Tivoli® Storage Manager for Enterprise Resource Planning
Version 6.2

Data Protection for SAP®
Installation and User's Guide for DB2

SC33-6341-11

Tivoli® Storage Manager for Enterprise Resource Planning
Version 6.2

Data Protection for SAP® Installation and User's Guide for DB2

SC33-6341-11

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

This edition applies to Data Protection for SAP Version 6 Release 2 Modification Level 0 (product number 5608-E05), available as a licensed program product, and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters. This edition replaces SC33-6341-10.

Contents

Figures

Tables

Preface

This publication documents how to use IBM Tivoli Storage Manager for Enterprise Resource Planning Data Protection for *SAP*® Version 6.2. 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 Version 6.2, March 2010.

Note on Advanced Copy Services and FlashCopy Manager

The product *IBM Tivoli Storage Manager for Advanced Copy Services* (*TSM for ACS*) was replaced by *IBM Tivoli FlashCopy Manager*. References in this publication, and in error messages, to *TSM for ACS* are also applicable to the *Tivoli FlashCopy Manager*.

Comments

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

Please 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.

Publications

IBM 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/v6r2.

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

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

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

Tivoli Storage Manager publications

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

Table 1. IBM Tivoli Storage Manager troubleshooting and tuning publications

Publication title	Order number
IBM Tivoli Storage Manager Client Messages and Application Programming Interface Return Codes	SC27-2877
IBM Tivoli Storage Manager Server Messages and Error Codes	SC27-2878
IBM Tivoli Storage Manager Performance Tuning Guide	GC23-9788
IBM Tivoli Storage Manager Problem Determination Guide	GC23-9789

Table 2. Tivoli Storage Manager server publications

Publication title	Order number
IBM Tivoli Storage Manager for AIX Installation Guide	GC23-9781
IBM Tivoli Storage Manager for AIX Administrator's Guide	SC23-9769
IBM Tivoli Storage Manager for AIX Administrator's Reference	SC23-9775
IBM Tivoli Storage Manager for HP-UX Installation Guide	GC23-9782
IBM Tivoli Storage Manager for HP-UX Administrator's Guide	SC23-9770
IBM Tivoli Storage Manager for HP-UX Administrator's Reference	SC23-9776
IBM Tivoli Storage Manager for Linux Installation Guide	GC23-9783
IBM Tivoli Storage Manager for Linux Administrator's Guide	SC23-9771
IBM Tivoli Storage Manager for Linux Administrator's Reference	SC23-9777
IBM Tivoli Storage Manager for 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

Table 2. Tivoli Storage Manager server publications (continued)

Publication title	Order number
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 Integration Guide for Tivoli Storage Manager FastBack	SC27-2828

Table 3. 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 4. 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 Using the Application Programming Interface	SC23-9793

Table 5. Tivoli Storage Manager Data Protection publications

Publication title	Order number
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

Support information

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

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

Getting technical training

Information about Tivoli technical training courses is available online.

Go to these Web sites for training information:

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

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

Searching knowledge bases

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

Begin by searching the Tivoli Storage Manager Information Center at http://publib.boulder.ibm.com/infocenter/tsminfo/v6r2. From this Web site, you can search the current Tivoli Storage Manager documentation.

Searching the Internet

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

To search multiple Internet resources, go to the support Web site for Tivoli Storage Manager at http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager.

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

From the Support Web site, you can search various resources including:
- IBM technotes
- IBM downloads
- IBM Redbooks® publications
- IBM Authorized Program Analysis Reports (APARs)

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

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

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

To share your experiences and learn from others in the Tivoli Storage Manager user community, go to the Tivoli Storage Manager wiki at http://www.ibm.com/developerworks/wikis/display/tivolistoragemanager.

Using IBM Support Assistant

IBM Support Assistant is a complimentary software product that helps you with problem determination. You can install the stand-alone IBM Support Assistant application on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products that you use.

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

The product-specific plug-in modules provide you with the following resources:

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

Find add-ons for specific products here: http://www.ibm.com/support/docview.wss?&uid=swg27012689.

Finding product fixes

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

You can determine what fixes are available by checking the IBM Software Support Web site at http://www.ibm.com/support/entry/portal/.

- If you previously customized the site based on your product usage:
  1. Click the link for your Tivoli Storage Manager product, or one of the other Tivoli Storage Manager components that you want to find a fix for.
  2. Click **Downloads**, and then click **Fixes by version**.
- If you have not customized the site based on your product usage, click **Downloads** and search for your product.

Receiving notification of product fixes

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

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

1. From the support page at http://www.ibm.com/support/entry/portal/, click **My notifications** in the notifications module.
2. Sign in using your IBM ID and password. If you do not have an ID and password, click **register now** above the IBM ID and password.
3. Click the **Subscribe** tab to select your product family and click **Continue**.
4. Select the type of information that you want to receive, and add your personal preferences. You can specify how you want to be notified, how often, and you can also optionally select a folder for the notifications.
5. Click **Submit**.
6. For notifications for other products, repeat steps 4 and 5.

   Tip: You can also pick a product first, from the main support portal site, and then click in the **Notifications** section to create or update your subscription for that product.

