for SAP terminates with an error. Data Protection for SAP does not try to save redo logs with a higher sequence number because they will be saved in a later BRARCHIVE run.

Managing Tivoli Storage Manager Sessions

When redo logs are saved directly to a tape pool, the number of Tivoli Storage Manager sessions must not exceed the number of available tape drives. Be aware that BRARCHIVE might process redo logs while a database backup is still processing or several BRARCHIVE processes may run simultaneously. As a result, these combined sessions might exceed the number of available tape drives. To avoid this situation, save redo logs to disk storage pools and eventually have Tivoli Storage Manager migrate them to tape storage.

Versioning

When Data Protection for *SAP*® for Oracle versioning is active (as defined by the MAX_VERSIONS keyword), versioning information is kept in the `init<SID>.bki` configuration file. The version number is increased only after successful backups. Therefore, using the same `init.bki` configuration file for both backing up the database (BRBACKUP) and the redo logs (BRARCHIVE) is necessary in order to avoid the unexpected loss of redo log backups.

UNIX or Linux Crontab Example

UNIX or Linux cron jobs can be scheduled with the `crontab` command. This command launches an editing session that allows you to create a crontab file. The cron jobs and the appropriate times are defined within the crontab. The crontab can be customized with this command:

```
crontab -e
```

In this example, a cron job starts the shell script `backup.ksh` at 11:30 p.m. Monday through Friday and uses the SAP® database utility BRBACKUP to back up the SAP® database. This is the entry in the crontab that starts the script for this scenario:

```
30 23 * * 1,2,3,4,5 /usr/bin/su - ora<SID> -c "/oracle/SID/sapscripts/backup.ksh"
```

The content of `backup.ksh` is available in "Full Offline Backup Shell Script Sample" on page 70.

Crontab File Sample

```
# ------------------------------------------------------------------------
# crontab.sample:
# Sample crontab file to be included in the root crontab jobs.
# ------------------------------------------------------------------------
# Task:
# Submits backup/archive commands at regularly scheduled intervals
# using two simple shell scripts containing SAP backup/archive commands.
# ------------------------------------------------------------------------
#      *****     NOTE     *****     NOTE     *****     NOTE     *****
#
#          This file is intended only as a model and should be
#          carefully tailored to the needs of the specific site.
#
#      *****     NOTE     *****     NOTE     *****     NOTE     *****
# ------------------------------------------------------------------------
#
# Remarks on the crontab file format:
#
# Each crontab file entry consists of a line with six fields, separated
# by spaces and tabs, that contain, respectively:
#   o The minute (0 through 59)
#   o The hour (0 through 23)
#   o The day of the month (1 through 31)
#   o The month of the year (1 through 12)
#   o The day of the week (0 through 6 for Sunday through Saturday)
#   o The shell command
# Each of these fields can contain the following:
#   o A number in the specified range
#   o Two numbers separated by a dash to indicate an inclusive range
#   o A list of numbers separated by commas
```

```
#   o An * (asterisk); meaning all allowed values
#
# ------------------------------------------------------------------------
#
# For the following examples, the system id of the ORACLE database
# is assumed to be 'C11' and the username 'oraC11'.
#
# ------------------------------------------------------------------------
# Full database backup, scheduled every Friday at 8:00 p.m.
#
0  20    * * 5
# /usr/bin/su - oraC11 -c "/oracle/C11/sapscripts/backup/backup.ksh"
#
# ------------------------------------------------------------------------
# Save redo logs, scheduled twice a day at 11:30 a.m. and at 5:30 p.m.
# Monday through Friday
#
30 11,17 * * 1,2,3,4,5
/usr/bin/su - oraC11 -c "/oracle/C11/sapscripts/backup/archive.ksh"
```

The Data Protection for *SAP®* for Oracle Profile

The Data Protection for *SAP®* for Oracle profile provides keyword parameters that customize how Data Protection for SAP operates. A sample profile initSID.utl is provided on the product media. During installation on Windows systems, the sample profile (along with all other files) is placed in the `C:\Program Files\Tivoli\TDP4SAP` directory.

During installation on UNIX and Linux systems, this file is copied and renamed to `$ORACLE_HOME/dbs/init$ORACLE_SID.utl`, where *$ORACLE_HOME* is the Oracle home directory and *$ORACLE_SID* is the Oracle System ID (for example, `/oracle/<SID>/dbs/init<SID>.utl`).

These rules apply to the keyword syntax:

- Each line is analyzed separately.
- Keywords can start in any column of the line.
- Keywords must not be preceded by any string, except blanks.
- If a keyword is encountered several times, the last one is used.
- File processing ends when the *END* keyword is encountered or the end of file is reached.
- The comment symbol is the pound sign (#). Scanning of the current line stops when the comment symbol is encountered. No comment is allowed between the keyword and the value(s). For example:

```
#BRARCHIVEMGTCLASS   MLOG1                  <--  correct
BRARCHIVEMGTCLASS    MLOG1  #               <--  correct
BRARCHIVEMGTCLASS  # MLOG1                  <--  incorrect
```

- Although some keywords are required, most are optional. Each of the optional keywords has a preset default value.
- The `backint` program on Windows systems accepts the value of the profile name ('-p' option) in Universal Naming Convention (UNC) format as shown here : `\\SERVER_A\profiles\init<SID>.utl`. However, any file specifications within the profile must use the `drive:path` syntax.
- Additional profile information is provided in "Enable ProLE to access configuration files on a remote share" on page 30.

Data Protection for *SAP®* for Oracle profile parameter descriptions

The default value is underlined in these descriptions and applies if the parameter is not specified.

ADSMNODE *ORACLE_sid*
Specifies an *ORACLE_sid* that is registered to the Tivoli Storage Manager server as a Tivoli Storage Manager node. This parameter must be defined in conjunction with the respective SERVER statement, as shown in the sample profile. You can assign a different node name to your database system with this option. It should be used if you have several SAP® for Oracle database systems in your network with the same name, for example, <SID>, and they all use the same Tivoli Storage Manager server. This keyword must not be set when automated password handling is selected. It should be set for manual password handling as described in "7. Determine the Tivoli Storage Manager password method" on page 61.

BACKEND *pgmname [parameterlist]*
Specifies a program *pgmname* that is called by Data Protection for *SAP®* for Oracle after the backup function has completed and before program control is returned to the SAP backup utility. If *pgmname* is not fully qualified, the default search path is used to find the program. If not specified, no backend processing is done.

Example for UNIX or Linux:

```
BACKEND write operator@remotesite Backup of SAP database object completed.
```

This sends a message to a remote user when the backup has finished.

BACKUPIDPREFIX *6-charstring* | **SAP___**
Specifies a six-character prefix that is used to create a backup identifier for each archived object.

BATCH YES|NO
Specify NO if Data Protection for SAP is running with an operator standing by. Specify YES if Data Protection for SAP is running in unattended mode. In unattended mode, Data Protection for SAP terminates the run if operator intervention is required. The default for the BATCH parameter is YES for the backup run and NO for the restore run if the BATCH parameter is not present or is commented out in the Data Protection for SAP profile. This parameter has no effect if an RMAN backup or restore is started.

BRARCHIVEMGTCLASS *management_class [management_class...]*
Specifies the Tivoli Storage Manager management class(es) that Data Protection for SAP uses when called from BRARCHIVE. Each parameter string can consist of up to thirty characters. Specify a separate BRARCHIVEMGTCLASS for each log file copy requested. As a result, make sure the number of different BRARCHIVE management classes specified must be greater than or equal to the number of redo log copies (keyword REDOLOG_COPIES on page "Data Protection for *SAP®* for Oracle profile parameter descriptions." This parameter must be defined in conjunction with the respective SERVER statement, as shown in the sample profile.For more detailed information about implementing and using BRARCHIVEMGTCLASS see "Cooperation of Data Protection for *SAP®* for Oracle with BRARCHIVE" on page 119.

To use different TSM servers for backup and archive data, the value ':SKIP:' can be used to define a server stanza with no archive management classes. This value is allowed for the parameter BRARCHIVEMGTCLASS only.

BRBACKUPMGTCLASS *management_class [management_class...]*
Specifies the Tivoli Storage Manager management class(es) Data Protection for SAP uses when called using BRBACKUP. The parameter string can consist of up to thirty characters. This parameter must be defined in conjunction with the respective SERVER statement, as shown in the sample profile.

BUFFCOPY SIMPLE | PREVENT | AUTO
This optional parameter controls how Data Protection for SAP uses the internal buffers for transferring data during a backup. If set to SIMPLE, data buffers are copied when they are sent between Tivoli Storage Manager components. This is the default. If set to PREVENT, the original data buffers are sent between Tivoli Storage Manager components. For this mode, BUFFSIZE is restricted to a maximum of 896 KB. Furthermore, it cannot be selected when the Tivoli Storage Manager client encryption or client compression features are activated. If set to AUTO, Data Protection for SAP will run in PREVENT mode whenever the configuration supports it. Otherwise, SIMPLE mode is automatically selected. This parameter has no effect on restore operations.

BUFFSIZE *n* **| 131072**
This parameter specifies the block size (in bytes) for the buffers used for disk I/O. The size of the buffers sent to the Tivoli Storage Manager API is the value of BUFFSIZE increased by approximately 20 bytes. The valid range is from 4096 (4 KB) to 32 MB. Inappropriate values are adjusted automatically. If BUFFCOPY is set to PREVENT, the value of BUFFSIZE must not exceed 896 KB. If not specified, the default value is 131072 (128 KB) for UNIX or Linux systems and 32768 (32 KB) for Windows systems. In most cases, these values are appropriate. If you plan to increase the size of internal buffers, make sure that sufficient storage is available. The number of buffers acquired by Data Protection for SAP correlates to the number of files multiplexed in a data stream (keyword MULTIPLEXING) multiplied by the number of sessions (keyword SESSIONS). By activating RL_COMPRESSION, the number of buffers is doubled.

COMPR_INFO *path*
Specifies the file where Data Protection for SAP stores information about the compressed size of files. The *path* value specifies the full path and name of the file. When multiplexing is used, Data Protection for SAP attempts to optimize performance by putting files of the same size in one multiplexing stream. If RL_COMPRESSION is used in addition to multiplexing, the file sizes of the compressed files can differ very much from the original file sizes. Data Protection for SAP can collect information about the compressed file sizes and use it for further file sorting. This file size information is stored in the file specified by the COMPR_INFO parameter. If backups shall serve as a basis for simulations (see "Simulating Backup and Restore" on page 80), COMPR_INFO must denote a valid file and RL_COMPRESSION must be set to YES in order to get meaningful simulation results for compression. When the parameter RL_COMPRESSION is set to NO, this parameter has no effect. If specified, the information file is written after each backup and the information is

used by the following backups and simulations. If there is no compression information about a file because of a database extension, the uncompressed file size is used for file sorting.

CONFIG_FILE *<path>/init<SID>.bki*
Specifies the configuration file `init<SID>.bki` for Data Protection for SAP to store all variable parameters such as passwords, date of last password change, and the current version number. A single CONFIG_FILE should never be shared among multiple database instances or partitions or backup version control might not function correctly. This parameter is required.

END Specifies the end of the parameter definitions. Data Protection for SAP stops searching the file for keywords when END is encountered.

EXITONERROR YES | NO | *n*
This keyword specifies whether or not Data Protection for SAP exits on a backup or restore error during a BRBACKUP/BRRESTORE run. NO means do not exit if an error occurs. YES means exit if one file cannot be backed up. If a number is specified as an argument, Data Protection for SAP counts the number of errors (not warnings or retries) and exits after the specified number of errors. This keyword works only for the BRBACKUP/BRRESTORE runs. BRARCHIVE and RMAN runs always exit after the first error. This parameter is ignored if the BATCH parameter is set to NO.

FCS_FILE *path*
Specifies the profile for Data Protection for Snapshot Devices version 5.4. If Data Protection for SAP and Data Protection for Snapshot Devices version 5.4 are used together, this parameter is required. See the Data Protection for Snapshot Devices documentation for details. For a stand-alone installation of Data Protection for SAP, this parameter must not be used.

FILE_RETRIES *n* | **3**
This parameter specifies the number of retries when a file could not be saved or restored. This parameter has no effect if an RMAN backup/restore is started.

FRONTEND *pgmname [parameterlist]*
Specifies a program *pgmname* that is called by Data Protection for SAP in a backup run before the connection to the Tivoli Storage Manager server is established. If *pgmname* is not a fully qualified path, the default search path is used to find the program. If not specified, no frontend processing is not performed.

Example for UNIX or Linux:

```
FRONTEND write operator@remotesite Backup of SAP database
object is starting.
```

This sends a message to a remote user before backup begins.

LOG_SERVER *servername [verbosity]*
The *servername* value specifies the name of the Tivoli Storage Manager server to which log messages are sent. The *servername* must match one of the servers listed in a SERVER statement in order for Data Protection for SAP messages to be logged in the Tivoli Storage Manager server activity log. The *verbosity* value can be one of these specifications: ERROR, WARNING, or DETAIL. This value determines which messages are sent. The default value is WARNING, which means that error and warning messages are sent. ERROR sends only error messages. DETAIL sends all message types (errors, warnings, and informational messages). If there is

no LOG_SERVER statement in the profile, log messages are not sent to any of the Tivoli Storage Manager servers.

MAX_SESSIONS *n* | **1**
Specifies the maximum number of parallel Tivoli Storage Manager client sessions that Data Protection for SAP establishes for backup, archive (redo logs) and restore. Each session transfers one database object or, in the case of an RMAN backup or restore, a set of data blocks to or from the Tivoli Storage Manager server by using the Tivoli Storage Manager API client functions. This keyword is required. Data Protection for SAP optimizes the data transfer with regard to the physical location of the Oracle objects. Files stored on different volumes are backed up in parallel if multiple sessions are configured. A maximum of 32 parallel sessions may be configured. For a direct backup or restore on tape drives, the number of sessions must be less than or equal to the number of tape drives available for the backup. Make sure that the `mountlimit (mountl)` parameter in the device class is set to the number of available tape drives. Make sure that the `maxnummp` parameter of the node is set to the number of available tape drives. The value of keyword MAX_SESSIONS must be less than or equal to the sum of the SESSIONS values specified in the SERVER statements of the currently available servers. For more detailed information about implementing and using MAX_SESSIONS see "Cooperation of Data Protection for *SAP*® for Oracle with BRARCHIVE" on page 119.

MAX_ARCH_SESSIONS, MAX_BACK_SESSIONS, MAX_RESTORE_SESSIONS, MAX_CONTROL_SESSIONS
These parameters provide the same function as the MAX_SESSIONS parameter but they also provide a more specific use:

- MAX_ARCH_SESSIONS defines the number of parallel sessions used for archive (backup of log files). Usually archive does not need as many sessions as (data file) backups since the volume is much smaller with log files. This value overrides the value of MAX_SESSIONS for the backup of database files.
- MAX_BACK_SESSION defines the number of parallel sessions used for (data file) backup. This value overwrites the value of MAX_SESSIONS for the backup of database files.
- MAX_CONTROL_SESSIONS defines the number of parallel sessions used for backing up the control files after a database or redo log backup. If MAX_CONTROL_SESSIONS is not specified the number of sessions used for the control file backup is the same as for the corresponding database or redo log backup. Typically, for a control file backup, the number of sessions can be reduced in order to avoid unnecessary tape mounts. This value overwrites the value of MAX_ARCH_SESSIONS or MAX_BACK_SESSIONS for the backup of control files.
- MAX_RESTORE_SESSIONS defines the number of parallel sessions used for restore. For restore, more tape drives may be available than for backup. Using additional tape drives may speed up the data transfer for restore if the backup was written to a sufficiently large number of tapes. This value overwrites the value of MAX_SESSIONS for restore.

If MAX_SESSIONS is specified with one or more of these parameters, these specific parameters override the MAX_SESSIONS parameter. You must specify them all if you do not specify the MAX_SESSIONS parameter. For the valid range as well as the rules, refer to keyword MAX_SESSIONS.

MAX_VERSIONS *n* | **0**
The *n* value defines the maximum number of full database backup

versions to be kept in backup storage. The default setting for this value is 0, meaning that backup version control is disabled. If the number of versions found in backup storage is larger than the specified maximum number of backup versions (as specified by the parameter MAX_VERSIONS), the oldest versions are deleted (together with the corresponding tablespace and redo log files) until only the specified maximum number of most recent versions remain. Also, consider these characteristics:

- When Data Protection for SAP deletes an old full backup, all partial backups older than this full backup are also deleted.
- If the backups are distributed over multiple TSM servers and one of the servers is temporarily unavailable at the time of a new full backup, it will not be possible to find all the backup versions. This may result in retaining a backup that would otherwise have been deleted.

Tivoli Storage Manager uses the value of the RETVER parameter (specified when defining a copy group) to give files an expiration date. Use only one of these methods to control how long you keep backups:

- If you use Data Protection for SAP backup version control, you need to bypass this expiration function. Set the Tivoli Storage Manager parameter RETVER=9999 so that the files are not considered expired and are not deleted by Tivoli Storage Manager.
- If you use the Tivoli Storage Manager expiration function, you need to turn off Data Protection for SAP backup version control. Deactivate Data Protection for SAP backup version control by setting MAX_VERSIONS=0.

Information about defining a copy group is available in "4. Define a policy" on page 59.

MULTIPLEXING *n* | **1**

Specifies the number of files which are multiplexed into one data stream. The allowed range is from 1 to 8. The optimal value depends on the actual hardware environment. Multiplexing is most effective when fast tape access exists, fast networks are available, database files are compressed, and the CPU load is moderate. Optimal values are in the range from 1 to 4. If not specified, the default value of 1 means multiplexing is not used. This parameter has no effect if an RMAN backup or restore operation is started.

PASSWORDREQUIRED NO | YES

Specifies whether Tivoli Storage Manager requires a password to be supplied by the Tivoli Storage Manager client. This depends on the Tivoli Storage Manager installation. If not specified, the default is PASSWORDREQUIRED YES which implements manual password handling. This parameter must be defined in conjunction with the respective SERVER statement, as shown in the sample profile. Further details are described in "7. Determine the Tivoli Storage Manager password method" on page 61.

REDOLOG_COPIES *n* | **1**

Specifies the number of copies Data Protection for SAP stores for each processed Oracle redo log. The valid range is from 1 to 9. If not specified, Data Protection for SAP stores one copy of the redo logs. The number of different BRARCHIVE management classes (keyword BRARCHIVEMGTCLASS specified must be greater than or equal to the number of log file copies specified. For more detailed information about

implementing and using REDOLOG_COPIES see "Cooperation of Data Protection for *SAP*® for Oracle with BRARCHIVE" on page 119.

REPORT NO | YES | 2
If set to YES, Data Protection for SAP produces additional information such as information about transferred files. If set to 2, Data Protection for SAP generates an additional summary report containing detailed backup and restore performance statistics. This summary is displayed at the end of the complete operation. The output is sent to stdout, which is typically the console. If not specified, the default is REPORT NO. This keyword has no effect if an RMAN backup or restore operation is started.

RL_COMPRESSION NO | YES
If set to YES, Data Protection for SAP performs a null block compression of the data before they are sent over the network. Although RL compression introduces additional CPU load, throughput can be improved when the network is the bottleneck. It is not recommended to use RL compression together with the Tivoli Storage Manager API compression. If not specified, the default value is NO meaning null block compression is not performed. RL_COMPRESSION is only performed if a full database backup (BRBACKUP) was started. The offline log files (BRARCHIVE) are not compressed.

SERVER *servername*
This keyword specifies the name of the Tivoli Storage Manager server to which Data Protection for SAP backups are to be stored. This statement begins a server section in the Data Protection for SAP profile. At least one server section is required. Server sections are located at the end of the profile. A server section ends before a following SERVER keyword, before the END keyword, or at the end of the profile. These dependent keywords are applicable in a server section:

- ADSMNODE
- BRARCHIVEMGTCLASS
- BRBACKUPMGTCLASS
- PASSWORDREQUIRED
- SESSIONS
- TCP_ADDRESS
- USE_AT

The server name must be defined in the Tivoli Storage Manager profiles `dsm.sys` (UNIX and Linux) or `<servername.opt>` (for Windows). In order to set up alternate or parallel paths, each path is denoted by its own logical server name and corresponding server section, although these logical names refer to the same server. In this case, the Tivoli Storage Manager profiles specify the same TCP/IP address for these server names. In order to set up alternate or parallel servers, each server is represented by one or more server statements and the corresponding server sections (depending on the number of paths to the server). In this case, the Tivoli Storage Manager profiles specify different TCP/IP addresses for the different servers. Different server names result in different server entries in the Administration Assistant View TSM Server Utilization function while identical server names are considered to point to the same Tivoli Storage Manager server even if they are specified in different Data Protection for SAP profiles throughout the system landscape. Do NOT use any profile keywords, ADSM, or TSM as the servername.

SESSIONS *n* | **1**

The *n* value specifies the number of parallel sessions Data Protection for SAP uses for the server. This keyword is required in every server section. This parameter must be defined in conjunction with the respective SERVER statement, as shown in the sample profile.

SORT_FILE

To perform manual sorting, a file must be created (*sortfile*). This is an example of the sortfile contents:

```
/<path>/<filename1> disknumbers
/<path>/<filename2> disknumber
    .
     .
     .
/<path>/<filenameN> disknumber
```

The disk numbers are counted from 1 to n. They do not have any relation to the physical disks. You only have to specify the same number for the files on the same physical disk.

TCP_ADDRESS

Specifies the IP address of the Tivoli Storage Manager server in dotted decimal notation. This parameter overrides the value for the parameter TCPSERVERADDRESS in the Tivoli Storage Manager client system options file (`dsm.sys`) on UNIX or Linux or in the client options file (`<servername>.opt`) on Windows. The parameter TCP_ADDRESS must be defined in conjunction with the respective SERVER statement as shown in the sample profile.

TRACE FILEIO_MIN | FILEIO_MAX | COMPR_MIN | COMPR_MAX | MUX_MIN | MUX_MAX | TSM_MIN | TSM_MAX | ASYNC_MIN | ASYNC_MAX | APPLICATION_MIN | APPLICATION_MAX | SYSCALL_MIN | SYSCALL_MAX | COMM_MIN | COMM_MAX | DEADLOCK_MIN | DEADLOCK_MAX | PROLE_MIN | PROLE_MAX | BLAPI_MIN | BLAPI_MAX | SOCKET_DATA | ALL | OFF

This parameter writes trace information to the file specified with the TRACEFILE parameter. Arguments to TRACE can be any combination of the possible components and levels separated by spaces. A trace will only be written if both TRACE and TRACEFILE are specified. Do not use this parameter unless instructed to use it by Data Protection for SAP support. Using it can significantly deteriorate the performance of Data Protection for SAP.

TRACEFILE *path*

Specifies the name and location of the trace file for Data Protection for SAP to store all trace information. When TRACE is used, *path* specifies the full path and the name of file. If the value of TRACEFILE contains the string %BID, this string is replaced by the backup ID to get the path and name of the trace file actually used. For example, specifying `/tmp/%BID.trace` will yield a trace file `/tmp/myBackup.trace` for backup ID myBackup. A trace will only be written if both TRACE and TRACEFILE are specified.

TRACEMAX *n*

Specifies the maximum size of the trace file in KB. If not specified, the trace file size is unlimited.

USE_AT *days*

Specifies the days that the Tivoli Storage Manager server (specified with the corresponding SERVER keyword) is used. The *days* value can be numbers from 0 (Sunday) to 6 (Saturday). Multiple numbers can be used

when separated by spaces. If not specified, the default is to use the Tivoli Storage Manager server on all days. Make sure that the same Tivoli Storage Manager server is used for a simulation and its corresponding basis production backup. See "Simulating Backup and Restore" on page 80 for details on simulations. The parameter USE_AT must be defined in conjunction with the respective SERVER statement as shown in the sample profile. The parameter has no effect on actions other than backup.