Contacting IBM Software Support

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

Before you contact IBM Software Support, follow these steps:

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

Then see “Submitting the problem to IBM Software Support” on page xvii for information on contacting IBM Software Support.

Setting up a subscription and support contract

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

For IBM distributed software products (including, but not limited to, IBM Tivoli, Lotus®, and Rational® products, as well as IBM DB2® and IBM WebSphere® products that run on Microsoft® Windows® or 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:** You can call 1-800-IBMSERV (1-800-426-7378) in the United States, or 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**.

Determining the business impact

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

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

Describing the problem and 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 using a workaround for this problem? If so, be prepared to explain it when you report the problem.

Submitting the problem to IBM Software Support

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

Online

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

By 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.

New for Data Protection for *SAP* Version 6.2

The following feature is new for Data Protection for SAP for DB2 Version 6.2:

- Backup objects are partitioned into smaller segments to improve the handling of very large objects.

New for Data Protection for *SAP* Version 6.2

The following feature is new for Data Protection for SAP for DB2 Version 6.2:

- Backup objects are partitioned into smaller segments to improve the handling of very large objects.

Chapter 1. Protection for SAP database servers

Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP for DB2 protects SAP® system data and is integrated with the database-specific utilities of IBM DB2. Data Protection for SAP improves the availability of SAP database servers and reduces administration workload with automated data protection features that are designed specifically for SAP environments.

Data Protection for SAP provides these features and functions.

Data Protection for SAP for DB2 overview

Data Protection for SAP for DB2 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 DB2-based SAP® systems. It is integrated with DB2 backup and recovery facilities 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.

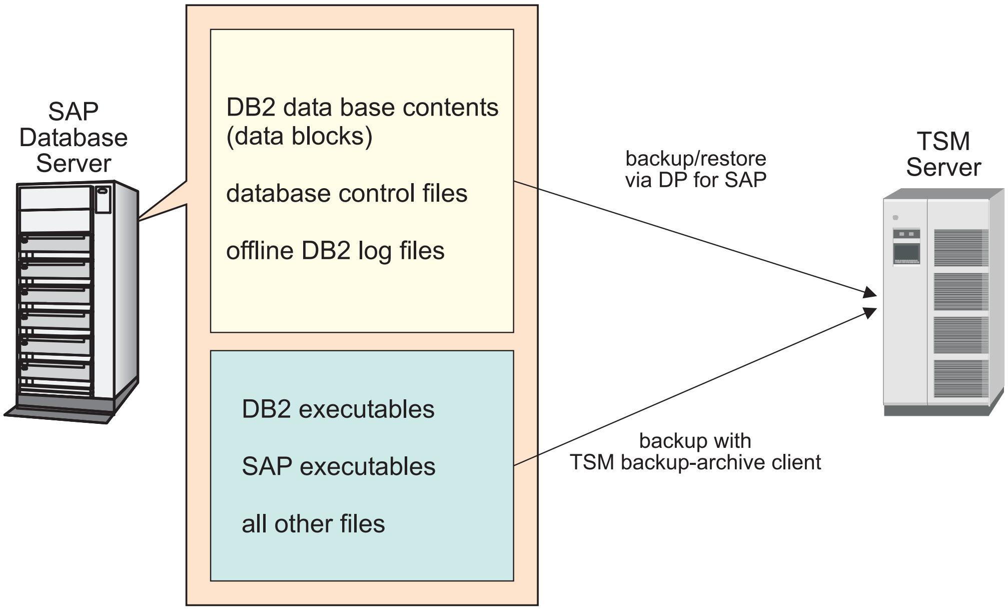


Figure 1. Scope of Data Protection for SAP for DB2

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 database contents, database specific control files, e.g. the database configuration, the history and the log file header, and offline DB2 log files.

Other files (such as SAP and DB2 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 DB2 executable files must be available before using Data Protection for SAP to restore and recover the database.

Data Protection for SAP integration with SAP®

Data Protection for SAP operates as an transparent link between DB2 and the Tivoli Storage Manager. A shared library is dynamically linked by DB2 backup/archive processes.

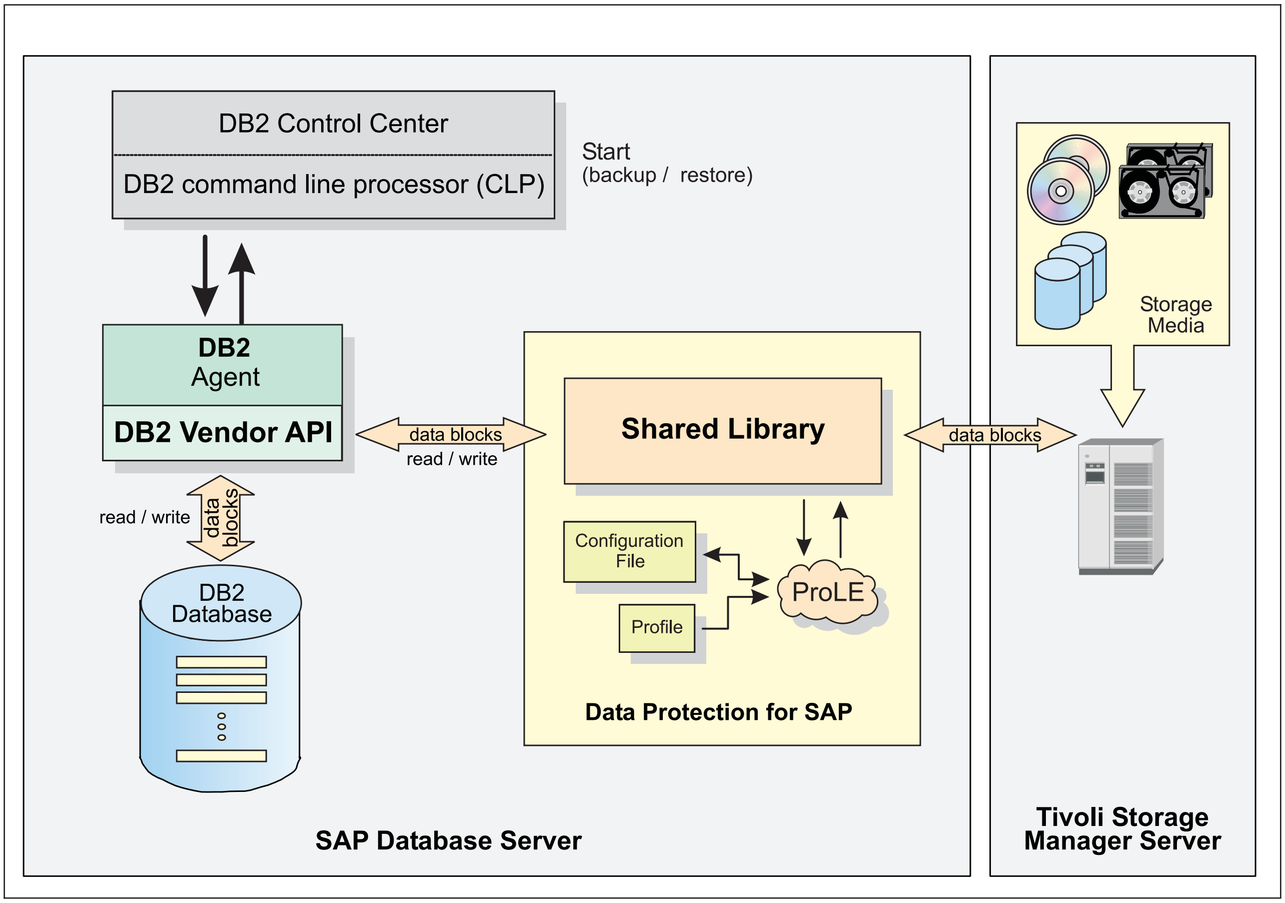


Figure 2. Integration of Data Protection for SAP with DB2

Data Protection for SAP also provides the Administration Assistant function for Data Protection for SAP which is used to increase administrator productivity. The Administration Assistant function for Data Protection for SAP 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 all SAP systems backed up by Data Protection for SAP, 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 87.

DB2 command line processor

The DB2 Command Line Processor (CLP) interprets commands for the DB2 database and passes control to a DB2 Server Process. In the case of Data Protection for SAP for DB2, the "LOAD *libraryname*" option instructs DB2 to invoke the Data Protection for SAP shared library. This process launches the backup or restore operation, dynamically loads the library, and communicates with Data Protection for SAP through the Vendor API.

For starting a backup or restore, the DB2 CLP communicates with the DB2 Server Process and provides information to the Server Process for processing the database.