Sample Data Protection for *SAP®* for Oracle Profile for UNIX or Linux

The sample profile (`initSID.utl`) is included in the Data Protection for *SAP®* for Oracle installation package. Although the UNIX, Linux, and Windows versions are similar, all example versions are provided.

```
#------------------------------------------------------------------------
#
# Data Protection for SAP (R) interface for ORACLE
#
# Sample profile for Data Protection for SAP (R) Version 6.1
# for UNIX
#
#------------------------------------------------------------------------
#
# This file should be renamed to $ORACLE_HOME/dbs/init$ORACLE_SID.utl
# where $ORACLE_HOME is the home directory of the Oracle database and
# $ORACLE_SID is the system ID of the Oracle database.
#
# See the 'Data Protection for SAP (R) Installation &
# User's Guide' for a full description.
#
# For a comment symbol the character '#' can be used.
# Everything following this character will be interpreted as comment.
#
# Data Protection for SAP (R) V6.1 accesses its profile
# in "read only" mode. All variable parameters like passwords, date of
# last password change, current version number will be written into the file
# specified with the CONFIG_FILE parameter. The passwords will be encrypted.


#------------------------------------------------------------------------
# Prefix of the 'Backup ID' which will be used for communication with
# BR*Tools and stored in the description field of the Tivoli Storage Manager
# archive function.
# Must be 6 characters.
# Default: none.
#------------------------------------------------------------------------
BACKUPIDPREFIX  SID___


#------------------------------------------------------------------------
# Number of parallel sessions to be established.
# Note: This number must not exceed the number of tape drives simultaneously
# available to the node on the Tivoli Storage Manager servers to be accessed.
# The valid range of MAX_SESSIONS is from 1 and 32.
# Default: none.
#------------------------------------------------------------------------
MAX_SESSIONS  1 # Tivoli Storage Manager client sessions


#------------------------------------------------------------------------
# Number of parallel sessions to be established for the database backup.
# Note: This number must not exceed the number of tape drives simultaneously
# available to the node for a database backup on the Tivoli Storage Manager
```

```
# servers to be accessed.
# The valid range of MAX_BACK_SESSIONS is from 1 to 32.
# Default: MAX_SESSIONS.
#------------------------------------------------------------------------
#MAX_BACK_SESSIONS 1 # Tivoli Storage Manager client sessions for backup


#------------------------------------------------------------------------
# Number of parallel sessions to be established for the redo log backup.
# Note: This number must not exceed the number of tape drives simultaneously
# available to the node for a redo log backup on the Tivoli Storage Manager
# servers to be accessed.
# The valid range of MAX_ARCH_SESSIONS is from 1 to 32.
# Default: MAX_SESSIONS.
#------------------------------------------------------------------------
#MAX_ARCH_SESSIONS 1 # Tivoli Storage Manager client sessions for archive


#------------------------------------------------------------------------
# Number of parallel sessions to be established for the backup of control
# files. This number is typically used to reduce the number of sessions
# to be used for the control file backup after another backup operation.
# The valid range of MAX_CONTROL_SESSIONS is from 1 to 32.
# Default: MAX_BACK_SESSIONS or MAX_ARCH_SESSIONS, depending on the type of
#          the control file backup.
#------------------------------------------------------------------------
#MAX_CONTROL_SESSIONS 1 # Tivoli Storage Manager client sessions for control
                        # file backup.


#------------------------------------------------------------------------
# Number of parallel sessions to be established for the restore of files.
# Note: This number must not exceed the number of tape drives simultaneously
# available to the node for restore processing backup on the Tivoli Storage
# Manager servers to be accessed.
# The valid range of MAX_RESTORE_SESSIONS is from 1 to 32.
# Default: MAX_SESSIONS.
#------------------------------------------------------------------------
#MAX_RESTORE_SESSIONS 1 # Tivoli Storage Manager client sessions for restore


#------------------------------------------------------------------------
# Number of backup copies of redo logs.
# The valid range of REDOLOG_COPIES is from 1 to 9.
# Default: 1.
#------------------------------------------------------------------------
#REDOLOG_COPIES  2


#------------------------------------------------------------------------
# Specifies whether a null block compression of the data is to be performed
# before transmission to Tivoli Storage Manager.
# Although RL compression introduces additional CPU load, throughput can be
# improved when the network is the bottleneck. RL compression in Data
# Protection for SAP (R) should not be used together with
# Tivoli Storage Manager API compression.
# Default: NO
#------------------------------------------------------------------------
#RL_COMPRESSION  YES


#------------------------------------------------------------------------
# Specifies how many files are read simultaneously and are multiplexed into
# one data stream to a Tivoli Storage Manager server. Multiplexing is usefull
# when the data rate to a Tivoli Storage Manager server is higher (fast
# tapes, fast network) than the I/O rate of a single disk.
# The valid range of MULTIPLEXING is from 1 to 8.
```

```
# Default: 1 (meaning no multiplexing)
#-------------------------------------------------------------------------
#MULTIPLEXING  2


#-------------------------------------------------------------------------
# Specifies the block size for disk I/O (in bytes).
# The default values have been chosen from our performance experiments in
# standard hardware environments.
# The valid range of BUFFSIZE is from 4KB to 32MB.
# Default: 131072 (128 KB) on UNIX, 32768 (32 KB) on Windows.
#-------------------------------------------------------------------------
BUFFSIZE  131072              # block size in bytes


#-------------------------------------------------------------------------
# This optional parameter controls how Data Protection for SAP(R) uses
# the internal buffers for transferring data during a backup.
# Valid values:   SIMPLE | PREVENT | AUTO
# Default: SIMPLE
#-------------------------------------------------------------------------
#BUFFCOPY              AUTO


#-------------------------------------------------------------------------
# Name of a program to be called before the backup task is started.
# Default: none.
#-------------------------------------------------------------------------
#FRONTEND              pgmname parameterlist


#-------------------------------------------------------------------------
# Name of a program to be called after the backup task is completed.
# Default: none.
#-------------------------------------------------------------------------
#BACKEND               pgmname parameterlist


#-------------------------------------------------------------------------
# Maximum number of data base backup versions to be kept.
# Note: Version control by Data Protection for SAP (R) is only activated
# if the R/3 release is 3.0C and higher and the parameter MAX_VERSIONS is
# not 0.
# The valid range of MAX_VERSIONS is from 0 to 9999.
# A value of 0 means no versioning.
# Default: 0, no versioning.
#-------------------------------------------------------------------------
#MAX_VERSIONS  4


#-------------------------------------------------------------------------
# Indicates whether processing is to be done unattended or whether human
# intervention is allowed.
# Default:
# YES for backup processing
# NO  for restore processing
#-------------------------------------------------------------------------
#BATCH                 YES                # unattended automated operation
#BATCH                 NO                 # manual operation


#-------------------------------------------------------------------------
# Control of error situations: Indicates whether and when database backups
# and restore operations should be ended when an error occurs during
# unattended processing.
# Valid values:
# YES: Exit if a single file cannot be backed up or restored.
```

```
# NO:  Do not exit when an error occurs.
# the number of errors resulting in exiting the processing.
# The valid range of EXITONERROR is from 0 to 100.
# Default: NO.
#------------------------------------------------------------------------
#EXITONERROR  3                  # exit after 3 errors


#------------------------------------------------------------------------
# Control of information for reporting purposes, e.g. messages, statistics.
# Default: NO (no additional data will be reported).
#------------------------------------------------------------------------
#REPORT   NO                  # no additional messages
#REPORT   YES                 # all additional messages
#REPORT   2                   # all additional messages + summary


#------------------------------------------------------------------------
# Controls generation of a trace file.
# Note: we recommend using the trace function only in cooperation with
# Data Protection for SAP (R) support.
# Default: OFF.
#------------------------------------------------------------------------
#TRACE   OFF


#------------------------------------------------------------------------
# The full path of the trace file.
# Note: for an actual trace the string '%BID' will be replaced by
# the current backupid.
# (.../backint_%BID.trace changes to .../backint_SAP___9809182300.trace).
# Default: none.
#------------------------------------------------------------------------
#TRACEFILE  /oracle/C21/dbs/backint.trace
#TRACEFILE  /oracle/C21/dbs/backint_%BID.trace


#------------------------------------------------------------------------
# Denotes the maximum size of the trace file in KB.
# If not specified, the trace file size is unlimited.
#------------------------------------------------------------------------
#TRACEMAX           <max size>            # trace file size in KB

#------------------------------------------------------------------------
# Specify the full path of the configuration file.
# Default: none.
#------------------------------------------------------------------------
CONFIG_FILE  /oracle/C21/dbs/initSID.bki


#------------------------------------------------------------------------
# Number of times to retry saving/restoring a file in case an error occurs.
# The valid range of FILE_RETRIES is from 0 to 100.
# Default: 3.
#------------------------------------------------------------------------
#FILE_RETRIES  3


#------------------------------------------------------------------------
# Denotes if Data Protection for SAP (R) shall send error/status
# information to a Tivoli Storage Manager server.
# The servername must match one of the servers listed in a SERVER statement.
# Valid values for verbosity are ERROR | WARNING | DETAIL.
# Default: none.
#------------------------------------------------------------------------
#LOG_SERVER             servername    [verbosity]
#LOG_SERVER             server_a      ERROR
```

```
#------------------------------------------------------------------------
# Denotes if Data Protection for SAP (R) shall use a manual sorting file
# for disk sorting.
# Default: none.
#------------------------------------------------------------------------
#SORT_FILE  /oracle/C21/dbs/manual_sort_file


#------------------------------------------------------------------------
# Denotes if Data Protection for SAP (R) shall use a compressed filesize
# sorting file for disk sorting.
# For backup simulations with compression (see manual) this parameter must
# be set to a valid file.
# Default: none.
#------------------------------------------------------------------------
#COMPR_INFO  /oracle/C21/dbs/initSID.cfi


#************************************************************************
# Statement for servers and paths.
# Multiple servers may be defined.
#************************************************************************


SERVER         server_a                # Servername, as defined in dsm.sys
  SESSIONS            2                # Maximum number of sessions
                                       # to server_a
  PASSWORDREQUIRED    YES              # Use a password
  ADSMNODE            NODE             # Tivoli Storage Manager Nodename
  BRBACKUPMGTCLASS    MDB              # Mgmt-Classes for database backup
  BRARCHIVEMGTCLASS   MLOG1 MLOG2      # Mgmt-Classes for redo log backup
# TCP_ADDRESS         192.168.1.1      # IP address of network interface
                                       # on server_a
                                       # Overrides IP address of dsm.sys
# USE_AT              0 1 2 3 4 5 6    # Days when server_a is used for
                                       # backup
#************************************************************************
# USE_AT : 0=Su 1=Mo 2=Tu 3=We 4=Th 5=Fr 6=Sa
# The valid range of USE_AT is from 0 to 6.
# Default: all days
#************************************************************************

#SERVER         server_b                # Servername, as defined in dsm.sys
#  SESSIONS            2                # Maximum number of sessions
                                       # to server_b
#  PASSWORDREQUIRED    YES              # Use a password
#  ADSMNODE            NODE             # Tivoli Storage Manager Nodename
#  BRBACKUPMGTCLASS    MDB              # Mgmt-Classes for database backup
#  BRARCHIVEMGTCLASS   MLOG1 MLOG2      # Mgmt-Classes for redo log backup
#  TCP_ADDRESS         192.168.1.1      # IP address of network interface
                                       # on server_b
                                       # Overrides IP address of dsm.sys
#  USE_AT              0 1 2 3 4 5 6    # Days when server_b is used for
                                       # backup
#************************************************************************
# USE_AT : 0=Su 1=Mo 2=Tu 3=We 4=Th 5=Fr 6=Sa
# Default: all days
#************************************************************************



#------------------------------------------------------------------------
```

```
# End of profile


END
```

Sample Data Protection for *SAP®* for Oracle Profile for Windows

```
#------------------------------------------------------------------------
#
# Data Protection for SAP (R) interface for ORACLE
#
# Sample profile for Data Protection for SAP (R)
# Version 6.1 for Windows 2000/2003
#
#------------------------------------------------------------------------
#
# See the 'Data Protection for SAP (R) Installation & User's Guide' for
# a full description.
#
# For a comment symbol the character '#' can be used.
# Everything following this character will be interpreted as comment.
#
# Data Protection for SAP (R) accesses its profile in "read only" mode.
# All variable parameters like passwords, date of last password change,
# current version number will be written into the file specified with the
# CONFIG_FILE parameter. The passwords will be encrypted.

#------------------------------------------------------------------------
# Prefix of the 'Backup ID' which will be used for communication with
# BR*Tools and stored in the description field of the Tivoli Storage Manager
# archive function.
# Must be 6 characters.
# Default: none.
#------------------------------------------------------------------------
BACKUPIDPREFIX  SID___


#------------------------------------------------------------------------
# Number of parallel sessions to be established.
# Note: This number must not exceed the number of tape drives simultaneously
# available to the node on the Tivoli Storage Manager servers to be accessed.
# The valid range of MAX_SESSIONS is from 1 and 32.
# Default: none.
#------------------------------------------------------------------------
MAX_SESSIONS  1 # Tivoli Storage Manager client sessions


#------------------------------------------------------------------------
# Number of parallel sessions to be established for the database backup.
# Note: This number must not exceed the number of tape drives simultaneously
# available to the node for a database backup on the Tivoli Storage Manager
# servers to be accessed.
# The valid range of MAX_BACK_SESSIONS is from 1 to 32.
# Default: MAX_SESSIONS.
#------------------------------------------------------------------------
#MAX_BACK_SESSIONS 1 # Tivoli Storage Manager client sessions for backup


#------------------------------------------------------------------------
# Number of parallel sessions to be established for the redo log backup.
# Note: This number must not exceed the number of tape drives simultaneously
# available to the node for a redo log backup on the Tivoli Storage Manager
# servers to be accessed.
# The valid range of MAX_ARCH_SESSIONS is from 1 to 32.
# Default: MAX_SESSIONS.
```

```
#------------------------------------------------------------------------
#MAX_ARCH_SESSIONS 1 # Tivoli Storage Manager client sessions for archive


#------------------------------------------------------------------------
# Number of parallel sessions to be established for the backup of control
# files. This number is typically used to reduce the number of sessions
# to be used for the control file backup after another backup operation.
# The valid range of MAX_CONTROL_SESSIONS is from 1 to 32.
# Default: MAX_BACK_SESSIONS or MAX_ARCH_SESSIONS, depending on the type of
#          the control file backup.
#------------------------------------------------------------------------
#MAX_CONTROL_SESSIONS 1 # Tivoli Storage Manager client sessions for control
                        # file backup.

#------------------------------------------------------------------------
# Number of parallel sessions to be established for the restore of files.
# Note: This number must not exceed the number of tape drives simultaneously
# available to the node for restore processing backup on the Tivoli Storage
# Manager servers to be accessed.
# The valid range of MAX_RESTORE_SESSIONS is from 1 to 32.
# Default: MAX_SESSIONS.
#------------------------------------------------------------------------
#MAX_RESTORE_SESSIONS 1 # Tivoli Storage Manager client sessions for restore


#------------------------------------------------------------------------
# Number of backup copies of redo logs.
# The valid range of REDOLOG_COPIES is from 1 to 9.
# Default: 1.
#------------------------------------------------------------------------
#REDOLOG_COPIES  2


#------------------------------------------------------------------------
# Specifies whether a null block compression of the data is to be performed
# before transmission to Tivoli Storage Manager.
# Although RL compression introduces additional CPU load, throughput can be
# improved when the network is the bottleneck. RL compression in Data
# Protection for SAP (R) should not be used together with
# Tivoli Storage Manager API compression.
# Default: NO
#------------------------------------------------------------------------
#RL_COMPRESSION  YES


#------------------------------------------------------------------------
# Specifies how many files are read simultaneously and are multiplexed into
# one data stream to a Tivoli Storage Manager server. Multiplexing is usefull
# when the data rate to a Tivoli Storage Manager server is higher (fast
# tapes, fast network) than the I/O rate of a single disk.
# The valid range of MULTIPLEXING is from 1 to 8.
# Default: 1 (meaning no multiplexing)
#------------------------------------------------------------------------
#MULTIPLEXING  2


#------------------------------------------------------------------------
# Specifies the block size for disk I/O (in bytes).
# The default values have been chosen from our performance experiments in
# standard hardware environments.
# The valid range of BUFFSIZE is from 4KB to 32MB.
# Default: 131072 (128 KB) on UNIX, 32768 (32 KB) on Windows.
#------------------------------------------------------------------------
BUFFSIZE  32768             # block size in bytes
```

```
#------------------------------------------------------------------------
# This optional parameter controls how Data Protection for SAP(R) uses
# the internal buffers for transferring data during a backup.
# Valid values:   SIMPLE | PREVENT | AUTO
# Default: SIMPLE
#------------------------------------------------------------------------
#BUFFCOPY              AUTO


#------------------------------------------------------------------------
# Name of a program to be called before the backup task is started.
# Default: none.
#------------------------------------------------------------------------
#FRONTEND              pgmname parameterlist


#------------------------------------------------------------------------
# Name of a program to be called after the backup task is completed.
# Default: none.
#------------------------------------------------------------------------
#BACKEND               pgmname parameterlist


#------------------------------------------------------------------------
# Maximum number of data base backup versions to be kept.
# Note: Version control by Data Protection for SAP (R) is only activated
# if the SAP R/3 release is 3.0C and higher and the parameter
# not 0.
# The valid range of MAX_VERSIONS is from 0 to 9999.
# A value of 0 means no versioning.
# Default: 0, no versioning.
#------------------------------------------------------------------------
#MAX_VERSIONS  4


#------------------------------------------------------------------------
# Indicates whether processing is to be done unattended or whether human
# intervention is allowed.
# Default:
# YES for backup processing
# NO  for restore processing
#------------------------------------------------------------------------
#BATCH                 YES                # unattended automated operation
#BATCH                 NO                 # manual operation


#------------------------------------------------------------------------
# Control of error situations: Indicates whether and when database backups
# and restore operations should be ended when an error occurs during
# unattended processing.
# Valid values:
# YES: Exit if a single file cannot be backed up or restored.
# NO:  Do not exit when an error occurs.
# the number of errors resulting in exiting the processing.
# The valid range of EXITONERROR is from 0 to 100.
# Default: NO.
#------------------------------------------------------------------------
#EXITONERROR  3                  # exit after 3 errors


#------------------------------------------------------------------------
# Control of information for reporting purposes, e.g. messages, statistics.
# Default: NO (no additional data will be reported).
#------------------------------------------------------------------------
#REPORT   NO                 # no additional messages
#REPORT   YES                # all additional messages
#REPORT   2                  # all additional messages + summary
```

```
#------------------------------------------------------------------------
# Controls generation of a trace file.
# Note: we recommend using the trace function only in cooperation with
# Data Protection for SAP (R) support.
# Default: OFF.
#------------------------------------------------------------------------
#TRACE   OFF


#------------------------------------------------------------------------
# The full path of the trace file.
# Note: for an actual trace the string '%BID' will be replaced by
# the current backupid.
# (...\backint_%BID.trace changes to ...\backint_SAP___9809182300.trace).
# Default: none.
#------------------------------------------------------------------------
#TRACEFILE  x:\oracle\C21\database\backint.trace
#TRACEFILE  x:\oracle\C21\database\backint_%BID.trace


#------------------------------------------------------------------------
# Denotes the maximum size of the trace file in KB.
# If not specified, the trace file size is unlimited.
#------------------------------------------------------------------------
#TRACEMAX           <max. size>             # trace file size in KB

#------------------------------------------------------------------------
# Specify the full path of the configuration file.
# Default: none.
#------------------------------------------------------------------------
CONFIG_FILE  x:\oracle\C21\database\initSID.bki


#------------------------------------------------------------------------
# Number of times to retry saving/restoring a file in case an error occurs.
# The valid range of FILE_RETRIES is from 0 to 100.
# Default: 3.
#------------------------------------------------------------------------
#FILE_RETRIES  3


#------------------------------------------------------------------------
# Denotes if Data Protection for SAP (R) shall send error/status
# information to a Tivoli Storage Manager server.
# The servername must match one of the servers listed in a SERVER statement.
# Valid values for verbosity are ERROR | WARNING | DETAIL.
# Default: none.
#------------------------------------------------------------------------
#LOG_SERVER             servername    [verbosity]
#LOG_SERVER             server_a      ERROR


#------------------------------------------------------------------------
# Denotes if Data Protection for SAP (R) shall use a manual sorting file
# for disk sorting.
# Default: none.
#------------------------------------------------------------------------
#SORT_FILE  x:\oracle\C21\database\manual_sort_file


#------------------------------------------------------------------------
# Denotes if Data Protection for SAP (R) shall use a compressed filesize
# sorting file for disk sorting.
# For backup simulations with compression (see manual) this parameter must
# be set to a valid file.
```

```
# Default: none.
#------------------------------------------------------------------------
#COMPR_INFO  x:\oracle\C21\database\initSID.cfi


#************************************************************************
# Statement for servers and paths.
# Multiple servers may be defined.
#************************************************************************


SERVER         server_a                 # Servername, as defined in dsm.sys
  SESSIONS             2                # Maximum number of sessions
                                        # to server_a
  PASSWORDREQUIRED     YES              # Use a password
  ADSMNODE             NODE             # Tivoli Storage Manager Nodename
  BRBACKUPMGTCLASS     MDB              # Mgmt-Classes for database backup
  BRARCHIVEMGTCLASS    MLOG1 MLOG2      # Mgmt-Classes for redo log backup
# TCP_ADDRESS          192.168.1.1      # IP address of network interface
                                        # on server_a
                                        # Overrides IP address of dsm.sys
# USE_AT               0 1 2 3 4 5 6    # Days when server_a is used for
                                        # backup
#************************************************************************
# USE_AT : 0=Su 1=Mo 2=Tu 3=We 4=Th 5=Fr 6=Sa
# The valid range of USE_AT is from 0 to 6.
# Default: all days
#************************************************************************

#SERVER         server_b                 # Servername, as defined in dsm.sys
#  SESSIONS             2                # Maximum number of sessions
                                        # to server_b
#  PASSWORDREQUIRED     YES              # Use a password
#  ADSMNODE             NODE             # Tivoli Storage Manager Nodename
#  BRBACKUPMGTCLASS     MDB              # Mgmt-Classes for database backup
#  BRARCHIVEMGTCLASS    MLOG1 MLOG2      # Mgmt-Classes for redo log backup
#  TCP_ADDRESS          192.168.1.1      # IP address of network interface
                                        # on server_b
                                        # Overrides IP address of dsm.sys
#  USE_AT               0 1 2 3 4 5 6    # Days when server_b is used for
                                        # backup
#************************************************************************
# USE_AT : 0=Su 1=Mo 2=Tu 3=We 4=Th 5=Fr 6=Sa
# Default: all days
#************************************************************************


#------------------------------------------------------------------------
# End of profile


END
```

Defining the Custom SQL file

Note: The custom SQL file is intended to be implemented or modified only by IBM support personnel with a detailed knowledge of the process involved and the internal Administration Assistant function for Data Protection for *SAP*® database. This section does not discuss this process in detail.

The custom SQL file must be named customSQLFile.txt and placed in the installation directory (or folder) of the Administration Assistant. For example:

```
C:\Program Files\tdpr3assi\customSQLFile.txt
```

The custom SQL file contains this structure:

```
# CUSTOM SQL FILE Comment

<sql>SQL statement</sql><description> ... </param>
<sql>SQL statement</sql><description> ... </param>
...
```

As an aid to explaining the entry structure, it is shown in the following with each tag set in a separate line:

```
<sql>SQL statement</sql>
<description>Description of the SQL statement</description>
<programid>0</programid>
<actionid>0</actionid>
<displaygroup>1,3</displaygroup>
<backuptype>2</backuptype>
<executionmode>0</executionmode>
<param>parameter-value1</param>
<param>parameter-value2</param>
...
<param>parameter-valuen</param>
```

Each entry must be coded in a single line.

The tag definitions are as follows:

Table 12. Contents of the Custom SQL File

Tag	Definition
#	Comment line
<sql>	An SQL statement that defines which data is to be sent. **Note:** 1. Only SELECT statements will be executed. 2. A semicolon at the end of the line is not permitted. 3. The maximum line length is 400 characters.
<description>	Description of the SQL statement (maximum length: 300 characters)
<programid>	Specifies the program that handles the result of the SQL statement. • programid 0: Administration Assistant
<actionid>	Defines the way the result will be handled, depending on the programid (currently, the only value for actionid is 0): • (programid 0: Administration Assistant): Send e-mail when threshold exceeded (SQL statement returns data)
<displaygroup>	List of display group IDs separated by commas, or "ALL" for all display groups.
<system>	List of system IDs separated by commas, or "ALL" for all systems.
<backuptype>	List of backup types separated by commas, or "ALL" for all backup types. • 0: Archive • 1: Partial backup • 2: Incremental backup • 3: Full backup

Table 12. Contents of the Custom SQL File (continued)

Tag	Definition
<executionmode>	executionmode sets the time the entry will be performed (i.e., the SQL statement issued): • 0: Entry will be performed after each backup run • 1: Entry will be performed periodically
<param>	Parameters needed by the programs. The number of parameters depends on the selected program and action. Multiple parameters are coded using repeating <param></param> tag pairs. • (programid 0: Administration Assistant): – One parameter, consisting of the e-mail address list (separated by semicolons)

Consider these facts about the custom SQL file:

- Each entry in the file must be on a single line.
- If executionmode is 1, the <system>, <displaygroup>, and <backuptype> tags are ignored, and the SQL statement will be executed periodically.
- If executionmode is 0, the SQL statement will be executed after the backup completes, but only if the system tag matches the system on which the backup was performed, or the displaygroup tag matches the displaygroup the system belongs to. Furthermore, the <backuptype> tag must match the backup type of the backup performed.
- The <system> and <displaygroup> tags are mutually exclusive.
- The custom SQL file will be reloaded periodically by the Administration Assistant Server component. The server does not need to be restarted.

Defining Thresholds Using the Custom SQL File

A custom threshold can be defined in the custom SQL file. The corresponding entry has the following values for the indicated tags:

Table 13. Tags for Defining Thresholds in the Custom SQL File

Tag	Value
<sql>	An SQL statement that will return data when the threshold is exceeded.
<programid>	0 (Administration Assistant)
<actionid>	0 (send e-mail when threshold exceeded)
<executionmode>	1 (run periodically)
<param>	(Optional) One or more e-mail addresses, separated by semicolons. If no e-mail address is given, only a panel indication is given that the threshold has been exceeded. **Note:** Multiple e-mail addresses are given in a single <param></param> tag pair, not in multiple pairs.

Sample Custom SQL File

This is a sample of a custom SQL file.

```
# CUSTOM SQL FILE FOR THE ADMINISTRATION ASSISTANT
#
# This file should only be changed by an IBM Employee
# After the changes you have to check this file using CustomSQLFilecheck
#
# NOTE: Each entry must be coded in one line. The multi-line format
# shown below is for illustration purposes only.
#
#
# Sample threshold definition: backup size > 500 GB, display group 1, backup type 2
#
<sql>select * from AdminAssistant.tsmrun where amount > 500000000000</sql>
<description>Amount over 500 GB</description>
<programid>0</programid>
<actionid>0</actionid>
<displaygroup>1</displaygroup>
<backuptype>2</backuptype>
<executionmode>0</executionmode>
<param>emailAdress@email.com</param>
#
```

Data Protection for *SAP®* for Oracle files and samples

Use these file samples to assist with Data Protection for *SAP®* for Oracle operations.