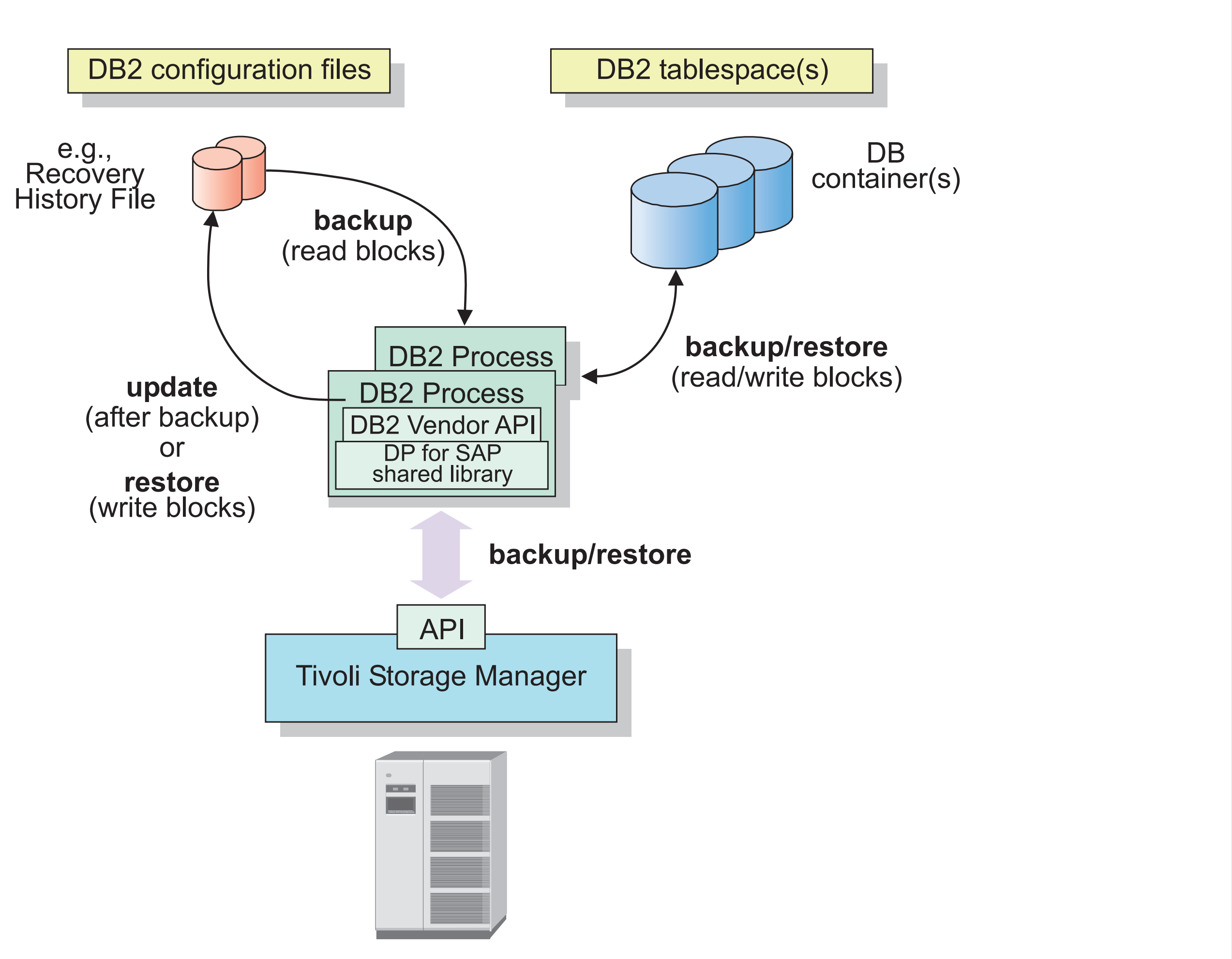


Figure 3. DB2 Backup Architecture

The DB2 **BACKUP DATABASE** command performs this DB2 Server process:

- creates a unique timestamp to identify the backup
- loads Data Protection for SAP dynamically as a shared library
- reads the data from the database containers
- reads the DB2 configuration files
- creates data blocks containing the backup image and passes these blocks to the data mover part of Data Protection for SAP

The Data Protection for SAP shared library sends the data to the Tivoli Storage Manager server storage (tape or disk). At the end of the backup process, the DB2 Server process logs the backup in the Recovery History File.

The DB2 **RESTORE DATABASE** command performs this DB2 Server process:
- loads Data Protection for SAP dynamically as a shared library
- requests the backup data from the shared library

The Data Protection for SAP shared library
- checks with the Tivoli Storage Manager if the backup image is available
- retrieves the data blocks from TSM
- passes the data blocks to the DB2 Server Process

The DB2 Server Process
- restores the DB2 data to the database containers
- logs the restore in the Recovery History File

DB2 Backup Object Manager utility

Backup objects, such as database or tablespace backups and DB2 log files, can be managed with the Data Protection for SAP for DB2 Backup Object Manager. Information about Backup Object Manager commands and options is provided.

The Backup Object Manager is a utility that performs these tasks:
- Verify and store a Tivoli Storage Manager password.
- Find backup objects in Tivoli Storage Manager.
- Check the properties of the backup objects in Tivoli Storage Manager.
- Remove any backup object from Tivoli Storage Manager.
- Backup database and selected tablespaces.
- Restore database and tablespace backups to the corresponding database.
- Retrieve files from Tivoli Storage Manager and restore them to the file system.
- Perform a redirected restore of databases (cloning).

The Backup Object Manager is designed to handle DB2 log files archived with Data Protection for SAP, the SAP® tool BRARCHIVE, and those files archived with Data Protection for SAP and the DB2 Log Manager. No special Backup Object Manager customization or configuration is necessary. Due to the log chain concept used by the DB2 Log Manager, all log files archived on Tivoli Storage Manager with Data Protection for SAP will be associated to one of these chains by the Backup Object Manager. However, the SAP-DB2 Administration Tools BRARCHIVE and BRRESTORE do not support the log chain concept. Therefore, log files archived with BRARCHIVE and Data Protection for SAP will be associated with a default value. For example, the first log chain is `'0'` or `'C0000000'`. However, log files archived with the DB2 Log Manager and Data Protection for SAP will be associated with the appropriate log chain number and handled by the Backup Object Manager accordingly. Detailed information regarding the DB2 Log Manager and the log chain concept is available in your DB2 *Administration Guide* documentation.

This graphic displays how the Backup Object Manager interacts with the Tivoli Storage Manager server and the SAP database Server:

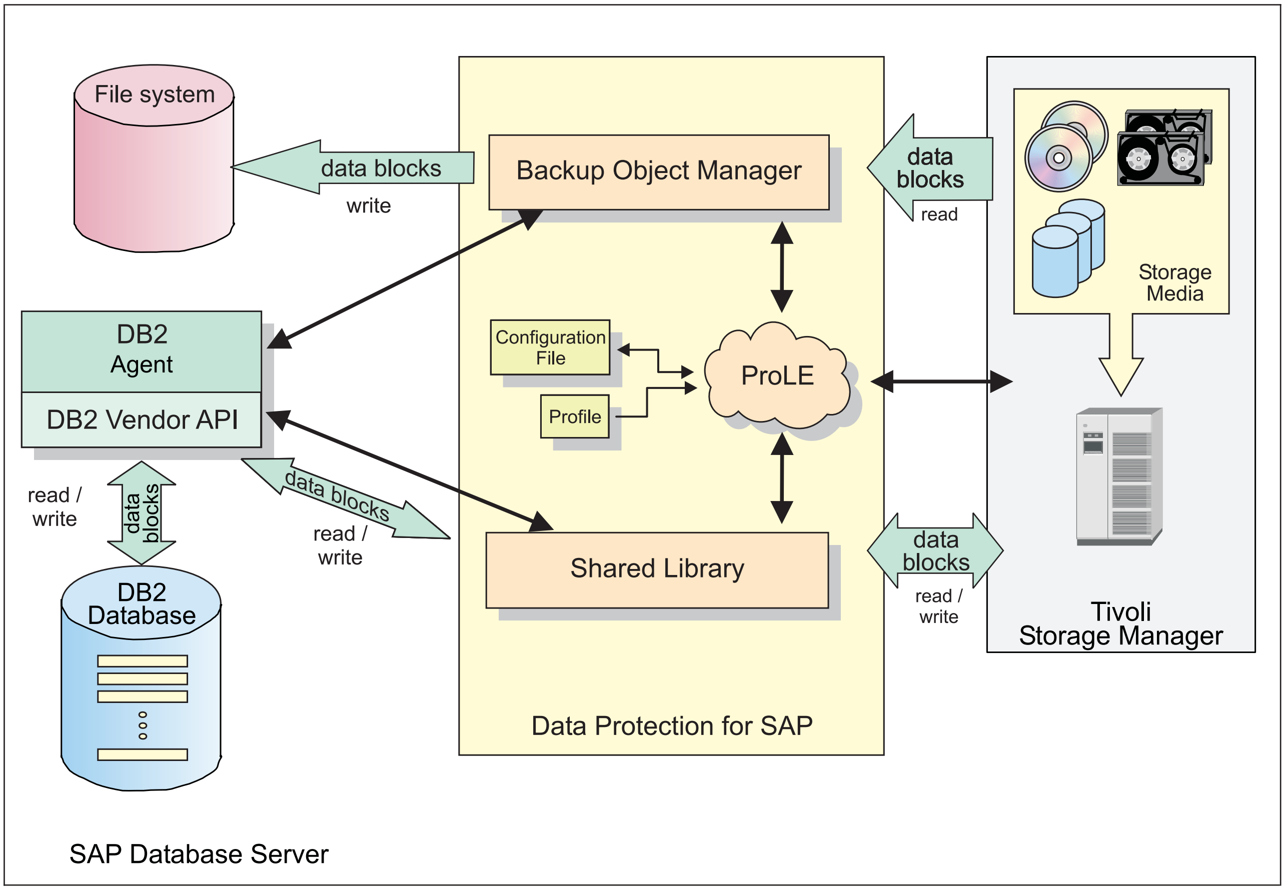


Figure 4. Data Protection for SAP Backup Object Manager

The Backup Object Manager works with database backups, DB2 log files, and raw files that might comprise any files of the file system. The tasks that can be performed with the Backup Object Manager are processed in different ways:

- Requests to verify the Tivoli Storage Manager password are passed directly to Tivoli Storage Manager.
- Requests to display or delete any data are answered by accessing the Tivoli Storage Manager server directly, thus working with the data actually available on Tivoli Storage Manager.
- Requests to restore DB2 log files and raw files are also processed using the Tivoli Storage Manager client.
- Requests to backup or restore any DB2 database data are routed to the DB2 agent. The DB2 agent employs the Data Protection for SAP shared library.

The Backup Object Manager is available for use upon successful installation and setup of Data Protection for SAP. Since the Backup Object Manager utilizes the settings in the Data Protection for SAP profile and configuration file and the settings of the XINT_PROFILE, TDP_DIR, and DB2_VENDOR_LIB environment variables, no additional installation and setup steps are required.

DB2 Log Manager

Data Protection for SAP for DB2 is integrated with the built-in DB2 Log Manager. As a result, when Data Protection for SAP is registered within the DB2 database configuration, the DB2 Log Manager uses Data Protection for SAP for archiving and retrieving log files.

Log files used in an SAP® environment are in one of these four states:

Online active
The log file is used by DB2 for current logging transactions.