Save and Delete Redo Logs Batch File Sample

```
@echo off
rem ------------------------------------------------------------------------
rem file name: archive.cmd
rem ------------------------------------------------------------------------
rem Sample BRArchive batch file
rem ------------------------------------------------------------------------
rem Task:
rem Invokes the SAP utility BRArchive in order to save ORACLE's archived
rem redo logs (using Data Protection for SAP (R) ) and deletes the redo
rem logs from their original location. After completing this, the BRArchive
rem protocol is saved separately.
rem ------------------------------------------------------------------------
rem ***** NOTE ***** NOTE ***** NOTE *****
rem
rem This script is intended only as a model and should be
rem carefully tailored to the needs of the specific site.
rem
rem ***** NOTE ***** NOTE ***** NOTE *****
rem ------------------------------------------------------------------------
rem
rem Remarks on the parameters of BRArchive:
rem
rem -u system/manager ORACLE username/password
rem -sd save and delete archived redo logs
rem -c run BRArchive in quiet mode
rem (-n number of redo logs to be saved,
rem default is 10000,
rem which means all available)
rem
rem The following should be configured within the SAP profile
rem initC21.sap:
rem
rem backup_dev_type = util_file
rem causes BRBACKUP to use the external program
```

```
rem Data Protection for SAP (R)
rem util_par_file = %ORACLE_HOME%\database\initC21.utl
rem Data Protection for SAP (R) profile
rem ------------------------------COMMAND----------------------------------
brarchive -u system/manager -sd -c
```

Save and Delete Redo Logs Shell Script Sample

```
#!/bin/ksh
# ------------------------------------------------------------------------
# archive.ksh:
# Sample BRARCHIVE shell script
# ------------------------------------------------------------------------
# Task:
# Invokes the SAP utility brarchive in order to save ORACLE's archived
# redo logs (using Data Protection for SAP (R) ) and deletes the redo
# logs from their original location. After completing this, the brarchive
# protocol is saved separately.
# ------------------------------------------------------------------------
#      *****     NOTE     *****     NOTE     *****     NOTE     *****
#
#          This script is intended only as a model and should be
#          carefully tailored to the needs of the specific site.
#
#      *****     NOTE     *****     NOTE     *****     NOTE     *****
# ------------------------------------------------------------------------
#
# Remarks on the parameters:
#
# -u system/manager     Oracle username/password
# -sd                   save and delete archived redo logs
# -c                    run BRARCHIVE in unattended mode
# (-n                   number of redo logs to be saved, default is 10000,
#   which means all available)
#
# The following should be configured within the SAP profile initC11.sap:
#
# backup_dev_type = util_file
#  causes brbackup to use the external program backint
# util_par_file =  initC11.utl
#  Data Protection for SAP profile
#
# --------------------------------COMMAND----------------------------------
brarchive -u system/manager -c -sd
```

Sample Shell Script for Scheduling a Report from a UNIX Scheduling Client

The `scheduledReport.sh` file is provided in the Data Protection for *SAP*® for Oracle package and is copied to the Administration Assistant function for Data Protection for *SAP*® installation path.

```
#------------------------------------------------------------------------
#
# Tivoli Storage Manager for ERP. Data Protection for SAP® for Oracle
#
# Sample command file for the Administration Assistant scheduling client
#
# ------------------------------------------------------------------------
#      *****     NOTE     *****     NOTE     *****     NOTE     *****
#
#          This script is provided as a model and should be
#          carefully tailored to the needs of the specific site.
#
#      *****     NOTE     *****     NOTE     *****     NOTE     *****
```

```
#-------------------------------------------------------------------------
export CLASSPATH=/reporting/Admt.jar:$CLASSPATH
export PATH=/usr/bin:$PATH
java -classpath $CLASSPATH com.ibm.bkit.schedulerIF.Sched_Main xxx.xxx.xxx.xxx...
... 1099 myReport ADMIN admin directory=/myreports log=/tmp/reportlogs
```

Sample Command File for Scheduling a Report from a Windows Scheduling Client

The scheduledReport.cmd file is provided in the Data Protection for *SAP*® for Oracle package and is copied to the Administration Assistant function for Data Protection for *SAP*® Server component installation path.

```
#-------------------------------------------------------------------------
#
# Tivoli Storage Manager for ERP. Data Protection for SAP® for Oracle
#
# Sample command file for the Administration Assistant scheduling client
#
# ------------------------------------------------------------------------
#      *****     NOTE     *****     NOTE     *****     NOTE     *****
#
#          This script is provided as a model and should be
#          carefully tailored to the needs of the specific site.
#
#      *****     NOTE     *****     NOTE     *****     NOTE     *****
#-------------------------------------------------------------------------
set CLASSPATH=C:\ProgramFiles\reporting\Admt.jar
set PATH=C:\Program Files\IBM\Java142\jre\bin:%PATH%
java -cp %CLASSPATH% com.ibm.bkit.schedulerIF.Sched_Main xxx.xxx.xxx.xxx ...
... 1099 myReport ADMIN admin directory=C:\reports log=C:\reportlogs
```

Client User Options File Sample (dsm.opt) UNIX and Linux

```
************************************************************************
* IBM Tivoli Storage Manager                                           *
*                                                                      *
* Sample Client User Options file for Unix platforms                   *
************************************************************************

SErvername       server_a
Tapeprompt       No
DOM              /usr/sap /sapmnt/C11 /usr/sap/trans /oracle/C11
```

Client User Options File Sample (dsm.opt) Windows

Data Protection for *SAP*® for Oracle requires a client options file dsm.opt to be present in the location indicated by environment variable DSMI_CONFIG. The specific options used by Data Protection for *SAP*® for each server however are taken from files <server>.opt residing in the same path.

```
************************************************************************
*
* DSM.OPT (for Data Protection for SAP (R) )
*
* This file is intentionally left empty. It must be present in the location
* indicated by environment variable DSMI_CONFIG. The specific options used
* by Data Protection for SAP for each server however are taken from files
* <server>.opt residing in the same path.
*
* Please note: This client options file is not meant to be used by other
*              TSM clients.
*
************************************************************************
```

Client System Options File Sample (dsm.sys)

```
************************************************************************
* IBM Tivoli Storage Manager                                           *
*                                                                      *
* Sample Client System Options file for Unix platforms                 *
************************************************************************


SErvername  server_a
  COMMmethod         TCPip
  TCPPort            1500
  TCPServeraddress   your_ITSM_server_1
  TCPBuffsize        32
  TCPWindowsize      24
  Compression        Off
  InclExcl           /usr/lpp/adsm/bin/inclexcl.list

SErvername  server_b
  COMMmethod         TCPip
  TCPPort            1500
  TCPServeraddress   your_ITSM_server_2
  TCPBuffsize        32
  TCPWindowsize      24
  Compression        Off
  InclExcl           /usr/lpp/adsm/bin/inclexcl.list
```

Include/Exclude List Sample (UNIX and Linux)

```
* ------------------------------------------------------------------------
* inclexcl.list:
* Sample include/exclude list
* ------------------------------------------------------------------------
* Task:
* Include/Exclude list of files and directories for TSM incremental backups
* ------------------------------------------------------------------------
*      *****     NOTE     *****     NOTE     *****     NOTE     *****
*
*          This file is intended only as a model and should be
*          carefully tailored to the needs of the specific site.
*
*      *****     NOTE     *****     NOTE     *****     NOTE     *****
* ------------------------------------------------------------------------
*
* For all AIX systems
*
exclude /unix
exclude /.../core
exclude /u/.../.*sh_history
exclude /home/.../.*sh_history
*
* Note: It is recommended to perform system backups on a regular
*       basis (e.g. using 'smit mksysb'). Consequently, you can exclude
*       at least the following directories (which make up about 30 MB).
*
exclude /usr/games/.../*
exclude /usr/bin/.../*
exclude /usr/lbin/.../*
exclude /usr/mbin/.../*
exclude /usr/sbin/.../*
* ------------------------------------------------------------------------
*
* For those using AFS, exclude the cache filesystem or file
*
* exclude /usr/vice/cache/*
* exclude /var/vice/cache/*
* or
```

```
* exclude /afscfs
* ------------------------------------------------------------------------
*
* This stuff is either not worthwhile to be included or should be backed up
* using SAP's BR*Tools utilities brbackup/brarchive.
*
exclude /oracle/C11/saparch/.../*
* exclude /oracle/C11/sapbackup/.../*
* exclude /oracle/C11/sapreorg/.../* (There may be important scripts
*                                     located, check it out and decide.)
exclude /oracle/C11/sapdata*/.../*
exclude /oracle/C11/sapraw*/.../*
* ------------------------------------------------------------------------
*
* With the above include/exclude list we implicitly include everything not
* excluded above. Especially for DP for SAP (R), this means including:
*      /sapmnt/C11     > 270 MB
*      /usr/sap        > 14 MB
*      /oracle/stage   > 89 MB
*      /oracle/C11     > 90 MB
* and  OS  related     > 220 MB
* ------------------------------------------------------------------------
```

Include/Exclude List Sample (Windows)

This sample include/exclude list is intended for the standard client user option file. The purpose is to exclude files that are easy to restore or that are already saved by Data Protection for *SAP*® for Oracle from routine Tivoli Storage Manager incremental backups. Typically, such files are Windows system files and Oracle database files.

```
************************************************************************
* This Include-Exclude list is used for incremental backups of file
* systems by the Tivoli Storage Manager command-line backup client.
* Therefore the name of this file has to be set under the keyword InclExcl
* in the standard Tivoli Storage Manager client user option file "dsm.opt".
*
* Since the backup of the ORACLE database is done by
* Data Protection for SAP (R) and not by Tivoli Storage
* Manager command-line backup client, the ORACLE database should be excluded
* from backups by the Tivoli Storage Manager command-line backup client.
*
* Note 1:
* The environment variable DSM_CONFIG contains the full file name of
* the Tivoli Storage Manager client user option file "dsm.opt".
* Note 2:
* This Include-Exclude is not used by Data Protection for SAP (R).
*
************************************************************************
Exclude *:\...\*.swp
Exclude *:\...\*.obj
Exclude *:\...\*.csm
Exclude *:\...\*.dsk
Exclude *:\...\*.bak
Exclude *:\...\win386.swp
Exclude *:\...\386spart.par
Exclude *:\...\pagefile.sys
Exclude *:\...\*.par
Exclude *:\...\SYSTEM32\CONFIG\*.*
Exclude *:\...\SYSTEM32\CONFIG\...\*
Exclude *:\IBMBIO.COM
Exclude *:\IBMDOS.COM
*
*Exclude the following ORACLE database files:
*
```

```
Exclude *:\oracle\C21\saparch\...\*
Exclude *:\oracle\C21\sapbackup\...\*
Exclude *:\oracle\C21\sapreorg\...\*
Exclude *:\oracle\C21\sapdata*\...\*
```

Client Options Files Sample (<server>.opt)

Data Protection for *SAP*® for Oracle requires a corresponding client option file `<server>.opt` for each Tivoli Storage Manager server. These files must reside in the same directory. This directory must also contain the client options file `dsm.opt`, which is specified in the environment variable DSMI_CONFIG. The contents of this (second) `dsm.opt` file is ignored by Data Protection for SAP.

```
************************************************************************
*
* SERVER.OPT
*
* Data Protection for SAP (R) obtains the necessary information about
* a Tivoli Storage Manager server 'server' from a client option file
* called '<server>.opt'. For each Tivoli Storage Manager server a
* corresponding client option file is required.
*
* Note: This file contains the client options for the Tivoli Storage Manager
* server called 'server_a'.
*
* Please see the Tivoli Storage Manager documentation for details.
*
************************************************************************
COMMmethod         TCPIP
SLOWINCR           NO
COMPression        OFF
*NODEname           C21
TCPPort            1500
TCPServeraddress   xxx.xxx.xxx.xxx
PASSWORDACCESS     PROMPT
TCPBUFFSIZE        31
TCPWINDOWSIZE      32
```

Data Protection for *SAP*® for Oracle planning sheets

Uses these planning sheets to assist with installing and configuring Data Protection for *SAP*® for Oracle.

Data Protection for *SAP*® for Oracle (base product) planning sheet

Collect the information in this planning sheet before attempting to install Data Protection for *SAP*® for Oracle. This table is also provided in file form as `planning_sheet_oracle` for UNIX and Linux and `planning_sheet_oracle.txt` for Windows.

Table 14. Installation Parameters for Data Protection for SAP

UNIX or Linux	Windows	Installation Parameter
X	X	Oracle database SID:

Table 14. Installation Parameters for Data Protection for SAP (continued)

UNIX or Linux	Windows	Installation Parameter
X	X	Path where the SAP BR*Tools reside: Default: /usr/sap/<SID>/SYS/exe/run or C:\oracle\<SID>\sapmnt\SYS\exe\run
X	X	Tivoli Storage Manager server name or IP address:
X	X	Tivoli Storage Manager node name: Tivoli Storage Manager node configured on the Tivoli Storage Manager server named for the backup of the SID denoted above. For details, refer to "5. Register a node" on page 60.
X	X	Tivoli Storage Manager management classes for database and redo log backups. Management classes configured for the database backup and for the backup of redo logs. For details, refer to "4. Define a policy" on page 59. Default: MDB for database backups, MLOG1 and MLOG2 for redo log backups.
	X	Path where the Tivoli Storage Manager API resides (contents of environment variable DSMI_DIR): Default: C:\Program Files\Common Files\tivoli\TSM\api64
	X	Path to client option file of Tivoli Storage Manager (contents of environment variable DSMI_CONFIG). For details refer to the Tivoli Storage Manager documentation.
	X	Path to Tivoli Storage Manager log files (contents of environment variable DSMI_LOG): The Tivoli Storage Manager API will create the file `dsierror.log<` in this path. For details, refer to the Tivoli Storage Manager documentation. Default: C:\temp
	X	Installation path for Data Protection for SAP executable files: C:\Program Files\Tivoli\TSM\tdp_r3\ora64
X	X	Path for Data Protection for SAP configuration files (directory for SAP configuration files). During the installation, the Data Protection for SAP configuration files will be saved to this path. If old configuration files are found, they are renamed to `<filename>.nnn`, where `nnn` is a three-digit decimal number.This path must not contain blanks. Default: /oracle/<SID>/dbs or C:\orant\database

Table 14. Installation Parameters for Data Protection for SAP (continued)

UNIX or Linux	Windows	Installation Parameter
X	X	Options: • Use of Oracle RMAN. • Use of the Administration Assistant (see "Administration Assistant function for Data Protection for *SAP*®" on page 5 and Table 15). The Administration Assistant should be installed prior to Data Protection for SAP so that the interface between the two can be automatically established.

Administration Assistant function for Data Protection for *SAP*® planning sheet

Collect the information in this planning sheet before attempting to install the Administration Assistant function for Data Protection for *SAP*®. This table is also provided in file form as `planning_sheet_aa` for UNIX and Linux, and `planning_sheet_aa.txt` for Windows.

Table 15. Installation Parameters for the Administration Assistant function for Data Protection for SAP®

Installation Option	Installation Parameter
Installation type.	Decision as to whether the Administration Assistant is to be installed on a single host (typical installation) or distributed across multiple hosts (custom installation). Default: Single-host
Server/client communication mode	Decision as to whether the Administration Assistant Server component and clients communicate in nonsecure mode via HTTP or secure mode via HTTPS. Default: Nonsecure
Database type	Decision as to which DBMS the Administration Assistant should use. Select either the installation of the bundled Apache Derby package or the use of an existing Apache Derby or IBM DB2 installation. Default: Installation of Apache Derby as bundled with product.
Data migration	If you want to migrate data from an existing Administration Assistant environment, enter the directory containing the *.aa files. Default: No migration.
Software language	Decision as to whether to install only the English version of the program or all national language versions. Default: English-only

Table 15. Installation Parameters for the Administration Assistant function for Data Protection for SAP® (continued)

Installation Option	Installation Parameter
Parameters applying to the Administration Assistant Server component	Hostname or IP address: Default: Hostname of current system Port number for Data Protection for *SAP*® for Oracle (ProLE) connect. This port number must be made known to all instances of Data Protection for SAP that are to be managed and monitored by this Server component instance. Default: 5126 Port number for client connect in non-secure mode (HTTP). Default: 80 Port number for client connect in secure mode (HTTPS). Default: 443 RMI registry port number Default: 1099 Port number for performance data from Database Agent Default: 5129 Port number for communication with Database Agent Default: 5128
Parameters applying to the Administration Assistant Database Agent component	Hostname or IP address: Default: Hostname of current system Port number for Data Protection for SAP (ProLE) connection Default: 5125 Port number for communication with Administration Assistant Server component Default: 5127
Parameters applying to the Administration Assistant Database component (Apache Derby)	Hostname or IP address: Default: Hostname of current system Port number for database connect Default: 1527 User ID and password to access internal database.

Table 15. Installation Parameters for the Administration Assistant function for Data Protection for SAP® (continued)

Installation Option	Installation Parameter
Parameters applying to the Administration Assistant Database component (IBM DB2)	Hostname or IP address: Default: Hostname of current system Port number for database connect Default: 50000 User ID and password of the system user for which the DB2 instance should be installed that the internal database should access.
Installation directory	Installation directory (on each host) Default: `/opt/tivoli/tsm/tdp_r3_assist` on UNIX and Linux, or `C:\Program Files\tdpr3assi` on Windows.
Product Support	Location of mail.jar (Java Mail)
Product Support	Location of activation.jar (Java Beans Activation Framework):
History file	History file directory (on Server component host) Default: `history` (in installation directory) History file retention time (days). Can be changed via the Administration Assistant client. Default: 14

Table 15. Installation Parameters for the Administration Assistant function for Data Protection for SAP® (continued)

Installation Option	Installation Parameter
Secure Communication	Information on the public key infrastructure (PKI): • *Keystore name*. Keystore containing the private and public keys of the Administration Assistant Server component when running in secure mode. If you do not yet have a public key infrastructure, the keystore can be created during the installation process. • *Keystore password*. Password ensuring the consistency of the keystore. The server's key pair must be protected by the same password. • *Truststore name*. Truststore containing a set of trusted certificates. When running in secure mode, the Administration Assistant's server certificate must be verified against this truststore when the server is started. • *Truststore password*. Password ensuring the consistency of the truststore. This is only required if a trusted certificate needs to be imported into the truststore during the installation process. • *Certificate file*. Path of the certificate file in case you already have a server certificate issued by a certificate authority. • *Certificate creation information*. Information on the X.500 distinguished name (common name, organizational unit, organization name, locality name, state name, and country code) and on the validity period required in case a new self-signed certificate is to be created during the installation process. For details on this information, refer to the X.500 and X.509 standards. • *New certificate file name*. If the public key of a newly created server key pair needs to be distributed to client machines it will be exported to this file. • *CSR file name*. If the newly created server key pair will be used to request a certificate signed by a Certificate Authority, the Certificate Signing Request will be written to this file.
Internal database managed by DB2	DB2 JDBC Universal Driver. The corresponding packages are bundled with your IBM DB2 installation. • db2jcc.jar location:Default: None • db2jcc_license_cu.jar location:Default: None The Administration Assistant database is enabled for automatic storage and has a set of one or more associated storage paths. Enter at least one disk or path that DB2 is allowed to assign and allocate for its table space containers. Default: None The name of the internal database is predefined and cannot be changed. Default: `AADB`

Table 15. Installation Parameters for the Administration Assistant function for Data Protection for SAP® (continued)

Installation Option	Installation Parameter
Internal database managed by Apache Derby	Database directory: Default: `aaDBSupport` (in installation directory) Name of the internal database Default: 'adminAssistant' Retention time for data in database (days). (To save this data, the backup facilities offered by Derby can be used.) Default: 175
Documentation	Option: English-only or all languages Default: English-only

Tips for network settings

Helpful information to assist with adjusting your network is provided.

Network Settings of the Tivoli Storage Manager

The performance adjustments for Tivoli Storage Manager are performed by editing these configuration files:

- Tivoli Storage Manager server option file `dsmserv.opt`
- Tivoli Storage Manager backup-archive client option file `dsm.sys` (UNIX and Linux systems) or `server.opt` (Windows systems).

This table shows the corresponding Tivoli Storage Manager configuration file attributes with the recommended values.

Table 16. Tuning Tivoli Storage Manager Configuration File Attributes

Attributes	Value	Description
`TCPBuffsize`	`32`	Specifies the size, in kilobytes, of the buffer used for TCP/IP send requests. This option affects whether or not Tivoli Storage Manager sends the data directly from the session buffer or copies the data to the TCP buffer. A 32K buffer size forces Tivoli Storage Manager to copy data to its communication buffer and flush the buffer when it fills.
`TCPNODelay`	`YES`	Specifies whether the server should send small amounts of data or allow TCP/IP to buffer the data. Disallowing buffering may improve throughput but more packets will be sent over the network.
`TCPWindowsize`	`640 (AIX)` `63 (others)`	Specifies the size, in kilobytes, which will be used for the TCP/IP sliding window for the client node. This is the size of the buffer used when sending or receiving data. The range of values is 0 to 2048.

Additional information can be found at: http://www-306.ibm.com/software/tivoli/products/storage-mgr-erp/.

Networks with Large Bandwidth-Delay Product

For networks with a large bandwidth-delay product, it is recommended to activate the TCP enhancements as specified in RFC1323. For example, the network on an AIX machine can be configured with the `no` command. This command sets or displays current network attributes in the kernel. Details about the `no` command are available in the `man` page of `no` of your operating system.

This table shows the network attributes with their recommended values:

Table 17. Tuning of Network Settings

Attributes	Value	Description
`rfc1323`	`1`	Enables TCP enhancements as specified by RFC 1323, TCP Extensions for High Performance. The default is `0`. A value of `1` specifies that all TCP connections will attempt to negotiate the RFC enhancements.
`sb_max`	`131072`	Specifies the maximum buffer size allowed for a socket. The default is 65536 bytes. From the point of view of performance recommendations, the `sb_max` value should be twice the `TCPWindowsize` set within the Tivoli Storage Manager configuration file `dsm.sys`.

Set these values issuing these commands by the root user on the appropriate machine:

```
no -o rfc1323=1
no -o sb_max=131072
```

The `no` command does not perform range checking. It therefore accepts all values. If used incorrectly, the command might cause the system to become inoperable. These changes will be lost at system reboot. To make changes permanent, edit the `/etc/rc.net` file.

SP Switch (RISC 6000)

If an SP switch (RISC 6000) is used, the following two values should be set as shown in this table:

Table 18. Tuning of SP Switch Buffer Pools

Attributes	Value	Description
`rpoolsize`	`1048576`	The receive pool is a buffer pool for incoming data. The size for values is in bytes.
`spoolsize`	`1048576`	The send pool is a buffer for outgoing data. The size for values is in bytes.

The buffer pool settings can be changed using the `chgcss` command. After the changes, it is necessary to reboot the node.

Appendix A. Messages

Data Protection for *SAP®* (Oracle) Messages

Information about how to locate how to find message files (log files) and descriptions of the individual messages issued by Data Protection for *SAP®* for Oracle is provided.

The messages begin with the prefix **BKI** and are listed in numerical order. For each message, the following information is provided:

- Message number
- Severity code

  The following letters give an indication of the severity of the action that generated the message. The severity codes and their meanings are as follows:

E	Error	Processing cannot continue.
W	Warning	Processing can continue, but problems may occur later.
I	Information	Processing continues. User response is not necessary.

- Explanation
- User Response

How to find files containing message output (log files)

Data Protection for *SAP®* for Oracle process results are logged in files. These files are located in the path indicated by the TDP_DIR environment variable. After the installation, TDP_DIR points to the subdirectory `tdplog` of the path for the Data Protection for SAP configuration files. If TDP_DIR is not set, or if a log file cannot be created in the path pointed to by TDP_DIR, the log files are created in path `/tmp` (UNIX or Linux) or in the path pointed to by environment variable TEMP (Windows). Information on how to set or change the TDP_DIR value is available in "Prerequisites" on page 24. The Data Protection for SAP shared library writes to the `tdpdb2.<SID>.<node name>.log` log file. The Backup Object Manager writes to the `backom.log` log file.

Data Protection for SAP process results are logged in files. These files are located in the following paths:

- UNIX or Linux: `$SAPDATA_HOME/sapbackup` for backup and restore runs
- UNIX or Linux: `$SAPDATA_HOME/saparch` for redo log archive runs

Windows:

- `%SAPDATA_HOME%\sapbackup` for backup and restore runs
- `%SAPDATA_HOME%\saparch` for redo log archive runs

All log files written during a backup, restore or archive operation are listed in summary log files with start and end timestamps. The summary log files are located in the same directory as the log files themselves and have the following names:

- `back<SID>.log`
- `rest<SID>.log`
- `arch<SID>.log`

If you are running Oracle RMAN, the log file `sbtio.log` (which is specified by `user_dump_dest` in the Oracle control files) might also need to be viewed. For most installations, this file is defined as `$SAPDATA_HOME/saptrace/usertrace/sbtio.log`. This file contains all messages issued by the Data Protection for SAP RMAN connector during operation of Oracle RMAN.

BKI0000E Profile not specified.

Explanation:

Cannot locate the profile.

User response:

Ensure that a profile is available. (Oracle) Note that the BACKINT call must have the following form: *backint -p init<SID>.utl* .

BKI0004E Function not defined.

Explanation:

BRTOOLS, BRBACKUP, or BRARCHIVE passed an invalid argument to Data Protection for SAP.

User response:

Ensure that you have the correct version of BR*Tools installed. Valid functions are: *-f backup* or *-f restore* or *-f password* or *-f delete* or *-f inquire*.

BKI0005I Start of program at: *time*

Explanation:

Data Protection for SAP received control from a BR*Tools utility at the time denoted.

User response:

None.

BKI0006E Type for backup not defined [*type***]. Please use 'file' or 'file_online'.**

Explanation:

Data Protection for SAP expects as the backup type parameter only *file* or *file_online*.

User response:

If you start Data Protection for SAP manually to do a backup, ensure that the type option (`-t`) receives the correct arguments (file or file_online). If your Data Protection for SAP has been invoked by one of the SAP database utilities (for example, **BRBACKUP**), ensure that the SAP backup profile `init<SID>.sap` is customized correctly) .

BKI0007E Mode *mode* **requires the environment variable** *environment variables* **to be set.**

Explanation:

Not all environment variables required have been set. At least *environment variables* where missing.

User response:

Set the missing environment variables.

BKI0008E The environment variable *name* **is not set correctly. The current value is** *value***.**

Explanation:

The value of the environment variable *name* is wrong.

User response:

Set *name* to an appropriate value.

BKI0020I End of program at: *time*

Explanation:

(Oracle) Data Protection for SAP returned control to a BR*Tools utility at the time denoted. (DB2) Program tdppasswd ended at the time indicated.

User response:

None.

BKI0021I Elapsed time: *elapsedtime*

Explanation:

The time needed for the complete backup was *elapsedtime*.

User response:

None.

BKI0023I Time: *current_time***Done:** *saved_bytes (percent) of bytes***Estimated end time:** *end_time*

Explanation:

Finished saving a specific object at *current_time*. The *saved_bytes* amount of the total number of *bytes* have been saved. *percent* shows the percentage. This call will be completed at the estimated *end_time*.

User response:

None.

BKI0024I Return code is: *return code*

Explanation:

A return code of 0 means no errors or warnings occurred. If the return code is 1, at least one warning

was issued by the program. If the return code is 2, at least one error message was issued.

User response:

For return codes other than 0, check the run log for warnings or error messages.

BKI0027I **Time:** *current_time* **Objects:** *current_num* **of** *total_num***in process:** *file_name***MGMNT-CLASS:** *management_class***TSM Server:** *server name***.**

Explanation:

Data Protection for SAP started saving *current_num* files at *current_time*. The total number of files to save is *total_num*. The file *file_name* is currently being processed. The files are transferred to the Tivoli Storage Manager server *server name*, which stores them in the management class *management_class*.

User response:

None.

BKI0032E **Error opening file** *file name***:** *system error description*

Explanation:

A system error occurred during opening of the file *file name*. *system error description* will describe the error in more detail.

User response:

Read the *system error description*.

BKI0048E **No password for node <node> on server <server> given on command line. When entering passwords in batch mode, you must supply values for ALL stanzas in the profile.**

Explanation:

The batch mode of the password function requires a data set for all TSM server stanzas in the profile.

User response:

Check the profile for active server stanzas. Use that information and try it again.

BKI0049I **Please enter password for node** *nodename* **on server** *server name*

Explanation:

The password for the node *nodename* on the Tivoli Storage Manager server *server name* has to be entered for storing it in the DP for SAP configuration file.

User response:

Enter the password for the corresponding Tivoli Storage Manager server.

BKI0050I **Please enter password for node** *nodename* **on server** *server name* **again**

Explanation:

In order to avoid typing errors, you have to enter the password twice.

User response:

Enter the password again.

BKI0051I **Password successfully verified for node** *nodename* **on server** *server name***.**

Explanation:

The password for the node *nodename* on the Tivoli Storage Manager server *server name* was changed successfully.

User response:

None.

BKI0052E **Password verification for node** *nodename* **on server** *server name* **failed.**

Explanation:

The password you entered for the node *nodename* on the Tivoli Storage Manager server *server name* was wrong.

User response:

Enter the password again. If this error still exists, contact your Tivoli Storage Manager administrator.

BKI0053I **Time:** *current_time***Objects:** *current_num* **of** *total_num***done:** *file_name* **with:** *bytes* **saved withdescription** *object_desc***.**

Explanation:

Data Protection for SAP completed saving *current_num* file at *current_time*. The total number of files to be saved is *total_num*. The file *file_name* with the size *bytes* is saved with the description *object_desc*.

User response:

None.

BKI0054I **Time:** *current_time***Objects:** *current_num* **of** *total_num***done:** *file_name* **with:** *bytes***restored with description** *object_desc***.**

Explanation:

Data Protection for SAP completed restoring of *current_num* file at *current_time*. The total number of files to be restored is *total_num*. The file *file_name* with

the size *bytes* is restored with the description *object_class*.