Online retained
The log file is not used by DB2 for current logging transactions. However, it contains transactions with unwritten data pages. An unwritten data page is a page that has not received data from the buffer pool to disk. As a result, the log file is needed by DB2 to perform a crash recovery or roll-back operation. The DB2 Log Manager copies a filled online log file to a possible archive location. Do not use operating system commands for copying online log files.

Offline retained
The log file is not used by DB2 for current logging transactions and it does not contain transactions with unwritten data pages. In addition, it is not needed to perform a crash recovery or a roll-back operation. The log file is archived to a location specified by the database configuration. When archived successfully, DB2 deletes the log from the database log directory.

Archived
Filled or closed log files that were archived to Tivoli Storage Manager storage.

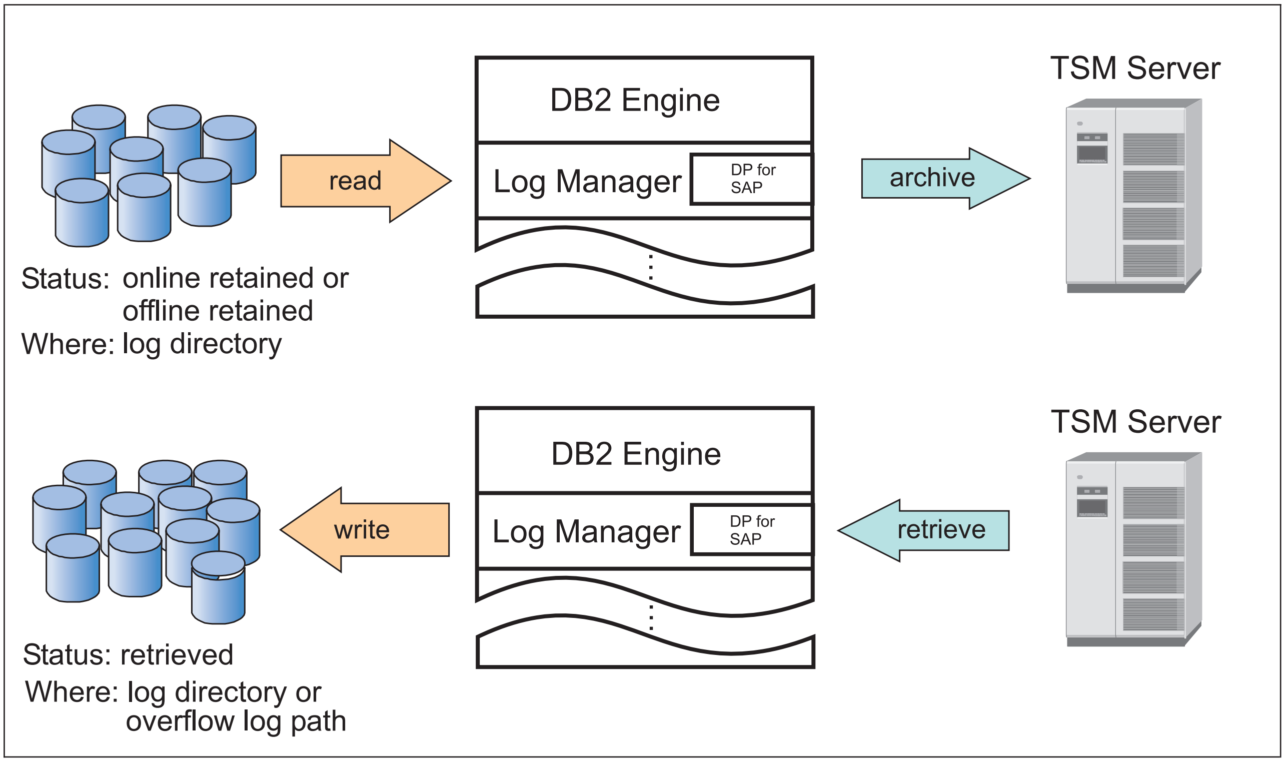


Figure 5. Log Management with DB2 Log Manager and Data Protection for SAP

Data Protection for SAP for DB2 is loaded dynamically by the DB2 Log Manager as a shared library on UNIX or Linux, , or as a dynamic link library (DLL) on Windows, and runs as part of the DB2 engine. When a log file is ready to be archived (online/offline retained), the DB2 Log Manager starts the archive process by passing the file as blocks to Data Protection for SAP. The data is then sent (by Data Protection for SAP) to Tivoli Storage Manager storage.

When a database rollforward recovery is issued, the DB2 Log Manager first checks if the corresponding log files are located either in the log path or in an overflow log path as specified in the DB2 rollforward command invocation. If the log files are not found at one of these locations, the DB2 Log Manager accesses Data Protection for SAP to determine if the log images are available on Tivoli Storage Manager. If available, Data Protection for SAP retrieves the data from Tivoli Storage Manager and sends them as blocks to the DB2 Log Manager which writes the log files to the file system. The log files are then applied to the database using DB2 processes.

Detailed information about the DB2 Log Manager is available in your DB2 *Administration Guide*.

Backup objects and types of failures

Data Protection for SAP for DB2 backs up and restores SAP® database objects only as shown in Figure 6.

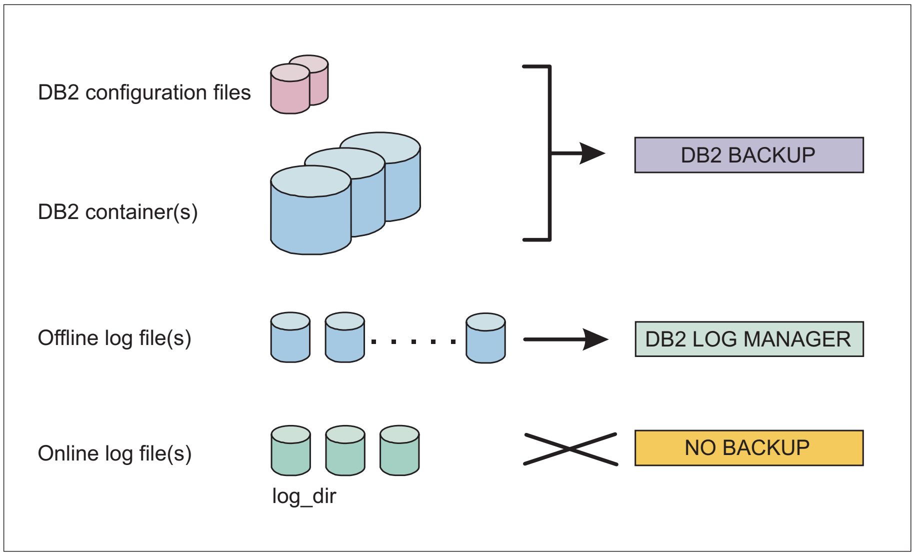


Figure 6. DB2 Backup Objects

Corrupt database
In case of a corrupted database (caused by user errors or transaction failures), the database can be restored to a specific point in time. Restoring only the database and configuration files should be sufficient for a specific point in time operation. As a result, a backup image of the database and the corresponding DB2 log files are required.

Hardware failure
In the event of a storage hardware failure, the database is typically restored to the most recent point in time. Thus, the most recent database image and DB2 log files are restored. However, the database executable files, SAP system data, and user data might also need to be restored in the event of a hardware failure. 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 database container files and offline log files that have been backed up or archived by Data Protection for SAP. See "Include/Exclude List Sample (UNIX and Linux)" on page 149 or "Include/Exclude List Sample (Windows)" on page 150 for example include-exclude lists. Example include-exclude list files are also provided in the Data Protection for SAP installation directory.

Disaster recovery
For a complete disaster recovery operation, all operating system data must be restored along with the database image, DB2 log files, database executable files, SAP system data, and user data. 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 data. Since there is no provision for backing up online DB2 log files that are required for disaster recovery, place the DB2 log directory on a mirrored disk.

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 DB2 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. 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).

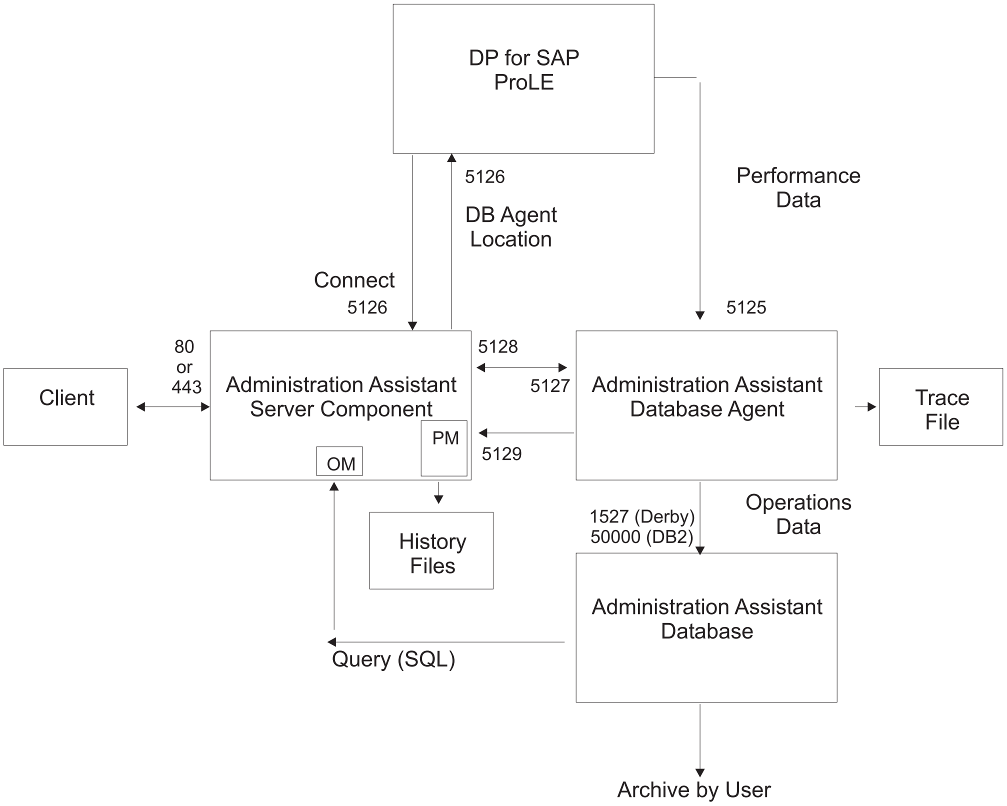


Figure 7. Administration Assistant function for Data Protection for SAP Components (with Default Port Numbers)

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 8 on page 11.