User response:

None.

BKI0055I **Object** *objectname* **with** *size* **saved with description** *description***.**

Explanation:

The object *objectname* was saved successfully.

User response:

None.

BKI0056I **Object** *objectname* **with** *size* **restored with description** *description***.**

Explanation:

The object *objectname* was restored successfully.

User response:

None.

BKI0057I **Time:** *current_time* **Object** *objectname* **with** *size* **saved with description** *description***.**

Explanation:

The object *objectname* was saved successfully.

User response:

None.

BKI0058I **Time:** *current_time* **Object** *objectname* **with** *size* **restored with description** *description***.**

Explanation:

The object *objectname* was restored successfully.

User response:

None.

BKI0059E **You have to set the environment variable DSMI_CONFIG to the full filename of the Tivoli Storage Manager client option file 'dsm.opt'.**

Explanation:

Tivoli Storage Manager client option file not found.

User response:

Verify that the Tivoli Storage Manager option file `dsm.opt` is pointed to by DSMI_CONFIG.

BKI0060E **The parameter** *parameter* **is not known.**

Explanation:

The command parameter *parameter* is unknown.

User response:

Check the specified command parameter and try again.

BKI0061W **The output file** *file name* **is not valid.**

Explanation:

The specified output file *file name* could not be created.

User response:

Check that *file name* is a valid file name on your operating system. Also check that the application has the appropriate permissions to create the file within the specified directory. The directory must already exist. If the file already exists, rename the old one.

BKI0062E **The input file** *file name* **is not valid.**

Explanation:

Unable to read the input file *file name* correctly.

User response:

Check the path and name of the input file and the appropriate file access permission.

BKI0063E **The UTL file** *file name* **is not valid.**

Explanation:

Unable to read the input file *file name* correctly.

User response:

Check the path and name of the profile (UTL file) and the appropriate file access permission.

BKI0064E **The option** *option* **is unknown.**

Explanation:

An option is invalid or unknown.

User response:

Check the specified option(s) and try again.

BKI0065E **The argument is missing for option** *option***.**

Explanation:

Every option requires an argument.

User response:

Insert the missing argument and try again.

BKI0101I Session *session*: Please enter 'cont' to continue or 'stop' to cancel.

Explanation:

If Data Protection for SAP is running in unattended mode (profile keyword BATCH), it terminates the current run if operator intervention is required.

User response:

Enter 'cont' or 'stop'.

BKI0102I Your reply: *reply*.

Explanation:

The reply you made is confirmed.

User response:

None.

BKI0311E Request canceled by user.

Explanation:

(Oracle) BACKINT terminated at user's request. (DB2) Program terminated at user's request.

User response:

None

BKI0400I TDP is waiting for BRBACKUP

Explanation:

Data Protection for SAP is waiting for BRBACKUP to set a table space in the begin/end backup mode.

User response:

None.

BKI0405I TDP waited *num_sec* sec. for BRBACKUP in util_file_online communication.

Explanation:

This message indicates the total amount of time DP for SAP waited for BRBACKUP to set a table space in "begin backup" or "end backup" mode. The wait time given is the sum of the wait times for all table spaces participating in the backup.

User response:

None.

BKI0410E Cannot open or delete switch file *file name*. Check permissions.

Explanation:

If Data Protection for SAP is not installed correctly (as the root user on UNIX or Linux or administrator group on Windows) then Data Protection for SAP is not able to open the necessary communication file to the SAP system.

User response:

Check the file permission.

BKI0411E Maximum time waiting for BRBACKUP expired.

Explanation:

The SAP database utilities did not respond within the expected time.

User response:

Contact your SAP administrator.

BKI0412E BRBACKUP wasn't able to switch requested table space in BEGIN/END BACKUP mode.

Explanation:

Data Protection for SAP could not continue the backup, because BRBACKUP was not able to switch the requested table space in BEGIN or END backup mode. This is necessary for locking the table space.

User response:

Contact your SAP administrator.

BKI0413E Error while requesting table space switch.

Explanation:

BRBACKUP could not switch table space in BEGIN or END backup mode.

User response:

Contact your SAP administrator.

BKI0414E Error while requesting table space switch.

Explanation:

BRBACKUP reported an error while trying to switch a table space in BEGIN or END backup mode.

User response:

Contact your SAP administrator.

BKI0450I Version 2 restore: *file*

Explanation:

A restore of data backed up with Data Protection for SAP version 2 was executed.

User response:

None.

BKI0452E **This version of *product* has expired.**

Explanation:

This is a test version that has expired.

User response:

Order a release version of the product or contact your IBM/Tivoli Sales Representative.

BKI0453W **This version of *product* will expire in *number* days.**

Explanation:

This is a test version with a time limit. It will expire in *number* days.

User response:

Order a release version of the product or contact your IBM/Tivoli Sales Representative before the version expires.

BKI0454I ***** This copy is NOT FOR RESALE. *****

Explanation:

This version is not for resale.

User response:

None.

BKI0455E **License file *file name* does not exist.**

Explanation:

The license file `agent.lic` was not found where expected.

User response:

Make sure that the `agent.lic` file resides in the same directory as the `init<SID>.utl` file.

BKI0456E **Unable to access license file *file name*.**

Explanation:

The license file could not be accessed.

User response:

Make sure the access permissions allow read/write access.

BKI0457E **License file *file name* contains invalid data/checksum.**

Explanation:

The license file is invalid.

User response:

Make sure you have the right `agent.lic` file for the right platform installed. `agent.lic` files are platform dependent.

BKI0458I **Fake-Mode is activated.**

Explanation:

This message signals that the current operation is a simulated operation. Simulations can be performed using the Administration Assistant.

User response:

None.

BKI0459E **More than one mux file is found with the same name *detailed backup description*.**

Explanation:

Two or more data sources with name *detailed backup description* exist.

User response:

Contact the product administrator.

BKI0460E **No mux file was found with the name <name>.**

Explanation:

A mux file is a data structure holding internal metadata needed for restore puposes. Each backup image gets a mux file assigned.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI0461I **Created tracefile '<tracefile>' for process ID <id>.**

Explanation:

The named trace file has been created.

User response:

None.

BKI1000E **Syntax error in line *line*: *statement***

Explanation:

The statement *statement* in the Data Protection for SAP profile is unknown or incorrect.

User response:

Correct the error and try again.

BKI1001E **Syntax error in file** *file name***. Exiting Program.**

Explanation:

A syntax error has been detected in the file *file name* and the action has been halted.

User response:

Correct the error(s) in the file *file name* and try again.

BKI1002E **BACKUPIDPREFIX must be** *number_of_characters* **characters.**

Explanation:

The length of BACKUPIDPREFIX must be *number_of_characters* characters.

User response:

Enter a BACKUPIDPREFIX with the required length (for example, SAP___, BKI___).

BKI1003W **Please set REDOLOG_COPIES to a number between 1 and** *max_copies***. Now it is set to** *act_copies***.**

Explanation:

Data Protection for SAP currently supports 1 to 9 copies of offline (redo) log files.

User response:

Adapt the REDOLOG_COPIES settings in the Data Protection for SAP profile.

BKI1004W **You should specify the BACKUPIDPREFIX before the TRACEFILE statement, so that the BACKUPIDPREFIX can be used in the tracefile name.**

Explanation:

The BACKUPIDPREFIX is used to build the Name of the tracefile. Therefore, BACKUPIDPREFIX must be specified before the TRACEFILE statement.

User response:

Define a 6-character BACKUPIDPREFIX in the Data Protection for SAP profile (for example, SAP___, BKI___)

BKI1005W **The tracefile name** *trace_filename* **should be absolute.**

Explanation:

None.

User response:

Specify an absolute tracefile name, for example `/oracle/C21/saptrace/tracefile` or `/db2/C21/saptrace/tracefile` .

BKI1006E **The SERVERNAME must be less than** *max_char* **characters.**

Explanation:

You have used a SERVERNAME with more than *max_char* characters.

User response:

Use a shorter SERVERNAME.

BKI1007E **The NODENAME must be less than** *max_char* **characters.**

Explanation:

You have used a NODENAME with more than *max_char* characters.

User response:

Use a shorter NODENAME.

BKI1008E **The MANAGEMENTCLASSNAME must be less than** *max_char* **characters.**

Explanation:

You have used a MANAGEMENTCLASSNAME with more than *max_char* characters.

User response:

Use a shorter MANAGEMENTCLASSNAME.

BKI1009W **Please set MULTIPLEX to a number between 1 and** *max_multiplex***. Now it is set to** *act_multiplex***.**

Explanation:

You have set multiplexing to an unsupported number. Data Protection for SAP now uses *act_multiplex*.

User response:

Set multiplexing to a number between 1 and *max_multiplex*.

BKI1010W **The configfile name** *configuration_filename* **should be absolute.**

Explanation:

None.

User response:

Specify an absolute file name, for example `/oracle/C21/dbs/initC21.bki` or `/db2/C21/dbs/initC21.bki`

BKI1011W **The sortfile name** *sortfile_filename* **should be absolute.**

Explanation:

None.

User response:

Specify an absolute file name, for example `/oracle/C21/dbs/sortfile`.

BKI1012E **Configfile not found or permission denied:** *configuration_filename***.**

Explanation:

Data Protection for SAP is unable to read the file *configuration_filename*.

User response:

This error could have various reasons, try the following:

1. Check the path of the configuration file. The path must be specified in the profile (parameter CONFIG_FILE).
2. Make sure that the file access permissions are set correctly.

BKI1013E **Profile not found or permissions denied:** *profile_filename***.**

Explanation:

Data Protection for SAP is unable to open the profile *profile_filename*.

User response:

(Oracle) Ensure that the SAP backup profile `init<SID>.sap` contains a valid entry `util_par_file` for the Data Protection for SAP profile. (DB2) Ensure that the vendor environment file contains a valid entry `XINT_PROFILE`. Furthermore, this file must be readable by Data Protection for SAP.

BKI1016W **The trace file name** *file name* **could not be opened for writing!**

Explanation:

The trace file could not be opened for writing.

User response:

Ensure that you have specified a correct path for the trace file.

BKI1017E **The server <server> is already defined. Please use another name or specify TCP_ADDRESS!**

Explanation:

The named server was already defined in the profile. Server stanzas with identical names are not allowed unless the keyword TCP_ADDRESS is defined in one of them.

User response:

Update the profile accordingly and try again.

BKI1019E **Failed to respond to a message received from XINT.**

Explanation:

This messages indicates an internal error.

User response:

Contact IBM Support.

BKI1020W **The compress info file** *file name* **should be absolute !**

Explanation:

The argument for the parameter COMPR_INFO in the profile is an relative filename.

User response:

Always use an absolute filename as argument for the parameter COMPR_INFO.

BKI1021E *component_name* **terminates the connection due to a previous error.**

Explanation:

A serious error has occurred which caused a shutdown of the communication channel between the *component_name* process and this application.

User response:

Look for previous error messages to detect the root cause of the problem.

BKI1022E *component_name* **terminates the connection due to a previous error.**

Explanation:

See message BKI1021E.

User response:

See message BKI1021E.

BKI1023W **Could not establish connection to log server** *log server name***.**

Explanation:

In the Data Protection for SAP profile, log server *log server name* is specified (keyword LOG_SERVER). However, a connection to the server named could not be established. No log records are sent to the log server.

User response:

- Check that the server name defined with keyword LOG_SERVER is spelled correctly in the Data Protection for SAP profile.
- Make sure there is a SERVER section in the profile for the log server defined with keyword LOG_SERVER.
- Check the corresponding SERVER section and correct any setup problems.
- Make sure that the log server named is available.

BKI1024E The file <filename> occurs twice in the <infile>.

Explanation:

The named file name occurs multiple times in the infile which is a violation of the interface specification.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI1200E Cannot read/write file: *file name***.**

Explanation:

The program is unable to read or write a data file (file name) of a table space being backed up or restored.

User response:

Check the file access permission of the affected file(s). Try again. If the problem still exists, contact the product's administrator.

BKI1201E There are no Tivoli Storage Manager Servers available.

Explanation:

Data Protection for SAP cannot locate a Tivoli Storage Manager server. This may be due to a configuration problem or to a problem while trying to connect to the Tivoli Storage Manager server. Most probably, a preceding error message points to the cause of the problem.

User response:

Look for and respond to preceding error messages. You may also want to check the Data Protection for SAP profile and the IBM Tivoli Storage Manager client options and client system options files.

BKI1202E You must specify either MAX_SESSIONS, or all three specific session options (MAX_ARCH_SESSIONS, MAX_BACK_SESSIONS, and MAX_RESTORE_SESSIONS).

Explanation:

Information on the number of Tivoli Storage Manager client sessions to be established by Data Protection for SAP is missing from the profile.

User response:

In the Data Protection for SAP profile, either specify a value for keyword MAX_SESSIONS, or specify values for the three specific session parameters (MAX_ARCH_SESSIONS, MAX_BACK_SESSIONS, and MAX_RESTORE_SESSIONS).

Any of the specific options can be specified in combination with MAX_SESSIONS. Then, it overrides the value of MAX_SESSIONS for the specific function.

BKI1203E Not enough sessions available (number of sessions required and number of sessions available).

Explanation:

The sum of available sessions specified in the various server statements (parameter SESSIONS) does not cover the required number of sessions (parameter MAX_SESSIONS).

User response:

Change the values of the corresponding parameters in the Data Protection for SAP profile, so that the condition mentioned in the explanation is fulfilled.

BKI1205E If you want *num_redo* **REDOLOGCOPIES on Tivoli Storage Manager-Server servername, you should give me at least** *num_mc* **different Archive Management Classes.**

Explanation:

Data Protection for SAP requires that the number of different Archive Management Classes (parameter BRARCHIVEMGTCLASS) on the Tivoli Storage Manager servers is equal to or greater than the number of redo log or log file copies (parameter REDOLOG_COPIES).

User response:

Define at least as many different Archive Management Classes as log file copies requested.

BKI1206W If you want *num_redo* **REDOLOGCOPIES on Tivoli Storage Manager Server** *server name***, you should give me at least** *num_mc* **different Archive Management Classes.**

Explanation:

The message appears during a BRBACKUP run. A BRARCHIVE run afterwards would fail.

User response:

Define at least as many different Archive Management Classes as log file copies requested.

BKI1207E Directory backup not supported

Explanation:

This option is not yet available.

User response:

Wait for a future release of Data Protection for SAP, which supports this option.

BKI1208W The object *file name* will be retried [*retry_num*]

Explanation:

An error occurred while processing object *file_name*. Data Protection for SAP is repeating the action according to the number of retries specified in the profile. *retry_num* is the current retry count.

User response:

If the problem persists check for and respond to preceding error messages

---

BKI1209E Object not found or not accessible *objectname*.

Explanation:

The object cannot be located.

User response:

The backup integrity is affected. Contact SAP or IBM Support.

BKI1210E Input file not found or not accessible *file name*.

Explanation:

Data Protection for SAP cannot locate the temporary file named. This file contains the list of Oracle objects to be backed up or restored. It is passed to DP for SAP by one of the BR*Tools utilities.

User response:

Ensure that you have the correct version of BR*Tools installed. For details, check with the release notes (RELNOTE).

BKI1211E There is something wrong with your CONFIG_FILE *file name*.

Explanation:

There is a problem with your Data Protection for SAP configuration file setup.

User response:

Check the file permission and the file name specified in the Data Protection for SAP profile keyword CONFIG_FILE.

BKI1212W The file *file name* was not found in the manual sorting file.

Explanation:

The file you want to back up was not found in the manual sorting file.

User response:

Check and correct the manual sorting file so that it contains all the files you are backing up.

BKI1214E TSM Error: *error text*

Explanation:

The specified TSM error occurred.

User response:

Check *error text* and correct the problem. For further information you may want to refer to *IBM Tivoli Storage Manager Messages*, SC32-9090.

BKI1215I Average transmission rate was *number* GB/h (*number* MB/sec).

Explanation:

The average transmission rate is displayed.

User response:

None.

BKI1216E There are no BRBACKUPMGTCLASSES available.

Explanation:

The BRBACKUPMGTCLASSES you have specified in your `init<SID>.utl` file are not correct.

User response:

Check the management classes on the TSM server and specify correct ones.

BKI1217E There are no BRARCHIVEMGTCLASSES available.

Explanation:

The BRARCHIVEMGTCLASSES you have specified in your init<SID>.utl file are not correct.

User response:

Check the management classes on the TSM server and specify correct ones.

BKI1218E Environment variable TEMP not set.

Explanation:

The required environment setup is incomplete.

User response:

Set the environment variable TEMP and try again.

BKI1222E Version mismatch error. Check setup (version_1:version_2).

Explanation:

Different components with inconsistent versions are used.

User response:

Check your setup or contact IBM Support.

BKI1223W A problem occurred during send of performance data to Administration Assistant .

Explanation:

There was a problem sending the performance data to the Administration Assistant over the network.

User response:

Check your setup or contact IBM Support.

BKI1224W Unable to initialize connection to Administration Assistant.

Explanation:

No operational data could be sent to the Administration Assistant during database backup or restore .

User response:

Check the logs for further information and try again.

BKI1227I Average compression factor was *number***.**

Explanation:

The data transferred had been compressed by the factor *number*.

User response:

None

BKI1228W Server *server name* **can not be used with password access method GENERATE in this environment. The process is running with user ID** *number* **but the effective user ID is** *number***.**

Explanation:

The user ID and the effective user ID of the process are different. In order to utilize the password access method GENERATE the IDs must be equal.

User response:

Change the value for the parameter ″PASSWORDACCESS″ in the file dsm.sys (UNIX and Linux) or *servername*.opt (Windows) from 'generate' to 'prompt'. Reset the password for this node at the Tivoli Storage Manager server and run (for Oracle) `backint -f password` or (for DB2) `backom -c password` . This prompts you for the password and stores it encrypted in the Data Protection for SAP configfile. Each time your password expires you have to repeat the last step.

BKI1229E Value for parameter BUFFSIZE (actual *cur_number***, maximum** *max_number***) is too large for BUFFCOPY mode PREVENT.**″

Explanation:

To utilize the BUFFCOPY mode PREVENT the value for the parameter BUFFSIZE must not be larger than *max_number*.

User response:

In the Data Protection for SAP profile, specify a BUFFSIZE less or equal to *max_number* if you need to prevent copying buffers when passing data between Tivoli Storage Manager components. If you need large buffers you can set option BUFFCOPY to SIMPLE or AUTO. As a consequence, buffers are copied when data is passed between Tivoli Storage Manager components.

BKI1230E The following file was not processed: *path***.**

Explanation:

The operation was terminated due to a previous error. As a consequence, the file named could not be processed. The cause of the error should be found in an earlier message.

User response:

Check for and respond to preceding error messages.

BKI1231E Maximum number of retries for file <filename> exceeded.

Explanation:

The number of retries configured in the profile keyword 'FILE_RETRIES' for the named file were reached.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support person

---

BKI1505E **Operation aborted because a different operation by this database client is already running.**

Explanation:

Different concurrent operations of the same type were started for the same database. This is not supported. The current operation is aborted.

This message is also issued when a cooperative operation of two or more participating partitions was started, but the profile settings used for the various partitions do not match.

User response:

Wait until the currently running operation has ended and try again. Make sure that multiple operations are not started concurrently for a database.

If this is a cooperative operation with two or more participating partitions, check that the profile settings of the various partitions (for example, DEVICE_TYPE, MAX_VERSIONS, etc.) do not differ. If they do, fix the profile settings, cancel the current operation, and start the operation again. Also, investigate the possibility of sharing the same profile among all partitions.

BKI1506E **Failed to execute command** *command***. Output follows:**

Explanation:

The system tried to execute the command cited. During execution, an error occurred. The output received from the command shell is listed following the message.

User response:

Determine the cause of the problem from the command and the output listed in the message, and resolve the problem.

BKI1507E **The process needs to run with root authority.**

Explanation:

The current process requires root authority.

User response:

Start the process under an account with root authority.

BKI1508E **The service** *service_name* **has terminated due to a previous error. Please check all logs for additional information.**

Explanation:

The cited service is no longer available.

User response:

Check the appropriate logs for the cause of its termination.

BKI1509E **Authentication failure. The password specified does not qualify for accessing** *component***.**

Explanation:

To access the named component, a password is required. However, the password provided could not be verified.

User response:

Make sure that the password files used by the different components of the system match.

BKI1510I **New connection received.**

Explanation:

The server received a new connection request.

User response:

None.

BKI1511I **New** *type_of_operation* **operation started for database instance** *instance***, database** *database_name***.**

Explanation:

A connection request resulted in the start of a new operation of the type indicated.

User response:

None.

BKI1512E **An error occurred during shutdown:** *Error information*

Explanation:

During shutdown of the component, a problem occurred. The error information is given.

User response:

Resolve the problem indicated by the error information.

BKI1513I **Database client connected: Instance** *instance***, database** *database_name***, partition** *partition_number*

Explanation:

This message follows a message BKI1511I and indicates the connection of one of the database clients taking part in the operation. A database client is an instance of the snapshot backup library representing a single partition of the database.

User response:

None.

BKI1514I Device client connected.

Explanation:

This message follows a message BKI1511I and indicates the connection of one of the device clients taking part in the operation. A device client is an instance of the device agent for the storage device.

User response:

None.

BKI1515I Client is logging to *file_name***.**

Explanation:

The client's log messages are written to the indicated file.

User response:

None.

BKI1517I Deleting target data container defined by *container_description***.**

Explanation:

The data in the container indicated is removed.

User response:

None.

BKI1518E Internal error: The system is trying to use the same device agent, although the synchronization mode is not PARALLEL.

Explanation:

The system has been told to use the same device agent for multiple database clients, but the database indicated serial synchronization mode. This setup is not supported.

User response:

Contact your IBM support personnel.

BKI1519E A failure occurred during initialization of one or more of the nodes participating in this operation. Please check the logs for more information.

Explanation:

Some problem occurred during the initialization of a new operation. The problem may be with any component required for this operation.

User response:

Check the acsd log file for messages BKI1515I to determine the log file names of the participating agents. Check the log files of each component for the cause of the problem.

BKI1520E Volume *volume_name* **is shared across partitions. Volume sharing is not allowed.**

Explanation:

At least two partitions own data residing on the volume indicated. This setup is not supported.

User response:

With the current disk layout of the database, the requested function cannot be used. If you want to use the function, change the disk layout of the database so that each data volume is dedicated to a partition.

BKI1521I Retaining *number* **backups**

Explanation:

When enforcing profile parameter MAX_VERSIONS, the indicated number of backups is kept.

User response:

None.

BKI1522E The requested meta-information (subject=*"description"***) is not available.**

Explanation:

Some meta-information about each backup is stored in the repository. An error occurred when trying to retrieve part of this information.

User response:

Contact your IBM support personnel.

BKI1523W Warning: The following containers were reused without being explicitly released: *description*

Explanation:

The containers defined by the description are used by the current backup. They were used before by a different backup. This message is expected in SAN environments where data containers are usually kept until they are reused. In this case, this message does not indicate a problem.

User response:

None.

BKI1525E The process *service_name* **is in an inconsistent state. Please check for previous errors and restart the process afterwards.**

Explanation:

The process indicated cannot continue with inconsistent data.

User response:

Check the logs for messages pointing to the cause of the inconsistency. After resolving any problems, restart the process.

BKI1526E **A configuration file (profile) must be provided.**

Explanation:

An operation was started without providing a profile.

User response:

Check the user documentation on how to provide the profile to the current process. Start the process again using a valid configuration file.

BKI1529E **The device '***device_type***' you entered is not supported by the wizard.**

Explanation:

The device type represents a certain type of storage device. While using the setup wizard, a device type was entered that is not supported by the current version of the wizard.

User response:

Refer to your user documentation for a list of the device types that are supported by default. Specify one of the supported types.

BKI1530E **Failed to launch the device agent for** *device_type***. Please consult your user documentation to make sure that all requirements for the specified device are met.**

Explanation:

The system was unable to launch the appropriate device agent for the type indicated because some of its requirements are not met.

User response:

Refer to your user documentation and make sure that the system is set up correctly for the specified device type.

BKI1534E **Unexpected version** *actual_version* **of the repository located in** *path***. Expected version:** *supported_version*

Explanation:

The server located the repository in the path indicated. However, the version of the repository located on disk does not match the current version of the server.

User response:

Make sure to use the correct instance of the server. Ensure that the path of the repository was specified correctly. Refer to the release notes for a list of possible incompatibilities.

BKI1535E **Unexpected characteristics (bitwidth=***number***) of the repository located at** *path***. Expected bitwidth:** *number*

Explanation:

The repository located in the path indicated was saved to disk using a bit width different from the bit width the server is using to load the repository.

User response:

Make sure to use the correct instance of the server. Ensure that the path of the repository was specified correctly. Refer to the release notes for a list of possible incompatibilities.

BKI1536E **The repository located at** *path* **is not valid.**

Explanation:

A repository could not be found at the location indicated by *path*.

User response:

Ensure that the path of the repository was specified correctly. Do not edit any files in the repository *path*.

BKI1537E **The repository located at** *path* **was written with an incompatible protocol (***protocol_version***). Expected protocol:** *protocol_version*

Explanation:

The repository found at the location indicated was written to disk using the protocol version named. However, the server currently supports the expected protocol version.

User response:

Ensure that the path of the repository was specified correctly. Do not edit any files in the repository *path*.

BKI1538E **Unexpected repository type. The path '***path***' does not point to a repository of type** *"protocol_type"***.**

Explanation:

The repository located in the path indicated was written to disk using a protocol different from the protocol supported by the server process.

User response:

Make sure to use the correct instance of the server. Ensure that the path of the repository was specified

correctly. Refer to the release notes for a list of possible incompatibilities.

BKI1539E **Root privileges required. Could not change user ID to root.**

Explanation:

The requested operation requires root privileges. However, the process could not acquire them.

User response:

Make sure the appropriate privileges (s-bit) are granted to the executable.

BKI1540E **/etc/inittab entries are limited to 127 characters. Please consult your user documentation for information on manually completing the installation procedure.**

Explanation:

The command line generated by the setup function exceeds 127 characters. This situation requires user intervention. The setup function did not update /etc/inittab.

User response:

Refer to your user documentation for information on what entries to add to /etc/inittab.

BKI1541E **/etc/inittab was not updated because some of the processes have apparently already been added. Please re-run the setup after calling the setup script with option '-a disable' if you want to change to a standard setup.**

Explanation:

During the automatic setup, entries for this product were detected in /etc/inittab. This is an indication that the product was not previously uninstalled.

User response:

Run the setup with option '-a disable' and then start the installation process again. If the entries in /etc/inittab should be retained, refer to your user documentation for information on how to complete the installation manually.

BKI1542E **Failed to uninstall because some of the processes to be uninstalled are still listed in /etc/inittab. Please re-run the setup after stopping the component by calling the setup script with option '-a stop'.**

Explanation:

Before uninstalling the product, the affected processes must be stopped. This is done by running the setup script with the option '-a stop', which will remove the entries from /etc/inittab and stop the processes.

User response:

Refer to your user documentation for information on the uninstall process. Run the setup with the option '-a stop' and then continue uninstalling.

BKI1543E **The component is still referenced within the /etc/inittab. In order to terminate the component rerun the setup script with option '-a stop'.**

Explanation:

The setup utility detected that the product is still active in the system. Apparently, its entries in /etc/inittab are not yet removed.

User response:

Call this process again with the option '-f stop'.

BKI1544E **New entries cannot be added to /etc/inittab because it already contains too many entries starting with 'ac'. Please refer your user documentation for a manual setup of this package.**

Explanation:

During setup, an unusually high number of entries beginning with 'ac' were detected in /etc/inittab. /etc/inittab was not modified.

User response:

Determine if these entries are expected, or if they were added due to a problem. If these entries are required, refer to your user documentation for information on how to complete the installation manually.

BKI1545E **IBM Tivoli Storage Manager for Advanced Copy Services is currently running.**

Explanation:

This failure happens during (de)installation and indicates that not all TSM for ACS components could be stopped.

User response:

Check that no backup or restore is currently running and retry the operation. If you have customized the process of starting TSM for ACS, it might be necessary to manually stop it by undoing those customization steps.

BKI1546E **IBM Tivoli Storage Manager for Advanced Copy Services was not started.**

Explanation:

This failure happens during installation and indicates that not all TSM for ACS components could be started successfully.

User response:

Check that all TSM for ACS components have the appropriate access rights and retry the operation. Contact the support function if the operation continues to fail.

BKI1547E **Failed to remove the data associated with the deleted backup** *backup_id***.**

Explanation:

The backup named was deleted. However, its data could not be removed from the repository and from the storage device.

User response:

Look for a previous message pointing to the cause of the problem. Resolve any problems indicated there. Once the cause of this problem is resolved, the daemon will take care of the deleted backups eventually.

BKI1548E **Failed to monitor the data associated with the deleted backup** *backup_id***.**

Explanation:

A background daemon is supposed to monitor the states of backups in order to determine if data needs to be deleted from the storage device. However, the monitor was not able to access the appropriate data.

User response:

Look for a previous message pointing to the cause of the problem. Resolve any problems indicated there. Once the cause of this problem is resolved the daemon will take care of the deleted backups eventually.

BKI1549E **Failed to load** *component_name* **due to the following reason:** *error_information***.**

Explanation:

The system was unable to load the named component of the product.

User response:

Check the error information given in the message. Resolve any problem indicated.

BKI1550W **Unable to perform required operations for container '<container>' for <time>.**

Explanation:

Any operation for the named container is suspended for the named period of time due to it is locked.

User response:

As soon as the container was unlocked, retry the required operation.

BKI1553I *Component_name* **is logging to** *path***.**

Explanation:

The file denoted is the log file of the named component.

User response:

If you need to check the log of the indicated component, look for this message to identify the log file to examine.

BKI1554W **The agent '***component_name***' terminated with exit code** *number.*

Explanation:

The process denoted ended with the given exit code.

User response:

Check the agent's log for any messages pointing to a problem. Resolve any problem indicated.

BKI1555I **Profile successfully created. Performing additional checks. Make sure to restart all ACS components to reload the profile.**

Explanation:

The setup wizard created a new profile. The profile will be validated.

User response:

Restart the ACS components after the wizard ends, in order to activate the new settings.

BKI1556E **Some data of backup** *backup_id* **are unavailable. It is impossible to restore the data requested.**

Explanation:

The system detected that some of the data originally contained in the backup is no longer available. The occurrence of this message depends on the type of storage device employed. For example, if an earlier backup data was restored from an N-Series device, some data of a later backup will be destroyed.

User response:

The backup is no longer complete and cannot be used for the requested operation. Try the operation with a different backup.

BKI1557I Device agent is logging to *path*.

Explanation:

The device agent's log messages are written to the file named.

User response:

None.

BKI1558E There are no mount agents registered for participant(s) *participant_list*

Explanation:

During a snapshot backup run, TSM for ACS detected that for the listed participant(s) no TSM for ACS device agent was started with the 'force mount' (-F) option. Typically, a participant corresponds to a DB2 partition. The current snapshot backup run will be deleted.

User response:

Make sure that for each participant (DB2 partition) a TSM for ACS device agent is started with the mount force option (-M) on the offload system.

BKI1559E Failed to verify consistency of data container (*data_container*)

Explanation:

During a snapshot backup run, TSM for ACS detected that the listed data container (typically an AIX volume group or an N Series volume) could not be imported/mounted successfully on the offload system. The current snapshot backup run will be deleted.

User response:

Check the TSM for ACS device agent log/trace file for errors and restart the snapshot backup after the problem is corrected.

BKI1560E Not all file systems have been validated by the mount agents!

Explanation:

During a snapshot backup run, TSM for ACS detected that not all file systems could be mounted successfully on the offload system. The current snapshot backup run will be deleted.

User response:

Check the TSM for ACS device agent log/trace file for errors and restart the snapshot backup after the problem is corrected.

BKI1561E Profile name <profile_name> does not point to a file.

Explanation:

The profile specification should be a fully qualified filename. Otherwise, it is assumed to be relative to the current directory of the command that issues the message, which may not be the desired directory.

User response:

Correct the name.

BKI1562E Deleting the backup as requested is impossible while any part of it is mounted.

Explanation:

A request was sent to delete a backup. However, some parts of the backup were still mounted. Presumably, a restore operation or an off-loaded tape backup is pending or in progress. Please note that an offloaded tape backup requires the snapshot backups of all partitions of the database.

User response:

Wait until the operation in progress has ended, then issue the delete request again.

BKI1563I The snapshot backup defined by timestamp *timestamp* for instance *instance*, database *database_name*, and partition *partition_number* cannot be restored.

Explanation:

This message appears when backups are queried for a restore. It indicates that a snapshot backup was encountered that is not in a restorable state. For example, snapshot backups created with a FLASHCOPY_TYPE of NOCOPY are not restorable. When queried for restore, unrestorable snapshot backups are not returned to the caller and therefore cannot be selected for restore.

User response:

None.

BKI1564W Backup <id> is marked for deletion. You need to unmount before it can be physically deleted.

Explanation:

A snapshot backup with the named id can only be deleted if all of its assigned file systems are unmounted successfully.

User response:

Issue the offload agent with the command '-f

unmount'. After all resources are freed, the deletion of the snapshot backup will be started.

BKI1568I **Removing backup <*backup_id*> from the repository because it has not been found on the storage device during reconciliation.**

Explanation:

During reconciliation the backup with id <*backup_id*> has not been found on the storage device. Therefore it is deleted from the repository to keep the repository and the valid backups on the storage in sync.

User response:

None.

BKI1569I **Updating backup <*backup_id*> in the repository because some parts of it have not been found on the storage device during reconciliation.**

Explanation:

Some parts of the backup with id <*backup_id*> have not been found on the storage box. The backup will be marked as incomplete in the repository and is not restorable anymore.

User response:

None.

BKI1570W **The following container could not be deleted from the storage box during reconciliation: <*volume_name*>.**

Explanation:

The volume <*volume_name*> could not be deleted from the storage box. It is not needed anymore because there is no corresponding backup in the repository.

User response:

Ignore the warning or try to delete the volume from the storage device manually.

BKI1571W **The specified value for 'RECON_INTERVAL' is 0. Be aware that every time a background monitor is started a reconcile will be scheduled so that other background operations will never be scheduled. This should be used for testing purposes only.**

Explanation:

If RECON_INTERVAL is 0 every time a background monitor is started it will start reconciliation. Other background operations as deletion or monitoring will never be scheduled.

User response:

Change RECON_INTERVAL to a value greater than 0 if you want to avoid this behavior.

BKI1572I **Starting reconciliation for device class <*device_class_name*>.**

Explanation:

The reconciliation will be started for the device class <*device_class_name*> of the profile.

User response:

None.

BKI1573I **The container <*volume_name*> has been successfully deleted from the storage box. It didn't belong to any backup in the repository.**

Explanation:

The volume <*volume_name*> has been successfully deleted from the storage box during reconciliation because it didn't belong to any backup in the repository.

User response:

None.

BKI2000I **Successfully connected to** *component_name* **on port** *portnumber*.

Explanation:

One of the Data Protection for SAP modules BACKINT or the backup library *libtdp_r3* initiated a successful connection to the background process *component_name* on port *portnumber*.

User response:

None.

BKI2001E **Socket error while connecting to** *component_name*: *reason*.

Explanation:

The background process *component_name* is not running.

User response:

Start *component_name* manually and try again.

BKI2003I **File** *file_name, BID* **deleted.**

Explanation:

The file *file_name* with the backup ID *BID* was deleted from the Tivoli Storage Manager.

User response:

None.

BKI2007E Unknown Port: *port*

Explanation:

The port specified for communication between *component_name* and BACKINT or the backup library is unknown.

User response:

Check the port value specified when *component_name* was started. Additionally, check the environment variable *PROLE_PORT* for the BACKINT environment. These two values must match.

BKI2008E Unable to connect to *component_name***.**

Explanation:

Internal error.

User response:

Contact IBM Support.

BKI2009I Deleting all versions with version number <= *version_number* **on server** *server_name***.**

Explanation:

All full database backups and their corresponding log file backups will be deleted from Tivoli Storage Manager storage, if their version number is less than or equal to *version_number*.

User response:

None.

BKI2010E Error occurred processing FRONTEND

Explanation:

An error occurred during the frontend processing.

User response:

Check the frontend script/program and the settings in the Data Protection for SAP profile (keyword FRONTEND) and try again.

BKI2011E Error occurred processing BACKEND.

Explanation:

An error occurred during the backend processing.

User response:

Check the backend script/program and the settings in the Data Protection for SAP profile (keyword *BACKEND*) and try again.

BKI2012E Passwords do not match. Try again.

Explanation:

The first and second password you entered do not match.

User response:

Enter the password correctly.

BKI2013I Starting FRONTEND Program.

Explanation:

The frontend program is executing.

User response:

None.

BKI2014I FRONTEND program finished.

Explanation:

The frontend program is finished.

User response:

None.

BKI2015I Starting BACKEND program.

Explanation:

The backend program is executing.

User response:

None.

BKI2016I BACKEND program finished.

Explanation:

The backend program is finished.

User response:

None.

BKI2017I Blocksize is set to *num_bytes* **bytes.**

Explanation:

The operational blocksize is *num_bytes* bytes.

User response:

None.

BKI2022E Unable to change mode of file *file name***:** *description*

Explanation:

Unable to change mode of file *'file name'*. *'description'* may contain the system error text.

User response:

Check the '*description*'. If the error persists, contact your service representative.

BKI2024E **Error in connection to** *component_name***.**

Explanation:

The connection to *component_name* terminated unexpectedly. This message might be displayed due to previous errors or after an unexpected termination of the *component_name* process.

User response:

Check for other error messages and restart *component_name* if necessary. Try again. If the problem persists, contact IBM Support.

BKI2025E **Failed to respond to a message received from** *component_name***.**

Explanation:

This is an internal error

User response:

Contact IBM Support.

BKI2026E **Unexpected exception in handler:** *handler*

Explanation:

This is an internal error.

User response:

Contact IBM Support.

BKI2027I **Using TSM API version** *your API version* **(compiled with** *compiled with version***).**

Explanation:

Version information about the TSM-API.

User response:

None

BKI2028W **Unable to terminate session** *session***.**

Explanation:

This is an internal error during cleanup that has no effect on the success of the service.

User response:

None

BKI2029E **The requested buffer allocator cannot be instantiated due to the following incompatibility:** *expression***.**

Explanation:

This is an internal error.

User response:

Contact IBM Support.

BKI2031E **A buffer allocator cannot simultaneously satisfy all of the following properties:** *list of properties*

Explanation:

This is an internal error.

User response:

Contact IBM Support.

BKI2033E **Cannot instantiate allocator of type** *allocator type* **with the following additional properties:** *list of properties*

Explanation:

This is an internal error.

User response:

Contact IBM Support.

BKI2913I **Version delete is configured to retain <number> backup generations. Checking for expired backups.**

Explanation:

The value assigned to the profile keyword MAX_VERSIONS is equivalent to the named number of backup generations (backup generation = full+incr+logs) to be retained on TSM.

User response:

None.

BKI4000W **The attributes of file** *file name* **cannot be restored. Reason: errno** *(error_num) error_desc***.**

Explanation:

The file *file name* was restored successfully but one or more file attributes (permission, ownership, date/time) of the file *file name* cannot be restored correctly.

User response:

Check the error number *error_num* and the error description *error_desc* to avoid this problem in the future. An initial solution could be to set the appropriate correct permission for the file *file name* manually.

BKI4001E **File** *file name* **cannot be created. Reason: errno (***error_num***)** *error_desc***.**

Explanation:

The file *file name* to be restored could not be

created/written. It is possible, that you do not have the appropriate rights for writing the file *file name* to the destination path.

User response:

Check the error number *error_num* and the error description *error_desc* to avoid this problem in the future. Furthermore, check the write permission of the user who started the restore.

BKI4002E **Error during write of file** *file name***. Reason: errno (***error_num***)** *error_desc***.**

Explanation:

An error occurs during the restore process of the file *file name*.

User response:

Check the error number *error_num* and the error description *error_desc* to avoid this problem in the future.

BKI4005E **Error allocating memory block for file** *file name***. BLOCKSIZE may be too large.**

Explanation:

Unable to request new memory blocks during the backup of file *file name*.

User response:

Verify that you have set a valid value for BLOCKSIZE. If you are not sure what value is valid, comment it out so the default value is used. Furthermore, you can check if you have enough RAM available with your machine. Also, check the memory usage during backup. It may be necessary to stop another application, increase memory, or change the configuration.

BKI4007E **File** *filename* **cannot be read. Reason: errno(***errno number***)** *errno text***.**

Explanation:

Data could not be read due to some system error. Check *errno text* for further information. If this error recurs, this might indicate some hardware problems.

User response:

Contact your system administrator.

BKI4008E **File** *filename* **cannot be opened. Reason: errno(***errno number***)** *errno text***.**

Explanation:

Could not open the file *file name* due to some system specific problems.

User response:

Contact your system administrator.

BKI4009E **Not enough space to write file** *file name***. Possible reasons: disk full or ulimit exceeded.**

Explanation:

The system rejected a request to write data into file *file name*. The storage media might not have enough free space to keep the file or the system rejected writing the file due to administrative resource constraints such as ulimits.

User response:

Contact your system administrator.

BKI4010E **SAP requires the file <filename> to be a regular file.**

Explanation:

To be able to support SAP environments the named file has to be a regular file.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI4011W **The backup device type (<filetype> <devicetype> <devsubtype>) differs from the restore device type (<filetype> <descr> <descr>) for <name>.**

Explanation:

A mismatch between the device types during backup and restore was detected.

User response:

Check the logs for further information.

BKI4012E **Unexpected EOF for file '<filename>' after reading <number> bytes.**

Explanation:

The end of file was reached unexpectedly.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI4013I **CreateFile() with dwFlagsAndAttributes='<attribute>'.**

Explanation:

A file with the nmed attribute was created.

User response:

None.

BKI4014E File '<filename>' cannot be accessed. Reason: errno(<number>) <errormsg>

Explanation:

A named file could not be accessed either for reading or writing.

User response:

Check the file permissions and if necessary adjust them accordingly. Try again.

BKI5000E Tivoli Storage Manager Error: *error_message*

Explanation:

During a connection of Data Protection for SAP to Tivoli Storage Manager server, a Tivoli Storage Manager error *error_message* occurred.

User response:

Use the Tivoli Storage Manager Messages guide and correct the Tivoli Storage Manager server error. Try your last action again.

BKI5001E Tivoli Storage Manager Error: *error_message*

Explanation:

During a connection of Data Protection for SAP to Tivoli Storage Manager server, a Tivoli Storage Manager error *error_message* occurred.

User response:

Use the Tivoli Storage Manager Messages guide and correct the Tivoli Storage Manager server error. Try your last action again.

BKI5002E Tivoli Storage Manager Error: *error_message*

Explanation:

See BKI5001E.

User response:

See BKI5001E.

BKI5003E Tivoli Storage Manager Error: *error_message*

Explanation:

See BKI5001E.

User response:

See BKI5001E.

BKI5004W Tivoli Storage Manager Error: *error_message*

Explanation:

See BKI5001E.

User response:

See BKI5001E.

BKI5005E Tivoli Storage Manager Error: *error_message*

Explanation:

See BKI5001E.

User response:

See BKI5001E.

BKI5006E Tivoli Storage Manager Error: *error_message*

Explanation:

See BKI5001E.

User response:

See BKI5001E.

BKI5007E Tivoli Storage Manager Error: *error_message*

Explanation:

See BKI5001E.

User response:

See BKI5001E.

BKI5008E Tivoli Storage Manager Error: *error_message*

Explanation:

See BKI5001E.

User response:

See BKI5001E.

BKI5009E Tivoli Storage Manager Error: *error_message*

Explanation:

See BKI5000E.

User response:

See BKI5000E.

BKI5010E **Tivoli Storage Manager Error:** *error_message*

Explanation:

See BKI5000E.

User response:

See BKI5000E.

BKI5011E **Tivoli Storage Manager Error:** *error_message*

Explanation:

See BKI5000E.

User response:

See BKI5000E.

BKI5012E **Cannot open TSM API message text file. Check if DSMI_DIR is set correctly. Current value of DSMI_DIR is:** *value*

Explanation:

The TSM-API could not be initialized.

User response:

Correct the value of the environment variable DSMI_DIR.

BKI5013E **Value for** *name* **is too long. Current value:** *value*

Explanation:

The value of the environment variable *name* has too many digits.

User response:

Check if the variable is set correctly.

BKI5014E **Tivoli Storage Manager Error:** *error_message*

Explanation:

See BKI5000E.

User response:

See BKI5000E.

BKI5015W **Data description could not be restored, because it was backed up with a newer version (objInf=support information)**

Explanation:

The TSM server hosts backups (data description) which were made with a new version of backint or backom, which ignores this data in further processing.

User response:

Upgrade the product.

BKI5016I **Time:** *current_time* **New TSM session created: MGMNT-CLASS:** *management_class***, TSM-Server:** *server_name***, type:** *session_type***.**

Explanation:

A new session to TSM server *server_name* has been established at *current_time*. Data will be stored in management class *management_class*.

User response:

None.

BKI5017E **Internal Tivoli Storage Manager Error: Transaction succeeded although it was expected to fail.**

Explanation:

An internal Tivoli Storage Manager error occurred.

User response:

Retry the action. If the error occurs again contact IBM Support.

BKI5018E **The requested buffer has a size (***current_size* **bytes) that is smaller than requested** *requested_size***.**

Explanation:

The request for a new buffer was successful. The buffer, however, does not have the requested size.

User response:

Check if the system is running low on memory and retry the action. If the error occurs again contact IBM Support.

BKI5019E **Error during delete of object <filename>:<object>**

Explanation:

A named file could not be deleted from a TSM server.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI5020E **Error while deleting objects :<objects>**

Explanation:

One or more named objects could not be deleted from a TSM server.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI5021W No data was deleted on the TSM Server because the environment variable ″XINT_FUNCTION_DELETE″ is set to ″DISABLE″.

Explanation:

The delete function was disabled temporarily.

User response:

If the delete function has to be re-activated, unset the environment variable XINT_FUNCTION_DELETE and try again.

BKI5022W Error during version delete. Not all backups that have expired could be removed.

Explanation:

The database backup finished successfully. Nevertheless, the deletion of expired backup sets failed.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6201I Checking status of database.

Explanation:

The actual status of the database will be checked to ensure a valid state for the subesquent operation.

User response:

None.

BKI6202E The log mode for this database is NOARCHIVELOG.

Explanation:

The log mode for this database is NOARCHIVELOG.

User response:

Change the log mode for this database to ARCHIVELOG.

BKI6203E The Oracle database is currently in read-only mode.

Explanation:

The Oracle database is currently designated as read-only. Processing stops.

User response:

Remove the read-only mode of the Oracle database and try again.

BKI6204E The Backup type is online but the mount mode is either nomount or startup restricted.

Explanation:

The Backup type is online but the mount mode is either nomount or startup restricted.

User response:

Change the mount mode to startup mount.

BKI6205I Changing Oracle mode to: <mode>.

Explanation:

The operational mode of the Oracle database is changed to the named mode.

User response:

None.

BKI6206E No table space was found for the Oracle database.

Explanation:

No table space was found for the Oracle database.

User response:

Make sure the correct database system identifier (SID) is specified.

BKI6207E Oracle database data files were not found.

Explanation:

Oracle database data files were not found.

User response:

Make sure the correct database system identifier (SID) is specified.

BKI6208E Oracle database control files were not found.

Explanation:

Oracle database control files were not found.

User response:

Make sure the correct database system identifier (SID) is specified.

BKI6209E The database failed to shut down during the FlashCopy operation.

Explanation:

The database attempted to shutdown because the backup type parameter is set to offline. The database failed to shutdown.

User response:

Manually shutdown the database you are trying to back up, then run the operation again.

BKI6210E Failed to open the output file: <filename>

Explanation:

The named output file could not be opened.

User response:

Either the file doesn't exist or the permissions are not sufficient for the requested operation. Check that the directory exists where an attempt is being made to access the output file and that sufficient permissions are granted. Try again.

BKI6211E Failed to copy the database controlfile. Please check log file '<filename>'.

Explanation:

The Oracle database control file doesn't exist.

User response:

Make corrective actions regarding the information to be found in the named log file and try again.

BKI6212I Suspend database.

Explanation:

The Oracle database to be flashed is going to be supended.

User response:

None.

BKI6213E An error occurred while attempting an 'alter system suspend' action. More details: <errormsg>

Explanation:

An error occurred while attempting an 'alter system suspend' action. Details can be found in the named message.

User response:

Make sure the Oracle database to be backed up is running, then try to suspend the system with a command line invocation. If the system suspends successfully, run the operation again.

BKI6214I Resume database.

Explanation:

The Oracle database to be flashed is going to be resumed.

User response:

None.

BKI6215E An error occurred while attempting an 'alter system resume' action. More details: <errormsg>

Explanation:

An error occurred while attempting an 'alter system resume' action. Details can be found in the named message.

User response:

Make sure the Oracle database to be backed up is running, then try to resume the system with a command line invocation. If the system resumes successfully, run the operation again.

BKI6216E Failed to get Oracle version information.

Explanation:

Failed to get Oracle version information using sqlplus.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6217I Database switched to next logfile.

Explanation:

The database switched to the next logfile.

User response:

None.

BKI6218E Backup ID to delete not specified.

Explanation:

To delete a backup a valid backup id has to be specified.

User response:

Specifiy a valid backup id and try again.

BKI6219I Backup to TSM: <filename>

Explanation:

Backing up the named file to TSM.

User response:

None.

BKI6220I Using Oracle profile section : <section>

Explanation:

The named Oracle profile section is used for the started operation.

User response:

None.

BKI6221I Database profile: <filename>

Explanation:

Using the named database profile.

User response:

None.

BKI6222E Database profile '<filename>' not found.

Explanation:

The named database profile was not found.

User response:

Check if the named profile exists and try again.

BKI6223I Detected control file: <filename>

Explanation:

The named Oracle control file was found.

User response:

None.

BKI6224I Create control file copy: <filename>

Explanation:

A named Oracle control file copy will be created.

User response:

None.

BKI6225I Create database parameter file '<filename>' from SPfile.

Explanation:

A named Oracle database parameter file will be created.

User response:

None.

BKI6226E Default directory for database parameter file '<filename>' not found.

Explanation:

The name Oracle parameter file could not be found within the default directory.

User response:

Ensure a valid Oracle parameter file exists in the default directory and try again.

BKI6227I Parameter 'database_control_file_restore' is set to yes in the profile. You will need to do the incomplete recovery after the restore.

Explanation:

The Oracle database control file is requested for restore.

User response:

None.

BKI6228E The database seems to be running. Restore not possible.

Explanation:

A running Oracle database was detected and therefore a restore is not possible.

User response:

Check if the started restore operation is valid. If yes, stop the running database and try again.

BKI6229I Restoring control file <controlfile>

Explanation:

The named control file will be restored.

User response:

None.

BKI6230I Set table space files in backup mode.

Explanation:

The table space files of the participating table spaces will be set in backup mode.

User response:

None.

BKI6231I End backup mode for table space files.

Explanation:

The backup mode for table space files of the participating table spaces will be reset.

User response:

None.

BKI6232I Looking for the latest backup.

Explanation:

An attempt is being made to pick the most current valid backup image for the requested operation.

User response:

None.

BKI6233I Restoring backup with ID <id>.

Explanation:

The backup with the named id will be restored.

User response:

None.

BKI6234E No backup found which could be restored.

Explanation:

There was no snapshot backup found which can be restored.

User response:

Verify your environment. If one or multiple valid snapshot backup exist and the restore still fails, contact your IBM support personnel.

BKI6235I Deleting backup with ID <id>.

Explanation:

The named snapshot backup is going to be deleted.

User response:

None.

BKI6236E Failed to delete backup with ID <id>. Reason: <reason>

Explanation:

The snapshot backup with the named id could not be deleted.

User response:

Check the logs and the named output for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6237E Backup failed. Please check RMAN log.

Explanation:

The offloaded backup to TSM using RMAN failed.

User response:

Make corrective actions regarding the information to be found in the named log file and try again.

BKI6238E Failed to switch logfiles. This is the output of the failed command:<output>

Explanation:

The command failed.

User response:

Check the logs and the named output for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6239E Failed to detect read mode. This is the output of the failed command:<output>

Explanation:

The command failed.

User response:

Check the logs and the named output for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6240E Failed to create a pfile from spfile. This is the output of the failed command:<output>

Explanation:

The command failed.

User response:

Check the logs and the named output for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6241E The tablespace file '<filename>' is a link and not a real file.

Explanation:

The named tablespace file has to be a real file. Instead, a link was detected.

User response:

Verify your environment. If the problem cannot be resolved contact your IBM support personnel.

BKI6242E Raw devices are not supported. ('<devicename>')

Explanation:

Raw devices are currently not supported.

User response:

For further details on this issue, contact your IBM support personnel.

BKI6243E Failed to excute sql cmd '<command>'. This is the output of the failed command:<output>

Explanation:

The named sql command failed.

User response:

Check the logs and the named output for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6250E Error during initialization: <description>

Explanation:

An error resulting in the named description was detected during the initialization phase of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6251E Error during start of backup: <description>

Explanation:

An error resulting in the named description was detected during the start of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6252E Error during partitioning: <description>

Explanation:

An error resulting in the named description was detected during the partitioning phase of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6253E Error during preparation of snapshot: <description>

Explanation:

An error resulting in the named description was detected during the preparation phase of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6254E Error during creation of snapshot: <description>

Explanation:

An error resulting in the named description was detected during the creation of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6255E Error during verification of snapshot: <description>

Explanation:

An error resulting in the named description was detected during the verification phase of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6256E Error during write of meta-information: <description>

Explanation:

An error resulting in the named description was detected during write of meta-information assigned to a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6257E Error during retrieval of meta data: <description>

Explanation:

An error resulting in the named description was detected during retrieval of meta data assigned to a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6258E Error during query-initialization: <description>

Explanation:

An error resulting in the named description was detected during the snapshot query-initialization phase.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6259E Error during retrieval of query information: <description>

Explanation:

An error resulting in the named description was detected during retrieval of query information of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6260E Error during end of query: <description>

Explanation:

An error resulting in the named description was detected during the end of query for snapshot phase.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6261E Error during start of restore: <description>

Explanation:

An error resulting in the named description was detected during the start of the snapshot restore phase.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6262E Error during restore: <description>

Explanation:

An error resulting in the named description was detected during the restore of a snapshot backup.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6263E Error during end of restore: <description>

Explanation:

An error resulting in the named description was detected during finishing of a snapshot restore operation.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6264E Error during start of delete: <description>

Explanation:

An error resulting in the named description was detected during the start of the snapshot delete phase.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6265E Error during end of delete: <description>

Explanation:

An error resulting in the named description was detected during finishing of a snapshot delete operation.

User response:

Check the logs for further information. After resolving the issue try again.

BKI6266E Restoring Oracle control files failed. Oracle control files are on raw volumes in the production server and those are supposed to be created manually on the backup server. It failed because of either control files are not created on the backup server or created incorrectly. Please check log file *filename***.n**

Explanation:

On the production server the Oracle control files reside on raw volumes. On the backup server they need to be restored in order to perform the backup to TSM. This process did fail.

User response:

Examine the content of the *filename*. It contains the output from the Oracle RMAN. A possible reason could be that the raw devices for the control files have not been created on the backup server.

BKI6267E Restoring Oracle control files failed. Please check log file *filename***.**

Explanation:

On the backup server the Oracle control files need to be restored in order to perform the backup to TSM. This process did fail.

User response:

Examine the content of the *filename*. It contains the output from the Oracle RMAN.

BKI6501I Initializing '<function>' request.

Explanation:

The offload agent will be initialized for a new function request.

User response:

None.

BKI6502I Executing '<function>' request.

Explanation:

The offload agent is executing a function request.

User response:

None.

BKI6503I Terminating '<function>' request.

Explanation:

The offload agent is terminating a function request. This also includes a cleanup of required resources.

User response:

None.

BKI6504E The '<function>' request failed.

Explanation:

A tsm4acs function, such as mount or unmount, failed unexpectedly.

User response:

Check the tsm4acs log as well as the appropriate device agent log and management agent log for further details.

BKI6505E Forced '<function>' requires the instance, database and snapshot timestamp filter arguments.

Explanation:

If a function is started with the option '-F' (forced) the filter arguments for the instance, database and snapshot timestamp also have to be specified to ensure the workflow will be applied only to one specific snapshot backup.

User response:

Specify the instance (-i), database (-d) and snapshot timestamp (-T) filter arguments as well.

BKI6506I Backup <backup id> was created with option TSM_ONLY. It is marked for deletion after the first TSM backup attempt.

Explanation:

The backup corresponding to <backup id> has been deleted. This is because the backup was made with TSM_BACKUP option TSM_ONLY and the TSM backup associated with this snapshot image has recently completed (successfully or unsuccessfully).

User response:

None.

BKI6507E Function '<function>' is not supported.

Explanation:

The function request is not supported by the offload agent.

User response:

Check the specified function.

BKI6508I Initializing partition(s) '<partition(s)>' of database '<database name>' as <type>.

Explanation:

The participating database partitions will be initialized on the target system. Valid initialization types are snapshot, standby and mirror.

User response:

None.

BKI6509E Failed to initialize partition(s) '<partition(s)>' of database '<database name>'.

Explanation:

The offload agent was not able to initialize one or more database partitions.

User response:

Check the offload agent log as well as the DB2 diagnostic log (db2diag.log) for further details.

BKI6510I Partition(s) '<partition(s)>' of database '<database name>' initialized successfully.

Explanation:

The participating database partitions were initialized successfully.

User response:

None.

BKI6511E The snapshot backup timestamp filter is not allowed in combination with tape backups.

Explanation:

The data to be off-loaded are typically under control of a versioning mechanism of either the backup mover or Tivoli Storage Manager. If multiple snapshots are in the queue to be off-loaded and the snapshot timestamp filter argument (-T) is incorrect, there is a potential risk of bypassing the established version control mechanism and losing tape backup images.

User response:

Do not specify the snapshot backup timestamp filter (-T) in combination with the function 'tape_backup'.

BKI6512I The '<function>' request for database '<database name>' with partitions (<partition(s)>) processed successfully.

Explanation:

The selected function for the participating partitions of a database was processed successfully.

User response:

None.

BKI6513I The resources of database '<database name>' with partitions (<partition(s)>) are already mounted.

Explanation:

All required file systems are already mounted on the target system.

User response:

None.

BKI6514E The specified filter did not result in a match in the snapshot repository.

Explanation:

The repository does not contain a snapshot backup that can be associated with the given filter arguments.

User response:

Check all specified filter arguments and try again.

BKI6515E A snapshot backup currently offloaded to tape is no longer mounted.

Explanation:

: A tsm4acs tape_backup workflow consists of the steps: mount, tape backup, unmount. When entering the unmount-phase, tsm4acs could not find the snapshot backup that was just backed up to tape. In principle, the tape backup might have finished successfully but some kind of a failure was detected that prevents the tape_backup cleanup phase from completing.

User response:

Check the tsm4acs log as well as the appropriate device agent log for further details.

BKI6516E Another '<function>' request for a snapshot backup is already running.

Explanation:

tsm4acs has detected that another request, such as mount or tape_backup, for a snapshot backup is running.

User response:

A new tsm4acs request can only be started if the old request has finished.

BKI6517I A snapshot backup exists which is already mounted.

Explanation:

The tsm4acs mount-request will not be executed due to an already mounted snapshot backup on the offload system.

User response:

None.

BKI6518I No snapshot backup exists which is currently mounted.

Explanation:

The tsm4acs unmount-request will not be executed because there is currently no snapshot backup mounted on the offload system.

User response:

None.

BKI6519I No snapshot backup is currently pending to be offloaded to tape.

Explanation:

The tsm4acs tape_backup request will not be executed because there is no snapshot backup in the TAPE_BACKUP_PENDING state.

User response:

None.

BKI6520I Starting database instance '<instance name>'.

Explanation:

The database instance on the target system will be started.

User response:

None.

BKI6521I Database instance '<instance name>' was started successfully.

Explanation:

The database instance on the target system was started.

User response:

None.

BKI6522W Database instance '<instance name>' already started.

Explanation:

The database instance on the target system is already running.

User response:

The offload agent workflow should not be affected. In general, no action is required.

BKI6523E Database instance '<instance name>' could not be started.

Explanation:

The database instance on the target system could not be started.

User response:

Check the DB2 diagnostic log (db2diag.log) for further details.

BKI6524I Stopping database instance '<instance name>'.

Explanation:

The database instance on the target system will be stopped.

User response:

None.

BKI6525I Database instance '<instance name>' was stopped successfully.

Explanation:

The database instance on the target system was stopped.

User response:

None.

BKI6526W Database instance '<instance name>' already stopped.

Explanation:

The database instance on the target system was already stopped.

User response:

Check the DB2 diagnostic log (db2diag.log) for indication of whether an unexpected failure was the cause. Also check the tsm4acs log for indications that the workflow, which includes shutdown of the database instance on the target system, reported unexpected failures.

BKI6527E Database instance '<instance name>' could not be stopped.

Explanation:

The database instance on the target system could not be stopped.

User response:

Check the DB2 diagnostic log (db2diag.log) for further details.

BKI6528E The file containing the list of partitions and hosts to be off-loaded could not be created.

Explanation:

The 'rah' host file is used by DB2 to determine the database partitions that must be processed in a DPF environment. By default, this file is 'db2nodes.cfg'. tsm4acs uses a temporary 'rah' host file to be able to handle only a subset of partitions.

User response:

The temporary 'rah' host file used by tsm4acs will be created under '$HOME/sqllib', where $HOME is the home directory of the DB2 instance owner. Ensure that the appropriate permissions are set and enough free space is available.

BKI6530E The default database path could not be determined.

Explanation:

The value of the default database path (DFTDBPATH) stored in the database manager configuration could not be retrieved.

User response:

Check the DB2 diagnostic log (db2diag.log) for details. Further, verify the database manager configuration to be issued by the DB2 instance owner as follows: `db2 get dbm cfg | grep DFTDBPATH`. Also for a more detailed analysis, enable the trace facility for the offload

agent and re-execute the function.

BKI6531I Cataloging database '<database name>' on path '<path>'.

Explanation:

The database on the target system will be cataloged.

User response:

None.

BKI6532I Database '<database name>' on path '<path>' cataloged successfully.

Explanation:

The database on the target system was cataloged successfully.

User response:

None.

BKI6533E Failed to catalog database '<database name>' on path '<path>'.

Explanation:

The database on the target system could not be cataloged.

User response:

Check the DB2 diagnostic log (db2diag.log) for further details. Additionally, for a more detailed analysis enable the trace facility of the offload agent and re-execute the function.

BKI6537I Database '<database name>' on path '<path>' already cataloged.

Explanation:

The database on the target system was already cataloged.

User response:

None.

BKI6539W The retry threshold for the snapshot backup was exceeded.

Explanation:

If tsm4acs is running in the daemon mode (-D), only one attempt will be made to offload a tape from a snapshot backup. This restriction was imposed to prevent an excessive number of offload retries for a snapshot backup.

User response:

A snapshot backup for which the retry threshold was exceeded can only be offloaded to tape using the manual mode of tsm4acs (-f tape_backup).

BKI6540I <Start time>: Starting backup of database '<database name>', partition(s) '<partition(s)>' with the following options: METHOD <offload backup method> SESSIONS <number of sessions> OPTIONS <options> BUFFERS <number of buffers> BUFFERSIZE <buffer size> PARALLELISM <degree of DB2 parallelism>

Explanation:

The off-loaded tape backup was started using the 'db2 backup database' command. The set of listed backup parameters gives a brief summary about the options and values that were used for the backup.

User response:

None.

BKI6541I End_time Instance Database Partition Snapshot_ID Tape_backup_ID

Explanation:

The backup is finished. A backup result table for all participating partitions of the database will be generated.

User response:

None.

BKI6542I <end time><instance name><database name><partition><snapshot id><tape backup id>

Explanation:

One entry of the backup result table reflects one partition of the database. The backup for a database partition succeeded if a valid tape backup ID (DB2 tape backup timestamp) was inserted. If the tape backup for a partition failed, the tape backup ID is set to '-'.

User response:

None.

BKI6544I Snapshot backup suspend time: <suspend time>

Explanation:

The snapshot backup suspend time specifies the minimum recovery time for all participating partitions.

User response:

None.

BKI6545I Write control file <ctrlfile>

Explanation:

The offload agent is writing the Oracle control file to a local file system.

User response:

None.

BKI6546I Write database parameter file <paramfile>

Explanation:

The offload agent is writing the database parameter file to a local file system.

User response:

None.

BKI6547I Do not overwrite database parameter file.

Explanation:

The offload agent will not overwrite the database parameter file.

User response:

None.

BKI6548I Start backup of database instance '<instance>'.

Explanation:

The offloaded tape backup of the named database instance was started.

User response:

None.

BKI6549I Finished backup of database instance '<instance>' successfully.

Explanation:

The offloaded tape backup of the named database instance finshed successfully.

User response:

None.

BKI6555I Selected snapshot backup with ID '<id>'.

Explanation:

The snapshot backup with the named id was selected to work with. The format of a snapshot id in that context is: <instance>,<database>,<timestamp>.

User response:

None.

BKI6556E Failed to retrieve metadata.

Explanation:

The metadata assigned to a snapshot backup could not be retrieved.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6557I The '<function>' request for database '<dbname>' processed successfully.

Explanation:

The offload agent has completed the named function successfully.

User response:

None.

BKI6558I The resources of database '<dbname>' are already mounted.

Explanation:

The offload agent has detected that all required resources of the named database are already mounted.

User response:

None.

BKI6560E Backint could not be found at '<directory>'.

Explanation:

The offload agent was unable to find the backint executable file needed for offloading the data to TSM.

User response:

The offload agent expects the backint executable at the default TSM for ERP installation location. Ensure that backint can be found accordingly and try again.

BKI6600E Unexpected error during '<function>'.

Explanation:

The offload agent has terminated unexpectedly due to an internal error while executing either a mount or an unmount request.

User response:

Check the logs of the involved components (management agent, offload agent, device agent) for further details and descriptions regarding the failure.

BKI6901I Response to Init request.

Explanation:

The device agent is responding to an initialization request.

User response:

None.

BKI6902I Response to Partition request.

Explanation:

The device agent is responding to a partitioning request.

User response:

None.

BKI6903I Response to Prepare Flash request.

Explanation:

The device agent is responding to a prepare snapshot request.

User response:

None.

BKI6904I Response to Restore request.

Explanation:

The device agent is responding to a snapshot restore request.

User response:

None.

BKI6905I Response to Flash request.

Explanation:

The device agent is responding to a snapshot backup request.

User response:

None.

BKI6906I Response to Verify request.

Explanation:

The device agent is responding to a verify request.

User response:

None.

BKI6907I Response to Complete Restore request.

Explanation:

The device agent is responding to a complete restore request.

User response:

None.

BKI6908I Response to Expiration request.

Explanation:

The device agent is responding to a snapshot backup expiration request.

User response:

None.

BKI6909I Response to Monitor request.

Explanation:

The device agent is responding to a background monitor request.

User response:

None.

BKI6910E Could not set user ID to <userid>. Error <error> - <errormsg>.

Explanation:

The user id of the device agent process could not be switched internally to the named user id.

User response:

Check the permissions of the binary and try again.

BKI6911E The effective user ID <userideff> of the process could not be set to the user <userid>. Error <error> - <error_msg>. Check that the device agent executable has the s-bit set.

Explanation:

Due to insufficient permissions of the device agent executable, the user id of the device agent process could not be switched internally to the named user id.

User response:

Check that the device agent binary has the s-bit set and try again.

BKI6912E Background operation shutting down in order to give precedence to a concurrent operation.

Explanation:

The background monitoring operation was canceled due to an operation of a higher precedence.

User response:

Check if the directory exists and further, if the permissions of the directory are set appropriately. Try again.

BKI6913E Wrong parameter provided with option '-c'.

Explanation:

The device agent specific command option '-c' consists of the two sub-components server and port, whereby the port is optional. If a server and port is specified, these values have to be seperated by a ':'.

User response:

Use the command option '-c' with the argument <server>[:<port>] and try again.

BKI6914E Invalid option '-K' specified.

Explanation:

The device agent specific command option '-K' is not allowed for explicit calls of a device agent executable. That parameter is reserved only for internal workflows, whereby a device agent is called by another binary.

User response:

Remove the command option '-K' from the caller string and try again.

BKI6915E Could not change directory to <directory>.

Explanation:

The application was unable to change to the named directory.

User response:

Check if the directory exists and further, if the permissions of the directory are set appropriately. Try again.

BKI6917E Failed to find volume group for file: <filename>

Explanation:

The volume group for the named file could not be found.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6918E Error when reading the correlation list or during the FlashCopy of the volume pairs.

Explanation:

An internal error occurred during the FlashCopy of volume pairs.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6919E Failed to cancel the copy relationship of volume pairs: rc=<rc>.

Explanation:

The device agent was unable to cancel the copy relationship of volume pairs. The withdraw operation failed.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6920E After 'withdraw done' was finished the update of the IDS repository failed: rc=<rc>.

Explanation:

The device agent was unable to update the IDS repository.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6921E Failed to monitor the FlashCopy.

Explanation:

An internal error occurred during monitoring of the background copy.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6922E Failed to allocate memory.

Explanation:

An internal error occurred during memory allocation.

User response:

Check the logs for further information. If the problem

cannot be resolved contact your IBM support personnel.

BKI6923I <copytype> control object already initialized.

Explanation:

The named copy type control object is already initialized and will be used for further processing by the device agent.

User response:

None.

BKI6924E Failed to initialize <copytype> control object.

Explanation:

An internal device agent error occurred during the initialization of the named copy type control object.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6925E Function call '<function>' failed.

Explanation:

An error was detected during execution of the named function.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6926I Adding '<filename>' to the Disk Mapper input list.

Explanation:

The device agent added the named file to the disk mapper input list.

User response:

None.

BKI6927E Failed to find N Series volume for file '<filename>'. Error: <error>.

Explanation:

The device agent was uanble to find the volume hosting the named file.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6928E File system not found. Failed to find NFS mount point for file: '<filename>'.

Explanation:

The device agent was unable to determine the file system hosting the named file.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6929E Not a file system of type NFS. Failed to find N Series volume for file: '<filename>'.

Explanation:

The file system where the named file is located is not of type NFS.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6930E Volume information missing. Failed to find N Series volume for file: '<filename>'.

Explanation:

The device agent was unable to detect the volume information for a given file.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6931E Function call '<function>' failed. Error: <error>.

Explanation:

An error was detected during execution of the named function.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6932E Function call '<function>' failed with rc=<rc>. Error: <error>.

Explanation:

An error was detected during execution of the named function.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6933I Volume '<volume>', snap ID = <id>.

Explanation:

The device agent is using the named volume as a snap volume.

User response:

None.

BKI6935I Unmounting '<mountpoint>'.

Explanation:

The device agent is unmounting the named mount point.

User response:

None.

BKI6936E Failed to unmount '<mountpoint>'.

Explanation:

The unmount of the named mount point failed.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6937I Mounting '<mountpoint>'.

Explanation:

The device agent is mounting the named mount point.

User response:

None.

BKI6938E Failed to mount '<mountpoint>'.

Explanation:

The mount of the named mount point failed.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI6939I Prepare for snap restore, volume '<volume>', snap ID = <id>.

Explanation:

The device agent is preparing the named volume for snap restoring.

User response:

None.

BKI6940I Prepare flash of group '<group>'.

Explanation:

The device agent is preparing the named group for flashing.

User response:

None.

BKI6941I <copy services server><copy services user><*><copy services type><copy services time out>**

Explanation:

Prints information about the configured storage device which will be used by the device agent workflow.

User response:

None.

BKI6942E The storage device '<device>' is not handled by this device agent.

Explanation:

The device agent cannot be used in combination with the named storage device.

User response:

Check the setup of your system landscape (hardware, software). If the problem cannot be resolved contact your IBM support personnel.

BKI6943I Hardware version installed: <major>.<minor>

Explanation:

The device agent has checked the version of the storage hardware to be used.

User response:

None.

BKI6944I NLS and tracing are already initialized.

Explanation:

The initialization of the NLS and of the trace facility were already done.

User response:

None.

BKI6945I **File system '<filesystem>' was already unmounted.**

Explanation:

The named file system is already unmounted and will be omitted from the unmount process.

User response:

None.

BKI6946E **The environment variable 'ODMDIR' is not specified. Please verify that the DB2 registry parameter DB2ENVLIST contains the value 'ODMDIR'. To set the DB2ENVLIST you need to issue the command: db2set -i <DB2 instance name> DB2ENVLIST='<current envlist> ODMDIR'**

Explanation:

On AIX, the device agent needs the ODM for internal purposes and has to be able for accessing the ODM components located under 'ODMDIR'.

User response:

Check the runtime environment for the environment variable 'ODMDIR'. If not specified, set it to the correct value. On AIX, for example, this would be typically '/etc/objrepos'. Further, the environment variable has to be registered within the DB2 profile registry variable DB2ENVLIST. Finally, the DB2 instance has to be restarted to activate the environmen adjustments.

BKI6947W **File system '<filesystem>' is already mounted.**

Explanation:

The named file system is already mounted. This means that the target set where the named file system is located will be skipped by the device agent.

User response:

Ensure there is a valid reason why that file system is already mounted. If so, no further action is required. Otherwise, it is recommended to check why this file system was already mounted.

BKI6948E **The container <*container_id*> has already been created. Please specify another name.**

Explanation:

The container with id <*container_id*> has already been created previously. Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6949E **Creation of the container <*container_id*> failed because no preceding group has been found or the preceding group is not valid. Current group is: <*group_id*>. Please specify a valid group at first using the <*command*> command.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6950W **The output file '<filename>' is not valid.**

Explanation:

The named output file could not be created or the permissions are insufficient.

User response:

Check for the right permissions and try again. If the problem cannot be resolved contact your IBM support personnel.

BKI6951E **Version mismatch error. Please check setup (<version>:<version>).**

Explanation:

The version of the device agent on one side and the version of the management agent on the other side don't match. Only binaries of identical version signatures are compatible.

User response:

Ensure the version signature of all participating binaries are identical. This can be checked either based on the logs or by issuing the commands with the command option '-v'.

BKI6952E **Error in connection to TSM ACS management agent.**

Explanation:

The device agent was unable to connect to the TSM ACS management agent.

User response:

Ensure the ACSD keyword of the global profile section has a valid hostname/port value combination assigned. Try again.

BKI6955E **<*container_id*> is not a valid container. Please specify a valid container.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6956E **The usability state <*usablility_state*> is not supported.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter. The given usability state <*usablility_state*> is not valid.

User response:

Contact your IBM support personnel.

BKI6962I **Response to File System Service request (<function>).**

Explanation:

The device agent is responding to a file system service request to service the named function.

User response:

None.

BKI6967E **The directory <directory> has nested mount points that are stored on more than one volume group. This is currently not supported.**

Explanation:

The application sent a request to recursively backup all data stored beneath <directory>. TSM for ACS cannot fulfill this backup request because the data stored in this directory path resides on file systems that are stored on multiple volume groups. This is currently not supported.

User response:

Migrate the data underneath <directory> to a single file system or migrate the file systems mounted underneath this directory tree to a common volume group. Note that the directory structure could also contain links to files residing in other file systems. In this case you might be able to resolve this problem by simply removing those links.

BKI6968E **<*command_1*> is not a valid keyword, expected <*command_1*>.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6969E **Found non-database files on the file systems to restore. Please provide a negative list or perform restore with option 'no_check' to allow overwriting those files.**

Explanation:

Although the previously mentioned files were not requested to be restored, they would be overwritten, because they reside on a file system that will be entirely overwritten during restore. In order to allow overwriting those files during restore they need to be added to a 'negative list' or the checking to prevent files from being overwritten needs to be disabled.

User response:

Edit the 'CLIENT' section of the profile. You can either set the parameter 'NEGATIVE_LIST' to 'NO_CHECK', to allow TSM for ACS to overwrite any file residing on a file system that will be restored, or you can set the parameter 'NEGATIVE_LIST' to point to a file (the 'negative list') which contains a list of all files and directories that are allowed to be overwritten. Any directory you add to the 'negative list' is processed recursively.

BKI6970I **Snapshot restore successful.**

Explanation:

The snapshot restore of a snapshot backup finished successfully.

User response:

None.

BKI6971E **Adding the key <*key*> to the container <*container*> failed because it already exists. Please use the <*command*> command if you want to update the key.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6972E **Updating the key <*key*> in the container <*container*> failed because it does not exist. Please use the <*command*> command if you want to add the key.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6973E **The group <*group*> has already been created. Please specify another name.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6974E **<*group*> is not a valid group. Please specify a valid group.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6975E **Adding the key <*key*> to the group <*group*> failed because it already exists. Please use the <*command*> command if you want to update the key.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6976E **Updating the key <*key*> to the group <*group*> failed because it does not exist. Please use the <*command*> command if you want to add the key.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6977E **The #<*first_command*> <*parameter*> command has to be preceded by a #<*second_command*> command.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6978E **<*command*> is not a valid keyword when updates to containers and groups are expected.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6279E **Script has continued without waiting. Expected output <*command*> from script but was: <*output*>.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6980W **Received #WARNING command with parameters: <*warning*>.**

Explanation:

A warning message has been received from the storage device with the parameters: <*warning*>.

User response:

Check the content of the warning.

BKI6981E **Received #ERROR command with parameters: <*error*>.**

Explanation:

An error message has been received from the storage device with the parameters: <*error*>.

User response:

Check the content of the error message.

BKI6982W **The script <*adapter_name*> returned with code 1. The logfile might contain further warnings.**

Explanation:

The storage device adapter had a return code of 1.

User response:

Please check the device agent logfile for further warnings.

BKI6983E **The following files have not been partitioned: <*file_names*>**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI6984E **Error during prepare phase. Nothing known about group <*group_name*>. It has not been created in the partition phase.**

Explanation:

Error in communication protocol between the device agent and the storage device adapter.

User response:

Contact your IBM support personnel.

BKI7048I **The default port to connect to** *server_name* **will be used.**

Explanation:

A server port for the connection to the named server was not explicitly specified. Therefore, the default port is used.

User response:

Make sure the named server is listening to the default port. In the case of connection failures, specify the server port in the profile.

BKI7049I **The default ProLE port will be used.**

Explanation:

The port for the internal communication of Data Protection for SAP is set during installation. The message indicates that this port is being used.

User response:

None.

BKI7051E **The environment variable XINT_PROFILE is not set. It must be set and contain the fully qualified path to the *.utl file to be used.**

Explanation:

The way Data Protection for SAP works is specified in a profile. When called, Data Protection for SAP looks for the environment variable XINT_PROFILE which must contain the fully qualified path to the profile.

User response:

Check the environment for XINT_PROFILE of the user who started Data Protection for SAP.

BKI7053E **Service setup failed due to previous error.**

Explanation:

Initialization of the product failed due to previous errors.

User response:

Check the product log file for further detailed messages.

BKI7055E **Service open failed due to previous error in data mover.**

Explanation:

The command could not be started due to previous errors.

User response:

Check the product log file for further detailed messages.

BKI7056E **Service open failed because configured TSM server could not be accessed.**

Explanation:

The command could not be started because the TSM server defined in the profile could not be accessed.

User response:

Check the product log file for further detailed messages.

BKI7057E **Service open failed because all configured sessions are currently in use.**

Explanation:

The command could not be started because all configured sessions in the profile are currently in use.

User response:

With Oracle RMAN the number of channels configured either in SAP profile or the RMAN script must be less

or equal to the maximum number of allowed sessions (MAX_SESSIONS). If multiple servers are used see the User's Guide for further details. Also check the Data Protection for SAP log file for further detailed messages.

BKI7058E **Service open failed because more than one file was found with the same name.**

Explanation:

The command could not be started because two or more files with the same name were found.

User response:

Check the product log file for further detailed messages.

BKI7059E **Service open failed because a file was not found.**

Explanation:

The command could not be started because a file specified was not found.

User response:

Check the product log file for further detailed messages.

BKI7060I *product* **<version>.<release>.<modification> (<build number>) <build date> session: process ID**

Explanation:

This message is to verify the version of the shared library used for backup. On UNIX and Linux systems this message will be written multiple times into the log per backup depending on the RMAN setup. On Windows, it is written just once.

User response:

None, if the right version is used. If the version within the log does not match the installed version, see 'RMAN Problem Resolution' in the *Data Protection for SAP® Installation and User's Guide*.

BKI7061I **Continuing to restore from next data copy.**

Explanation:

A saved data copy could not be restored from the primary data source. Due to multiple data copies available, the unit will switch to the next available data copy and continue to restore.

User response:

Although the data could be restored it should be investigated, why one of the data sources were not available.

BKI7301W **Data exchange file from Data Protection for Snapshot Devices for SAP®, <*filename*>, does not exist.**

Explanation:

The referenced file is expected by Data Protection for SAP® to exist and to contain information from Data Protection for Snapshot Devices for SAP® about the actual snapshot operation.

User response:

The absences of this files indicates a problem during the snapshot operation performed by Data Protection for Snapshot Devices for SAP®. Please check the logs of DP for Snapshot Devices for SAP® to determine the cause of the problem and try again.

BKI7303W **Profiles for Data Protection for Snapshot Devices for SAP® are different. backup:** *file name* **restore:** *file name*

Explanation:

During backup the profile used by DP for Snapshot Devices can be determined automatically. For restore and inquire operations the profile for DP for Snapshot Devices must be specified in the profile using the parameter FCS_FILE. For restore DP for Snapshot Devices must use the same profile as for backup.

User response:

Correct the entry for the FCS_FILE parameter in the profile (init<SID>.utl).

BKI7304I **Performing DISK ONLY backup**

Explanation:

The data for this backup is stored on snapshot-type disks only and will not be sent to TSM.

User response:

None

BKI7305E **Error during call to Data Protection for Snapshot Devices for SAP®** *error message*

Explanation:

DP for Snapshot Devices could not process the requested operation successfully. Processing may not stop at this point. Depending on the type of request (backup to both TSM and snapshot disks or to snapshot disks only, restore of data which is available in both modes) there are possibilities to recover from this error and continue operation.

User response:

Use the information from *error message* and the output of DP for Snapshot Devices to determine the cause of the problem and try again.

BKI7307W Data Protection for Snapshot Devices for SAP® reported an error during a snapshot-type operation. Do you want to continue to backup to TSM?

Explanation:

The backup was requested to be stored on both the TSM server and the snapshot-type disks. The snapshot operation has failed. Backup can continue to save data on the TSM server only.

User response:

Enter 'stop' if you want to solve the cause of this error and to try again. Enter 'cont' if you want to save this data on the TSM server only.

BKI7308E DISK ONLY backup has failed.

Explanation:

The current backup tried to store data on snapshot-type disks only and did not finish successfully.

User response:

Check the output from DP for Snapshot Devices prior to this error message to detect the root cause of this error and try again.

BKI7309W Data Protection for Snapshot Devices for SAP® reported an error during a snapshot-type operation. Do you want to continue to restore from TSM?

Explanation:

The data you wanted to be restored is located on the TSM server and on snapshot-type disks. The snapshot operation has failed. The process can continue to restore data from the TSM server.

User response:

Enter 'stop' if you want to resolve the cause of this error and to try again. Enter 'cont' if you want to restore from the TSM server.

BKI7310W Data Protection for Snapshot Devices for SAP® reported an error during a snapshot-type operation. CAUTION: Not all file systems are available. Do you want to retry the operation?

Explanation:

In contrast to message BKI7309W not all file systems are mounted. In this case it is not possible to continue the restore from the TSM server.

User response:

Enter 'stop' if you want to terminate this restore process. Enter 'cont' if you want to retry the snapshot process.

BKI7311I Profile used by DP for Snapshot Devices for SAP®:

Explanation:

The message shows the name of the profile used by DP for Snapshot Devices.

User response:

None

BKI7312W Profile for DP for Snapshot Devices for SAP® not specified in profile. For restore this must be specified

Explanation:

For restore and inquire operation in conjunction with DP for Snapshot Devices this parameter is mandatory. Without this parameter a restore using DP for Snapshot Devices is not possible and Data Protection for SAP will continue to inquire/restore from the TSM server only.

User response:

Add the parameter FCS_FILE to the Data Protection for SAP profile

---

BKI7313W Inquire results from DP for Snapshot Devices for SAP® are not available

Explanation:

Data Protection for SAP® was unable to retrieve information from DP for Snapshot Devices about available backups on snapshot-type disks. This message may be issued in consequence of message BKI7305E.

User response:

Check the output from DP for Snapshot Devices to determine the cause of the error and try again.

BKI7314E The data you want to restore is not available on the TSM server.

Explanation:

If a restore from snapshot-type disks can not be finished successfully Data Protection for SAP tries to continue to restore data from the Tivoli Storage Manager server. But if the backup was performed on snapshot disks only, the data can not be found on the TSM server.

User response:

Check the output from DP for Snapshot Devices prior to this error message to detect the root cause of this error and try again.

BKI7315W **The copy process of the files you want to restore is not yet finished. If you continue the files will be restored from TSM.**

Explanation:

The snapshot process running in the background has not finished moving the files from the source to the target volumes. A snapshot restore of these volumes is currently not possible.

User response:

After that message you will be asked if you want to continue or stop this operation. If you want to wait until the snapshot process has finished choose 'stop' and the restore attempt will terminate. If you choose 'continue' an attempt is made to restore the data from TSM if available.

BKI7316I **The following backup types for the BACKUPID** *Backup ID* **have been found: - TSM - Snapshot**

Explanation:

The backup for the backup ID *Backup ID* was stored on the Tivoli Storage Manager as well as on snapshot-type disks. For restore both data sources can be used.

User response:

None.

BKI7318E **The DP for Snapshot Devices for SAP® profile** *file name* **is not valid.**

Explanation:

The profile for DP for Snapshot Devices specified in `init<SID>.utl` could not be accessed.

User response:

Check the file name and the permissions for this file and try again.

BKI7319I **Start TSM restore**

Explanation:

The restore uses data from Tivoli Storage Manager.

User response:

None

BKI7320I **Start restore from snapshot.**

Explanation:

The restore is using data from snapshot-type disks.

User response:

None

BKI7321E **The DP for Snapshot Devices for SAP® profile** *file name* **found in parameter FCS_FILE of the DP SAP profile can not be used if you need to restore this backup.**

Explanation:

In the Data Protection for SAP profile the FCS_FILE parameter is set, however the DP for Snapshot Devices profile specified either

- is not a DP for Snapshot Devices profile
- does not point to the same DP for Snapshot Devices configuration file which was used by the preceding DP for Snapshot Devices `splitint` operation.

User response:

You need

- to correct the FCS_FILE parameter thus a valid DP for Snapshot Devices profile is used, for example the file DP for Snapshot Devices had used when running its snapshot function in the preceding brbackup task (see preceding message BKI7303W)
- to ensure that if different DP for Snapshot Devices SAP profiles are used, all use the same control file (the value of the IDS_CONTROL_FILE parameter in the DP for Snapshot Devices profile)

BKI7322E **Request for a partial restore or restore from snapshot with 'brrestore -m all' is not supported. In case of brrestore attempt rerun with -m full.**

Explanation:

DP for Snapshot Devices can only restore the whole content of a backup and not only a subset of a disk backup as requested. Most likely this is caused by running brrestore with the option '-m all'.

User response:

Restore complete backups only: run brrestore with the option '-m full'.

BKI7323W **Request for a partial restore or restore from snapshot with 'brrestore -m all' is not supported. If you want to restore the backup: - with a snapshot-type restore enter 'stop' and rerun brrestore with '-m full' - from TSM enter 'cont'**

Explanation:

This message has the same reason as message BKI7322E, but in this case the data is also available from the TSM server. So you may continue to restore this data without the snapshot functionality from TSM server.

User response:

Enter 'stop' if you want to try to restore a different set

of files. Enter 'cont' if you want to restore this data from TSM server.

BKI7324E Restore of multiple backup IDs in one run from a snapshot is not possible.

Explanation:

The data requested for this restore belongs to multiple backup IDs

User response:

Make sure the files you want to restore belong to one single backup ID and try again.

BKI7535W Error executing command *command name***. Reason: errno (***error number***)** *explanation***.**

Explanation:

The command *command name* could not be executed successfully.

User response:

Check the explanation *explanation* and the preceding output of the command execution to detect the cause of the error.

BKI7536I Execute command *command name***.**

Explanation:

The command *command name* is executed by the application. This message is followed by the output of the command executed.

User response:

None

BKI8201E SIMULATION CANCELED BY PRODUCTION OPERATION!!!

Explanation:

The current operation was a simulation performed via the Administration Assistant. This simulation was canceled since a production operation (backup or restore) has been started.

User response:

Check your backup schedule and run simulations only when no other operations are scheduled.

BKI8300I *Function_name* **returned with code** *return_information***.**

Explanation:

This message indicates that the named API function ended with the specified return information.

User response:

If the return information indicates a problem, look for preceding error messages in the log files. Otherwise, no response is required.

BKI8303E No <segment_name> section found for the instance '<id>'.

Explanation:

An error was detected while parsing the named profile segment name section.

User response:

Check the named profile segment name section and make appropriate adjustments.

BKI8304W The following error occurred while verifying the configuration for section '<section>':

Explanation:

An error was detected while parsing the named profile section.

User response:

Check the named profile section and make appropriate adjustments.

BKI8306E The keyword *keyword* **is not allowed multiple times within the profile.**

Explanation:

The keyword indicated was found more than once in the profile. However, this keyword must not be specified multiple times.

User response:

Correct the profile.

BKI8307E The parameter *keyword* **must be specified in the profile.**

Explanation:

A required keyword is missing in the profile.

User response:

Correct the profile.

BKI8308E Single argument required for parameter *keyword***.**

Explanation:

The keyword indicated requires a single value. However, two or more values are found in the profile.

User response:

Correct the profile.

BKI8309E **Missing argument for parameter** *keyword***.**

Explanation:

In the profile, a value is missing for the named parameter.

User response:

Correct the profile.

BKI8310E **The keyword** *keyword* **is not allowed.**

Explanation:

An invalid keyword was detected in the profile.

User response:

Correct the profile.

BKI8311E **For parameter** *keyword***, both server and port must be specified.**

Explanation:

A value of the named parameter is missing from the profile.

User response:

As the value for the specified parameter, specify both server and port.

BKI8312E **Error while parsing parameter** *keyword***. In order for '***value1***' to be valid '***value2***' is required to be an existing directory.**

Explanation:

Value1 was found to be an invalid value for the parameter named. For this specific parameter, a file name can be specified whose path must already exist in the system.

User response:

Specify the name of a file in an existing path.

BKI8317W *Product_name***: Verification of configuration requested by user. No backup started.**

Explanation:

The user requested a verification of the configuration. The backup flow continued without errors up to the point where the snapshot would actually be done and was then cancelled. The system is ready for a snapshot backup, but no action beyond verification has been taken so far.

User response:

None.

BKI8319W **Error while deleting old versions. This problem does not affect the new backup. Error information:** '*error_information*'

Explanation:

After a successful backup, the system tries to remove older backups of the database according to the value of profile parameter MAX_VERSIONS. However, a problem occurred while trying to remove expired backups. The new backup is not affected by this problem.

User response:

Check the appropriate log files in order to determine the cause of the problem. Resolve any problems indicated. In case the storage device runs out of storage because outdated snapshot backups have not been removed, delete these snapshot backups manually.

BKI8320I **Deleting full backup** *backup_id - backup_key***.**

Explanation:

After a successful backup, the system tries to remove older backups of the database according to the value of profile parameter MAX_VERSIONS. During this process, the full backup listed is removed.

User response:

None.

BKI8321I **Deleting partial backup** *backup_id* **for node:***host:partition_number***.**

Explanation:

After a successful backup, the system tries to remove older backups of the database according to the value of profile parameter MAX_VERSIONS. During this process, the backup listed for the named partition is removed.

User response:

None.

BKI8322E **Interface problem: Current database partition** *number* **not listed in the partition list.**

Explanation:

The partition list passed by the database does not contain the named partition participating in an operation.

User response:

Contact your IBM support personnel.

BKI8325E Failed to determine hostname.

Explanation:

The system was not able to determine the host name of the machine.

User response:

Make sure the system setup allows for querying the hostname via system function gethostname(). Ensure that the requirements for doing snapshot backups are met.

BKI8326E Failed to create log directory *path***.**

Explanation:

The log path indicated is not available in the system and could also not be created.

User response:

Check the properties of the path indicated and make sure that its properties and the properties of the parent directory are set accordingly. Make sure all prerequisites for doing snapshot backups are met.

BKI8327E Invalid value specified for parameter *keyword***:** *value*

Explanation:

A parameter value is not valid.

User response:

In case the parameter was specified in the profile correct the profile. In case the parameter was specified as a command line option, correct the entry.

BKI8328E *Product_name* **must be licensed to set parameter** *keyword* **to a value of** *value***.**

Explanation:

Selected functions are supported only with a full TSM license.

User response:

If you need the functionality requested, obtain a full TSM license and install the license file. Otherwise, in case the parameter was specified in the profile, correct the profile or, in case the parameter was specified as a command line option, correct the entry.

BKI8330E Parameter *keyword* **requires 'YES', 'NO', or number.**

Explanation:

For the named parameter, only numeric values, 'YES', and 'NO' are accepted.

User response:

Correct the profile or the call as appropriate.

BKI8331E The parameter *keyword1* **is not allowed if** *keyword2* **is set to** *value***.**

Explanation:

There is a dependency between parameters *keyword1* and *keyword2*. If the latter is set to the value named, *keyword1* must not be specified.

User response:

Correct the profile or the call as appropriate.

BKI8332E Failed to parse parameter *keyword***. File names in the profile need to be fully qualified.**

Explanation:

As the value of the parameter indicated, a fully qualified file name is expected. However, the specified value is not a fully qualified path.

User response:

Correct the profile or the call as appropriate.

BKI8333E In order to enable the parameter *keyword1* **you need to set** *keyword2* **to** *value***.**

Explanation:

There is a dependency between parameters *keyword1* and *keyword2*. If *keyword1* is specified, *keyword2* must be given the specific value indicated in the message.

User response:

Correct the profile or the call as appropriate.

BKI8334E Profile section *section_name* **is required for function** *operation***.**

Explanation:

The specified profile section is required in order to perform the requested operation. However, it is not included in the profile.

User response:

Correct the profile.

BKI8335E Profile section *section_name* **refers to a value for** *keyword* **that differs from the one used at backup time. Expected value:** *value***.**

Explanation:

The profile parameter named must not change its value between backup and restore. However, in the named profile section, the parameter has a value different from the value it had at backup time. This value is given in the message.

User response:

Correct the profile by setting the indicated parameter to the value indicated in the message.

BKI8336E **Invalid value specified for option** *keyword:value*

Explanation:

An option value is not valid.

User response:

Correct the call.

BKI8337E **Error while parsing profile: Missing section name.**

Explanation:

The profile is organized into named sections. However, a section name was not found.

User response:

Check that the profile name is specified correctly or that the default profile is a valid profile. Refer to your user documentation for the syntax of the profile or use the profile wizard to create a new profile.

BKI8338E **Error while parsing profile: Section** *section_name* **is not allowed to be nested.**

Explanation:

In the profile, the named section starts before the previous section ends. However, the section in question cannot be nested.

User response:

Correct the profile.

BKI8339E **Error while parsing profile: Profile section** *section_name* **is not valid.**

Explanation:

An invalid section name was found in the profile.

User response:

Correct the profile.

BKI8340E **Error while parsing profile: Profile section** *section_name* **must not be specified more than once.**

Explanation:

In the profile, only a single section with the name indicated can be specified. However, during parsing, a second occurrence was detected.

User response:

Correct the profile.

BKI8341E **Error while parsing profile: Profile section** *section_name* **missing.**

Explanation:

The required profile section indicated was not found in the profile.

User response:

Correct the profile.

BKI8343W **The parameter** *keyword1* **of** *keyword2 value2* **has changed its value from** *value1* **to** *value3***.**

Explanation:

The profile parameter named must not change its value between backup and restore. However, in the named profile section, the parameter has a new value *value3* different from the value *value1* it had at backup time. Both values are given in the message.

User response:

Check the log file for problems that may result from the change of parameter values. If so, you may want to change the profile, restoring parameter *keyword1* to the value it had when creating the backup in order to perform a specific operation.

BKI8345E **Error while parsing parameter** *keyword***. '***path***' is required to be** *type_information***.**

Explanation:

A path of the type indicated in the message is expected as a value of the named parameter. However, the specified path was not found to be of the correct type.

User response:

Correct the profile or the call as appropriate.

BKI8349I **Deleting incomplete backup** *backup_id-backup_key* **.**

Explanation:

After a successful backup, the system tries to remove older backups of the database according to the value of profile parameter MAX_VERSIONS. During this process, the incomplete backup listed is removed. A backup becomes incomplete when parts of its data expire. This can happen when a backup that is marked 'destructively restorable' is restored.

User response:

None.

BKI8351E Parameter <parameter> requires 'AUTO' or a decimal value.

Explanation:

The value specified for the named parameter does not comply with the defined range of values.

User response:

Check the named profile keyword and make appropriate adjustments.

BKI8352E Parameter <parameter> requires a decimal value.

Explanation:

The value specified for the named parameter does not comply with the defined range of values.

User response:

Check the named profile keyword and make appropriate adjustments.

BKI8353E Parameter <parameter> requires a value greater than '0'.

Explanation:

The value specified for the named parameter does not comply with the defined range of values.

User response:

Check the named profile keyword and make appropriate adjustments.

BKI8354E Parameter <parameter> requires 'NO' or 'YES'.

Explanation:

The value specified for the named parameter does not comply with the defined range of values.

User response:

Check the named profile keyword and make appropriate adjustments.

BKI8355E Parameter <parameter> requires 'ALL' or a comma separated list of decimal values.

Explanation:

The value specified for the named parameter does not comply with the defined range of values.

User response:

Check the profile keyword DBPARTITIONNUM and make appropriate adjustments.

BKI8356E <product_name>: interface problem in function <function>: Invalid call sequence; the library was not initialized.

Explanation:

An invalid internal call sequence was detected during execution of a dedicated function.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI8357E <product_name>: interface problem in function <function>: Invalid call sequence; the operation was not initialized.

Explanation:

An invalid internal call sequence was detected during execution of a dedicated function.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI8359E The profile parameter <parameter> has the wrong value '<value>'. The expected value is '<value>'.

Explanation:

A profile parameter (or keyword) has a wrong value assigned. An alternate value is expected.

User response:

Check the named TSM for ERP profile keyword and make appropriate adjustments.

BKI8360E Invalid <keyword> specified in the profile.

Explanation:

The value specified for a keyword is either wrong or is missing.

User response:

Check the named TSM for ERP profile keyword and make appropriate adjustments.

BKI8361E Found non-database files on the file systems to back up. Please provide a negative list or clean your file systems.

Explanation:

Although the previously mentioned files were not requested to be part of the backup, they will be copied because they reside on a file system that will be backed

up in its entirety. In order to allow backing up those files, they need to be added to a 'negative list' or the checking for such files needs to be disabled. Note that in case of a restore, these files would typically be restored, even if this were not desired.

User response:

Edit the 'CLIENT' section of the profile. You can either set the parameter 'NEGATIVE_LIST' to 'NO_CHECK', to allow TSM for ACS to back up any file stored in a file system that will be backed up, or you can set the parameter 'NEGATIVE_LIST' to point to a file (the 'negative list') that contains a list of all files and directories that are allowed to be processed during backup. Any directory you add to the 'negative list' is processed recursively. Note that there is only one 'negative list' for backup and restore. See BKI6969E for restore.

BKI8362E The trace parameters YES, NO, ON, and OFF cannot be set in conjunction with other trace parameters.

Explanation:

The values YES, NO, ON and OFF in conjunction with the TRACE keyword do not allow further trace flags to be set. They are mutually exclusive.

User response:

Check the TSM for ERP profile keyword TRACE and make appropriate adjustments.

BKI8363E The value <value> is not a valid trace flag.

Explanation:

The value specified for the TRACE keyword is invalid.

User response:

Check the TSM for ERP profile keyword TRACE and make appropriate adjustments.

BKI8364E Error while parsing parameter CONFIG_FILE. Directory '<directory>' for node '<node>' does not exist.

Explanation:

The base directory containing the TSM for ERP configuration file(s) for any participating DB2 partition does not exist or cannot be accessed.

User response:

Ensure that the directory denoting the base part of the CONFIG_FILE value (left part of the %DB2NODE substring) exists and has the right permissions.

BKI8365E The server stanza for LOG_SERVER '<server>' is missing.

Explanation:

A TSM server stanza used by the LOG_SERVER keyword is missing either in the option file (dsm.opt) or in the system options file (dsm.sys).

User response:

Either the value of the LOG_SERVER keyword in the TSM for ERP profile has to be adjusted or an entry must be made or adjusted in the appropriate option file.

BKI8366E The values for parameter <parameter> are expected to be in the range 0 to 6.

Explanation:

The values of the keyword USE_AT have to be in the range of 0 to 6.

User response:

Check the TSM for ERP profile keyword USE_AT and make appropriate adjustments.

BKI8367E You cannot freeze the filesystem without suspending or shutting down the database.

Explanation:

The prerequisites for freezing the filesystem are either to suspend the database or to bring the database offline.

User response:

Ensure either to suspend the database or to bring the database offline and try to freeze the filesystem again.

BKI8368E An invalid argument is specified for keyword <keyword>.

Explanation:

The specified argument could not be converted into an equivalent integer value.

User response:

Check the keyword argument and try again. If the problem cannot be resolved contact your IBM support personnel.

BKI8369E Failed to execute <program>. Reason: <reason>.

Explanation:

The execution of <program> failed.

User response:

Check the logs for further information. If the problem

cannot be resolved contact your IBM support personnel.

BKI8370E The profile option TARGET_DATABASE_SUSPEND= OFFLINE is not allowed for an online database backup.

Explanation:

A snapshot backup of a database that was not suspended can only be done in offline mode.

User response:

Start the BRBACKUP utility with the option '-t offline -d util_vol' and try again.

BKI8371E The profile parameter NEGATIVE_LIST is not allowed. Use BR*TOOLS option "-n" to specify the negative list.

Explanation:

The negative list value has to be specified in the init<SID>.sap profile via the option 'util_vol_nlist = (<nfile_name1>, <nfile_name2>, ...) | no_check'.

User response:

Adjust the init<SID>.sap profile accordingly and try again.

BKI8372E The profile option TARGET_DATABASE_SUSPEND=YES requires a backup of type volume_online.

Explanation:

A snapshot backup of a database that was suspended can only be done in online mode.

User response:

Start the BRBACKUP utility with the option '-t online -d util_vol' and try again.

BKI8373W Operation will execute with force option (-F).

Explanation:

The operation started will be run in forced mode, e.g. delete.

User response:

None.

BKI8374W Operation will terminate with an error because backint was executed with the verify option (-V).

Explanation:

The verify option simulates the requested option and does not create a valid backup or restore. In order to prevent the calling process from regarding the current operation as successful, the verify option will always yield a nonzero return code.

User response:

Do not use the verify option if you want to create a backup or restore.

BKI8375E The value of the environment variable ORACLE_SID is not allowed to have more than <number> digits.

Explanation:

The length of the ORACLE_SID value violates the defined range.

User response:

Check the current value of ORACLE_SID and if necessary, correct it according to the allowed length. Try again.

BKI8376E Verification of snapshot failed. Reason: <reason>

Explanation:

The snapshot backup could not be verified successfully.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI8377E Function <function> does not support multiple backup ids within a single operation.

Explanation:

TSM for ACS was requested to perform a volume <function> operation simultaneously for a set of objects that were backed up with multiple volume backup requests. This is currently not supported.

User response:

Use backups stored on the TSM server to perform redirected restores or adjust the restore command.

BKI8378E Redirected restore of volume backups is not supported yet.

Explanation:

TSM for ACS does not support restores to an alternate data location. The restore always needs to be made to the original data location.

User response:

Use backups stored on the TSM server to perform redirected restores.

BKI8379E Infile contains an invalid value: '<value>'

Explanation:

Each record of the infile has to start either with the string '#NULL' or with the backup Id.

User response:

Ensure each record of the infile satisfies the requirements. If the problem cannot be resolved contact your IBM support personnel.

BKI8380E The profile option TSM_BACKUP=YES requires a snapshot backup of all partitions of the database.

Explanation:

The profile option TSM_BACKUP=YES implies offloading a snapshot backup to TSM. If this option is specified, all database partitions have to be part of the snapshot backup.

User response:

Specify the 'ALL DBPARTITIONNUMS' clause as part of the DB2 backup command and try again.

BKI8381W The following error occurred while verifying the configuration for server '<server_name>' in the profile:

Explanation:

The profile section for server <server_name> is not correct. The actual error is following this message.

User response:

Adjust the profile and correct the error following this message.

BKI8382E The previous error(s) can be prevented by executing restore with negative list set to 'no_check'.

Explanation:

An error occurred while inspecting file systems for files that should be excluded during the backup/restore operation. This error precedes the current message. Note that the file system inspection can be turned off by setting the parameter 'NEGATIVE_LIST' to 'NO_CHECK'.

User response:

Resolve the root cause for this problem (previous error) or change the value of the parameter 'NEGATIVE_LIST' to 'NO_CHECK'.

Depending on the application type, this can be accomplished by

- (for DB2 and native Oracle) editing the TSM ACS profile and set the parameter 'NEGATIVE_LIST' to 'no_check'
- (for SAP® for Oracle) editing the BR*Tools profile *.sap and set the parameter 'util_vol_nlist' to 'no_check'

Note that changing 'NEGATIVE_LIST' to 'NO_CHECK' implies that TSM for ACS would potentially backup all files residing on the requested file systems. This true even if they were not explicitly requested and resided on the requested file systems, and even if they were not explicitly requested during the backup. At restore time all of these objects would typically be restored.

BKI8383E BR*Tools are required to set the environment variable BI_RUN for volume backups.

Explanation:

This is a unique ID from a BR*Tools run (normally it is the name of the BR*Tools log). If this variable is set then BACKINT recognizes that a call from BR*Tools 7.10 or higher was triggered.

User response:

Ensure that BR*Tools 7.10 or later is used and rerun the operation.

BKI8384E Failed to determine the APPLICATION_TYPE of the profile. Please invoke wizard with option -m <application type>.

Explanation:

'acsd -f wizard' was invoked to modify an existing profile, and the APPLICATION_TYPE could not be identified by inspecting this profile. This is required in order to properly adjust the profile.

User response:

Provide the application type when invoking the wizard with options 'acsd -f wizard -m <application type>'. The preferred method, however, is to call the setup script without options.

BKI8385E In order to create a new profile the wizard needs to be invoked with option -m <application type>.

Explanation:

'acsd -f wizard' was invoked to create a new profile. In this case it is required to specify the application type with option -m.

User response:

Provide the application type when invoking the wizard by using the options 'acsd -f wizard -m <application type>'. Alternatively, you can use the database-specific

version of the setup script (`setup_<database>.sh`) to create a new profile and configure TSM for ACS.

BKI8386E **Parameter** *parameter name* **requires a decimal value of 0 or greater.**

Explanation:

The value specified for the named parameter does not comply with the defined range of values.

User response:

Check the named profile keyword and make appropriate adjustments.

BKI8387W **Found additional files on the file systems to backup:** *filename*

Explanation:

Although the previously mentioned files were not requested to be part of the backup, they will be copied because they reside on a file system that will be backed up in its entirety.

User response:

Edit the 'CLIENT' section of the profile. You can either set the parameter 'NEGATIVE_LIST' to 'NO_CHECK', to allow TSM for ACS to back up any file stored in a file system that will be backed up, or you can set the parameter 'NEGATIVE_LIST' to point to a file (the 'negative list') that contains a list of all files and directories that are allowed to be processed during backup. Any directory you add to the 'negative list' is processed recursively. Note that there is only one 'negative list' for backup and restore. See BKI6969E for restore.

BKI8389W **The following volume groups or file systems are currently not accessible:** *volume groups* **or** *file systems*

Explanation:

The listed volume groups or file systems are not accessible. TSM ACS tries to verify that only database files reside in the volume groups or file systems that will be restored. But it was encountered that it was not possible to access the file systems (in the volume groups) to verify the database files because the file systems are not mounted or the volume groups are not imported, or both. This warning message is followed by message BKI9390E which gives more information.

User response:

This is just a warning message. Follow the instructions of the user response of BKI8390E.

BKI8390E **Failed to validate that only database files will be overwritten during restore, because some of the database file systems are currently not accessible. Please import volume groups and/or mount all file systems and restart the restore. If you cannot mount the file systems as a consequence of a disaster or a failing previous restore operation, this error can be prevented by executing restore with negative list set to 'no_check'.**

Explanation:

TSM ACS tries to verify that only database files reside in the volume groups / file systems that will be restored. But it was encountered that it was not possible to access the file systems (in the volume groups) to verify the database files because the file systems are not mounted and/or the volume groups are not imported.

User response:

There are two options to solve this problem:

1. Import all volume groups and mount all file systems that contain database files.
2. If the first option is not possible as a consequence of a disaster or a failing previous restore operation, the negative list check cannot be performed at all and must be switched to 'no_check'. Depending on the application type, this can be accomplished by
   - (for DB2 and native Oracle) editing the TSM ACS profile and set the parameter 'NEGATIVE_LIST' to 'no_check'
   - (for SAP® for Oracle) editing the BR*Tools profile *.sap and set the parameter 'util_vol_nlist' to 'no_check'

Note that changing NEGATIVE_LIST to NO_CHECK implies that TSM for ACS would potentially backup all files residing on the requested file systems. This true even if they were not explicitly requested and resided on the requested file systems, and even if they were not explicitly requested during the backup. At restore time all of these objects would typically be restored.

BKI8513W **'TDP_DIR' is not set. The temporary path will be used.**

Explanation:

The environment variable 'TDP_DIR' is not set and therefore, the log will be written to the system's temporary path instead.

User response:

Set the 'TDP_DIR' environment variable.

BKI8668I TDI created successfully.

Explanation:

The metadata concerning the phyiscal database layout necessary for automatic redirected restores driven by BackOM were created successfully.

User response:

None.

BKI8669I Free space of device with ID 'id' containing the container storage path 'storage_path' is <free_space>.

Explanation:

After assigning a container storage path to a dedicated device the remaining free space is calculated and returned to the user.

User response:

None.

BKI8670I Remaining free space of device with ID 'id' after assigning container 'container_name' of size <size> is <free_space>.

Explanation:

After assigning or creating a tablespace container on a dedicated device the remaining free space is calculated and returned to the user.

User response:

None.

BKI8671I Using automatic storage path(s) <storage_path>.

Explanation:

A dedicated automatic storage path will be used.

User response:

None.

BKI8672I Redefining container path(s) of automatic storage tablespace <tablespace_name> with ID <id>.

Explanation:

The path(s) an automatic storage tablespace uses as a starting point for the container(s) will be redefined.

User response:

None.

BKI8729I Checking system resources ...

Explanation:

Prior to starting the redirected restore by BackOM the existing system resources, e.g. free space of a file system will be checked.

User response:

None.

BKI8769E Found multiple TDIs matching the given timestamp. Additional search conditions needed.

Explanation:

More than one TDI file for a database backup image was found on the TSM server. In such a scenario, the integrity of the metadata assigned to a database backup images is violated and prevents an automatic redirected restore driven by BackOM.

User response:

Contact your IBM support personnel.

BKI8805I The restore was cancelled by the user. Existing data was not overwritten.

Explanation:

The existing database is still operational.

User response:

None.

BKI8819I The TSM objects matching 'search mask' will be deleted.

Explanation:

The cleanup of a failed TSM for ERP database backup will delete any partial TSM backup image of that run already stored on the TSM server and matching 'search mask' .

User response:

None.

BKI8899E Interface problem in function <function>: Value '<value>' of parameter '<parameter>' is not supported with DB2 version '<version>'.

Explanation:

An unknown action code during the program execution was encountered.

User response:

Contact your IBM support personnel.

BKI9001E **Internal error:** *error*

Explanation:

The following internal error: *error* has been encountered.

User response:

Contact IBM Support.

BKI9003E **Incompatible components installed:** *component name component name*

Explanation:

The components mentioned in the message text can not be used together. This may be the result of an incomplete upgrade.

User response:

Contact IBM Support.

BKI9005E *A* **not supported by** *B***.**

Explanation:

The installed version of product *B* does not support product *A*. Most likely you need to upgrade product *B*.

User response:

Contact the IBM Support.

BKI9006E **Internal error while reading environment variable:** *variable***.**

Explanation:

This is an internal error.

User response:

Contact IBM Support.

BKI9007W **An error occurred while terminating the application:** *the error*

Explanation:

While terminating the application, an error occurred. This has no impact on the success of the operation.

User response:

None

BKI9008E **This product requires at least version** *number* **of** *product name* **to be installed.**

Explanation:

The version of the application *product name* is not supported by this application. Most likely application *product name* needs to be upgraded.

User response:

Contact IBM Support.

BKI9009W **The following products are not compatible:** *product name* **(***product version***) and** *product name* **(***product version***).**

Explanation:

This message is similar to BKI9008E. But in this case it's not obvious which one of the products needs to be upgraded. .

User response:

Contact IBM Support

BKI9010E **Could not determine installation directory for <program>. Please restart the process using a fully qualified name.**

Explanation:

The name of the path where a given program is located could not be determined.

User response:

Contact your IBM support personnel.

BKI9011E **There was no response received within <number> seconds; time has expired.**

Explanation:

The communication between two program components was supended or stopped, which can lead to a timeout.

User response:

Contact your IBM support personnel.

BKI9013E **Concurrent restore of objects being backed up with multiple device agents is not supported.**

Explanation:

This special restore scenario is unsupported.

User response:

Contact your IBM support personnel.

BKI9014E **Failed to load library: <library> reason: <reason>**

Explanation:

The ACS library could not be loaded.

User response:

Contact your IBM support personnel.

BKI9015E **Failed to locate functions in library: <library> reason: <reason>**

Explanation:

One or more functions could not be found in the ACS library.

User response:

Contact your IBM support personnel.

BKI9200E **Additional support information: An exception was thrown at position:** *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support

User response:

Contact IBM Support.

BKI9201E **Additional support information: An Exception was thrown at position:** *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support

User response:

Contact IBM Support.

BKI9202E **Additional support information: An Exception was thrown at position:** *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9203E **Additional support information: An exception was thrown at position:** *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support

User response:

Contact IBM Support.

BKI9204E **Additional support information: An Exception was thrown at position:** *position* **(text=***description***).**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9205E **Additional support information: Unable to instantiate** *name* **at position** *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9206E **Additional support information: Unable to use** *actual* **when expecting** *expected* **at position** *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9207E **Additional support information: An exception was thrown at position:** *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9208E **System error** *errno***:** *errno text* **at position** *position***.**

Explanation:

A system call failed with *errno*.

User response:

Check *errno* and *errno text* with you system administrator. If you cannot resolve the problem, contact IBM Support.

BKI9209E **Additional support information: No handler registered for message type** *message***. Thrown at position:** *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9210E **ESD_AbortDispatchingException thrown at position:** *position***.**

Explanation:

An internal error occurred.

User response:

Contact IBM Support.

BKI9211E **Additional support information: An Exception was thrown at position:** *position***. (State** *state***)**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9212E **Additional support information: No handler registered for message type** *type***. Thrown at position:** *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9213E **Internal error: A memory allocation request failed at position:** *position***.**

Explanation:

This error message indicates an out-of-storage condition. It may occur due to a previous error, or it may be owed to a large size of the internal buffers

User response:

Check for and respond to preceding error messages. You may also want to reduce the size of the internal buffers (keyword BUFFSIZE in the Data Protection for SAP profile).

BKI9214E **Additional support information: An exception was thrown from a destructor. Callstack follows:** *callstack***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9215E **The maximum string length supported for <name> is <length>.**

Explanation:

The supported string length of a system component, e.g. file name or hostname has been violated.

User response:

Check the components involved in the operation. If the problem cannot be resolved contact your IBM support personnel.

BKI9216E **Additional support information: An exception was thrown at position:** *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9217E **Additional support information: An exception was thrown at position:** *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9218E **Additional support information: An exception was thrown at position:** *position***.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9219E **Additional support information: Invalid error type *type* encountered.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact IBM Support.

BKI9220E **Additional support information: Second call of *call*.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact your IBM Support.

User response:

Contact your IBM Support.

BKI9221E **The operation ended prematurely with return code <rc>. An exception was thrown at position: <file>(<line>).**

Explanation:

An operation could not be finished successfully due to an unexpected termination.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI9222E **A snapshot-type operation was interrupted. Additional support information: An exception was thrown at position: <file>(<line>).**

Explanation:

A snapshot operation could not be finished successfully due to an unexpected interruption.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI9223E **The operation will be aborted.**

Explanation:

In internal error during an operation leads to an abort of that operation.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI9224E **The operation will be aborted due to a previous error.**

Explanation:

An internal error during an operation leads to an abort of that operation.

User response:

Check the logs for further information. If the problem cannot be resolved contact your IBM support personnel.

BKI9225E **The keyword <*keyword*> has not been found in the line <*line*> of the file <*file_name*>. Please change it back to the original value if you modified it.**

Explanation:

Occurs for example if the entries in the file /etc/inittab have been modified before a second installation.

User response:

Change the modified <*line*> in the <*file_name*> back to the original value, <*keyword*> gives a hint to what is expected.

BKI9300E **Additional support information: Aborting 'send' operation. See previous error.**

Explanation:

This error may have been caused by previous errors.

User response:

Check for previous errors and correct them.

BKI9301E **Additional support information: State *state* does not match state pattern *pattern*.**

Explanation:

This error message typically follows a previous error. If so this error message can be ignored. Otherwise contact IBM Support.

User response:

Contact your IBM Support.

BKI9302E **Additional support information: Unused ESD_ReturnChannel destroyed. Dumping callstack: *callstack***

Explanation:

This error message typically follows a previous error. If

so this error message can be ignored. Otherwise contact your IBM Support.

User response:

Contact your IBM Support.

BKI9306I **Dumping callstack:** *call stack*.

Explanation:

This message is always preceded by an error message indicating the problem. It provides additional information that might help IBM Support to analyze the cause of the problem.

User response:

If you need to call IBM Support, provide the information given in this message together with the error information.

BKI9307E **Did not find a winsock dll compatible with version** *expected version*. **Version found is** *available version*

Explanation:

The product failed to load the appropriate `winsock dll`.

User response:

Contact your system administrator

BKI9308E **A socket request timed out after processing** *number of bytes* **bytes** *position*.

Explanation:

A socket request was issued with a timeout and the requested action could not be completed within the time specified. It was cancelled after processing *number of bytes* bytes.

User response:

If you need to call IBM Support, provide the information given in this message together with the error information.

BKI9309E **Operation terminated due to an explicit abort request.**

Explanation:

An operation was terminated due to customer intervention.

User response:

None.

BKI9310E **Could not add** *backup_id* **to the repository at** *path*.

Explanation:

The system was not able to add information on the named backup to the repository located in the path indicated.

User response:

Make sure the repository path is set correctly. If you need to correct the repository location, restart the server executable afterwards. If the problem persists contact your IBM support personnel.

BKI9311E **Could not find** *backup_id* **in the repository at** *path*.

Explanation:

Information on the backup denoted by the backup ID could not be found in the repository located in the path indicated.

User response:

Make sure the repository path is set correctly. If you need to correct the repository location, restart the server executable afterwards. If the problem persists contact your IBM support personnel.

BKI9312E *backup_id* **is currently locked in the repository at** *path*.

Explanation:

The information on the backup denoted by the backup ID is currently locked by a different process. Make sure to run only a single operation using a specific backup at a time.

User response:

Wait for the other operation to finish or abort this operation. Then start again. If the problem persists contact your IBM support personnel.

BKI9313E **Failed to update** *backup_id* **in the repository at** *path*.

Explanation:

The information on the named backup could not be updated in the repository located at the path named.

User response:

Check the logs for other messages pointing to the cause of this problem. Resolve any problems indicated. If the problem persists contact your IBM support personnel.

BKI9314E **Could not remove** *backup_id* **from the repository at** *path***.**

Explanation:

An attempt to remove the information on the backup named from the repository located at the path indicated failed.

User response:

Check the logs for other messages pointing to the cause of this problem. Resolve any problems indicated. If the problem persists contact your IBM support personnel.

BKI9315E **Could not access the repository at '***path***' because it is currently locked by another process.**

Explanation:

When starting up, the server tried to load the repository located at the path named. However, the repository was locked by a different process. This can happen if two server processes try to use the same repository. This is not supported.

User response:

Make sure each instance of the server uses its own repository.

BKI9316E **The path '***path***' does not point to a valid repository location.**

Explanation:

When starting up, the server could not locate its repository.

User response:

Correct the profile or the call as appropriate.

Appendix B. Accessibility features for Tivoli Storage Manager

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features of Tivoli Storage Manager are described in this topic.

Accessibility features

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

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices
- User documentation provided in HTML and PDF format. Descriptive text is provided for all documentation images.

The Tivoli Storage Manager Information Center, and its related publications, are accessibility-enabled.

Keyboard navigation

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

Tivoli Storage Manager follows AIX operating system conventions for keyboard navigation and access.

Tivoli Storage Manager follows HP-UX operating-system conventions for keyboard navigation and access.

Tivoli Storage Manager follows Linux operating-system conventions for keyboard navigation and access.

Tivoli Storage Manager follows Sun Solaris operating-system conventions for keyboard navigation and access.

Vendor software

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

Related accessibility information

You can view the publications for Tivoli Storage Manager in Adobe® Portable Document Format (PDF) using the Adobe Acrobat Reader. You can access these or any of the other documentation PDFs at the IBM Publications Center at http://www.ibm.com/shop/publications/order/.

IBM and accessibility

For more information about the commitment that IBM has to accessibility, see the IBM Human Ability and Accessibility Center at http://www.ibm.com/able.

Notices

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

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

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

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

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

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

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

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

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

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

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

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

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

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

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

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

Glossary

This glossary defines terms specific to Tivoli Storage Manager for Enterprise Resource Planning.

A comprehensive glossary for Tivoli Storage Manager is located in the Tivoli Storage Manager Version 6.1 information center: http://publib.boulder.ibm.com/infocenter/tsminfo/v6.

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

Activate policy set
In Tivoli Storage Manager, the process of validating the contents of a policy set and copying the policy set to the ACTIVE policy set.

Active policy set
In Tivoli Storage Manager, the policy set that contains the policy rules currently in use by all client nodes assigned to the policy domain. The active policy set is the policy set that was most recently activated for the policy domain.

Adaptive File Sequencing
During backup with the file interface BACKINT, this feature of Data Protection for SAP optimizes performance by calculating a certain sequence of files to be backed up. This sequence considers the file sizes to be backed up and the distribution of files on several disks.

Administration Assistant
A Web-browser based graphical interface to support and assist customizing of Data Protection for SAP, simulating changes to the configuration and infrastructure, and analyzing SAP database backup and restore operations The Administration Assistant consists of the Administration Assistant server-level components (Server, Database Agent, Database) and one or more instances of the Administration Assistant client.

Administration Assistant client
Part of the Administration Assistant; applet started in a Web browser to access the Administration Assistant Server component.

Administration Assistant Database Agent
Administration Assistant server-level component responsible for receiving data from Data Protection for SAP and forwarding it to the Administration Assistant Server component for display as well as to the Administration Assistant Database component for retention.

Administration Assistant Database component
Administration Assistant server-level component responsible for storing data received from Data Protection for SAP via the Database Agent in an internal Administration Assistant database.

Administration Assistant scheduling client
Part of the Administration Assistant creating reports from a command-line interface using predefined templates.

Administration Assistant Server component
Part of the Administration Assistant communicating with the ProLE processes or services of various database servers. Administrators access the Server component via Administration Assistant clients.

Administration Assistant Server component configuration file
The file containing the configuration of your Administration Assistant Server component. The default file name of the server configuration file is assist.cfg, located in the installation path of the Administration Assistant Server component.

Administrative client
In Tivoli Storage Manager, a program that runs on a file server, workstation, or mainframe that allows administrators to control and monitor the Tivoli Storage Manager server through administrator commands. Compare with backup-archive client.

Apache Derby
An open-source database management system developed by IBM and bundled with the Administration Assistant. It is

the default DBMS for the internal Administration Assistant database.

API client
See Tivoli Storage Manager API.

Archive copy group
In Tivoli Storage Manager, a policy object containing attributes that control the generation, destination, and expiration of archive files. An archive copy group belongs to a management class.

ARCHIVELOG mode
A database can run in ARCHIVELOG mode or in NOARCHIVELOG mode. Production systems must run in ARCHIVELOG mode in order to allow proper backup restore. Test systems can run in NOARCHIVELOG mode.

Backup-archive client
A component of Tivoli Storage Manager running on a workstation or file server, providing a means for backing up, archiving, restoring, and retrieving files to or from the TSM server. Compare with administrative client.

Backup copy group
A policy object containing attributes that control the generation, destination, and expiration of backup files. A backup copy group belongs to a management class.

Backup Server
A Tivoli Storage Manager server where Data Protection for SAP sends the backup data to and retrieves data when restoring.

Backup version control
A feature of Data Protection for SAP allowing the customer to specify the number of full database backups to be kept on the TSM server. Obsolete database backups are deleted together with all dependent data (for example log files, incremental backups, etc.).

BRARCHIVE
An SAP database utility to perform backups of offline redo log files in an SAP Oracle database environment.

BRBACKUP
An SAP database utility to do online/offline backups of SAP Oracle databases. BRBACKUP can be used to back up data files, control files and online redo log files.

BRCONNECT
This SAP database utility ensures, that the database status required for the online/offline backup of an SAP Oracle database remains unchanged during the backup. BRCONNECT will be started internally by BRBACKUP and BRARCHIVE

BRRESTORE
An SAP database utility to restore an entire Oracle database backup or parts of it, previously backed up with BRBACKUP or BRARCHIVE. Any non-database files and directories which were saved can also be restored. Subdirectories within the sapdata directories will be created automatically, when necessary.

BR*Tools
Utilities provided by SAP to simplify the administration of an Oracle database system within an SAP environment.

Client options file
A configuration file of the TSM client containing a set of processing options that identify the server, communication method, and options for backup, archive, hierarchical storage management, and scheduling. Its default name is dsm.opt on UNIX or Linux systems and `<servername>.opt` on Windows.

Client system options file
A configuration file of the TSM client residing on UNIX or Linux systems, containing a set of processing options that identify the Tivoli Storage Manager servers to be contacted for services. This file also specifies communication methods and options for backup, archive, hierarchical storage management, and scheduling. Its name is dsm.sys.

Cloning of a database
Restore a database to a different location and changing the database alias or SID while leaving the physical layout of the database unchanged.

Control file
A file associated with a database that maintains the physical structure and time stamps of all files within that database. The control file is updated continuously during database use and must be available for writing, if the database is mounted or opened.

Configuration File
See Data Protection for SAP configuration file. See Administration Assistant server configuration file.

Copy group
A policy object of the TSM server containing attributes that control the generation, destination, and expiration of backup and archive files. There are two kinds of copy groups: backup and archive. Copy groups belong to management classes.

Database Agent
See Administration Assistant Database Agent.

Database component
See Administration Assistant Database component.

Database server
The server where the SAP database resides. Data Protection for SAP and the TSM API must be installed on this server.

Data Protection for SAP configuration file
Binary file containing persistent information used by Data Protection for SAP, such as the TSM client password or the current backup version number. Its default file name is init.<SID>.bki.

Data Protection for SAP File Manager
A utility that simplifies the Data Protection for SAP inquire, restore and delete operations. It can be seen as an add-on to Data Protection for SAP.

Data Protection for SAP profile
ASCII file containing option keywords for configuring Data Protection for SAP. Its default file name is init.<SID>.utl.

Data block
The smallest unit of a database.

Data file
A physical operating system file on disk containing data structures of a database, such as tables and indexes. A data file belongs to a specific tablespace in a database.

Device class
A named group of storage devices of a TSM server with common characteristics. Each device class has a unique name and represents a specific device type such as disk, file, optical disk, or tape.

DISK A device class that is defined by Tivoli Storage Manager at installation. It is used to categorize disk drives.

Data Protection for SAP
An abbreviation for 'Data Protection for SAP', which is used in this document.

File Manager
See Data Protection for SAP File Manager

File space
A logical space in a TSM server assigned to a specific client. Clients can restore, retrieve, or delete contents of their file spaces from Tivoli Storage Manager server storage. Tivoli Storage Manager does not necessarily store all the files from a single file space together, but can identify all the files in server storage that came from a single file space.

Include/exclude list
A group of include and exclude option statements in a file. Tivoli Storage Manager backup-archive client uses the statements to determine whether to back up or migrate certain files, and to determine the associated management classes to use for backup, archive, and space management. The exclude options identify files that should not be backed up or migrated off the client node. The include options identify files that are exempt from the exclusion rules, or assign a management class to a file or group of files for backup, archive, or space management services. The include/exclude list is defined either in an include/exclude file (for UNIX or Linux clients) or in the client options file (for other clients).

Incremental backup
An incremental backup saves only those blocks within the database, which have been changed since the last full backup. SAP R/3 release 4.5.A and later versions permit incremental backups of Oracle databases using Oracle's Recovery Manager RMAN.

LAN-free backup
Backup to a backup server residing on system different from that of the database server. The database and backup servers are connected via LAN. However, backup data is transferred directly to the storage media via SAN.

Local backup
Backup to a local backup server.

Local backup server
Backup server residing on the same system as the database server does.

Management class
Within IBM Tivoli Storage Manager, a policy object that users can bind to a file in order to specify how the server manages the file. The management class can contain a backup copy group, an archive copy group, and space management attributes. The copy groups determine how the Tivoli Storage Manager server manages backup versions or archive copies of files. The space management attributes determine whether files are eligible for migration from space manager client nodes to Tivoli Storage Manager storage, and under what conditions.

Media Management API
An interface provided by Oracle to which vendors are able to write compatible software libraries. This software integrates with Oracle. Thus, an Oracle server process is able to issue commands to the media manager to write backup files out to sequential storage (e.g., Tivoli Storage Manager) and read files from sequential storage.

Node

1. TSM: A unique name used to identify a Tivoli Storage Manager client to the TSM server.
2. SMP: Single machine in a Symmetrical Multiprocessor (SMP) environment.

Offline redo log
If the database is in ARCHIVELOG mode and an online redo log is filled, it is copied to one (or more) archive log destination(s), which is typically the saparch directory in an SAP environment. This copy is the offline redo log (also called archived redo log).

Online redo log
The online redo log is a set of two or more files that record all changes made to Oracle data files and control files.

Path A connection between a Tivoli Storage Manager node and a Tivoli Storage Manager server interface. On the client side, a path is defined by a logical server name listed in the client option file dsm.sys (UNIX or Linux systems) or `<servername>.opt` (Windows systems). At the server side, the possible paths are defined by the network addresses of the Tivoli Storage Manager server.

Policy domain
Within Tivoli Storage Manager, a policy object that contains policy sets, management classes, and copy groups that are used by a group of client nodes.

Policy set
Within Tivoli Storage Manager, a policy object that contains a group of management class definitions that exist for a policy domain. At any one time there can be many policy sets within a policy domain but only one policy set can be active.

ProLE The background process (UNIX or Linux) or service (Windows) controlling backup and restore operations of Data Protection for SAP.

Recovery Manager (RMAN)
A tool used to back up, restore and recover Oracle databases. It can be used with or without a Recovery Catalog,. If a Recovery Catalog is not used, Recovery Manager decides how to back up, restore and recover the database using the control file of the database. Incremental backups of Oracle databases can only be done with RMAN.

Remote backup
Backup to a remote backup server.

Remote backup server
Backup server residing on a system different from that of the database server.

Retention
The amount of time, in days, that inactive files backed up or archived to a TSM server are kept by the backup server before they are deleted. Copy group attributes and default retention grace periods for the domain define retention.

RMI Remote Method Invocation (Java)

SAP BACKINT interface
An interface provided by BR*Tools utilities that can be used to access

external backup programs, for example Data Protection for SAP.

SAP Note
Document containing service information provided by SAP. SAP Notes can be accessed (with an SAP user ID and password) at the SAP Service Marketplace: http://service.sap.com/notes

Scheduling client
See Administration Assistant scheduling client.

Server configuration file
See Administration Assistant Server component configuration file.

Session
Single TCP/IP connection between a Tivoli Storage Manager node and a Tivoli Storage Manager server. A TSM server may be configured to allow a number of sessions from a TSM node to the server in parallel over the same communication path.

Scratch volume
A volume that is available for Tivoli Storage Manager use. The volume is either labeled, or blank or contains no valid data, and is not defined to Tivoli Storage Manager.

Server configuration file
See Administration Assistant Server component configuration file.

Session
Single TCP/IP connection between a Tivoli Storage Manager node and a Tivoli Storage Manager server. A TSM server may be configured to allow a number of sessions from a TSM node to the server in parallel over the same communication path.

Shared library
Shared library (UNIX) or dynamic link library (DLL, Windows) implementing the vendor API of DB2 for backup and restore solutions. Data Protection for SAP functionality is partly implemented as a shared library.

Storage pool
A storage pool is a named collection of storage volumes that are associated with one device class. Each storage pool represents a collection of volumes that are the same media type. For example, a storage pool that is associated with a device class for 8 mm tape contains only 8 mm tape volumes.

Tablespace
A database is divided into one or more logical storage units, which are tablespaces. Each tablespace has a set of data files exclusively associated with it.

Tivoli Storage Manager (TSM)
IBM Tivoli Storage manager, a client/server program that provides policy-driven storage management to customers in a multivendor computer environment.

Tivoli Storage Manager API
A set of functions that applications running on a client platform can call to store, query, and retrieve objects from Tivoli Storage Manager storage.

util_file_online
A (data file) backup using an external backup program addressed by the BACKINT interface. If an online backup is running, the backup status is set and completed dynamically for the tablespaces being backed up. In this way, the volume of offline redo log files during an online backup can be reduced significantly.

Validate
In Tivoli Storage Manager, the process of ensuring that the active policy set contains a default management class and reports on copy group definition errors.

Volume
The basic unit of storage for the Tivoli Storage Manager database, recovery log, and storage pools. A volume can be an LVM logical volume, a standard file system file, a tape cartridge, or an optical cartridge. Each volume is identified by a unique volume identifier. See database volume, scratch volume, and storage pool volume.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

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

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

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

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

SAP and SAP NetWeaver are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

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

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

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Program Number: 5608-E05

Printed in USA

SC33-6340-10