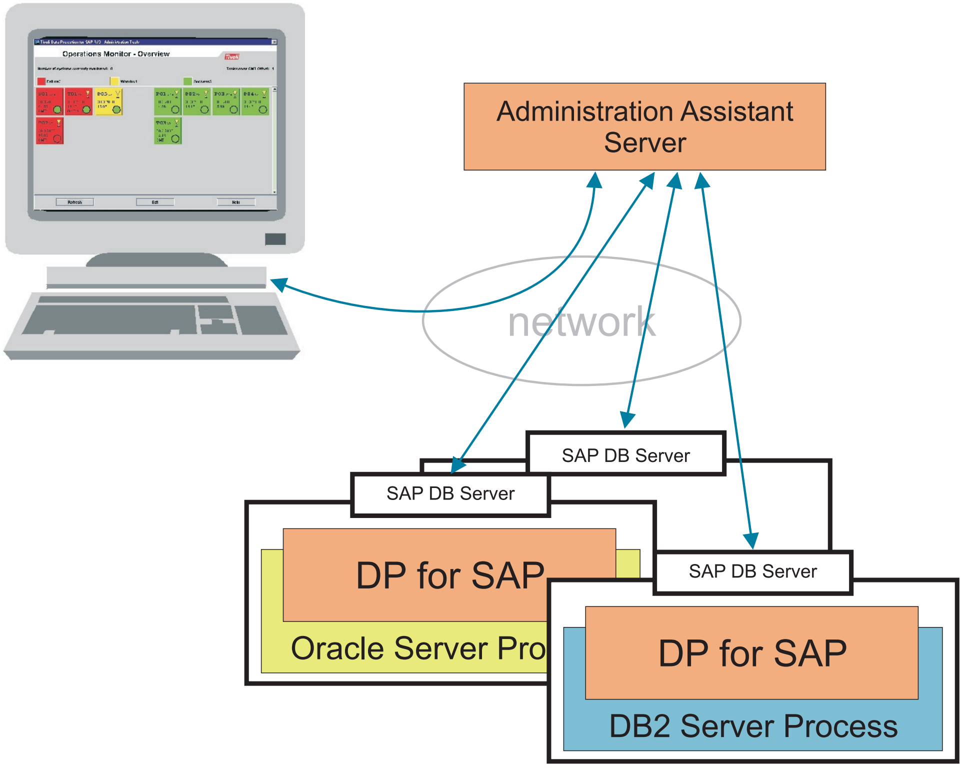


Figure 8. Example of an SAP Landscape

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 DB2 backup or restore operations is displayed. The Administration Assistant also saves this performance data and provides a graphical presentation for later analysis.

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* and *View performance data*.

Minimizing backup and restore processing with Data Protection for Snapshot Devices

Although Data Protection for SAP for DB2 provides extensive storage capabilities, business-critical databases might demand even faster recovery operations. Data Protection for SAP and the product *IBM Tivoli FlashCopy ManagerFlashCopy Manager* (formerly known as *IBM Tivoli Storage Manager for Advanced Copy Services*) provide backup and restore capabilities for the SAP® database on IBM FlashCopy® devices (such as IBM DS8000®, IBM SAN Volume Controller (SVC), and IBM XIV). These products can minimize downtime of the production systems by exploiting point-in-time copy functions exploited by these products.

Starting with DB2 9.5, DB2 offers a functionally restricted version of TSM for ACS or FlashCopy Manager known as DB2 Advanced Copy Services, which can be upgraded to an unrestricted level by installing the full FlashCopy Manager version (V2.1 or higher). In this environment, the software based on TSM for ACS is also called using the DB2 BACKUP DATABASE and RESTORE DATABASE commands, but they contain the keywords "USE SNAPSHOT" rather than the "LOAD *library*" phrase used to call the shared library for DP for SAP. "USE SNAPSHOT" causes DB2 to load and interact with the FlashCopy Manager Snapshot Backup Library.

FlashCopy Manager product information is available at this Web site: `http://www-01.ibm.com/software/tivoli/products/storage-flashcopy-mgr/`

.

Chapter 2. Planning for Data Protection for SAP for DB2 operations

Planning information regarding various component considerations is provided.

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 DB2" on page 102. 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 103.

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 the DB2 backup utility allows parallel access to tablespaces 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*. See "Archiving Inactive Data" on page 18 for additional information.

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 DB2 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 109.

Backup Server Considerations

Consider these items when setting up the Tivoli Storage Manager server. Note that Data Protection for SAP for DB2 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 18 and “Configure the Tivoli Storage Manager server” on page 58.

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' means backup of database contents, 'archive' means the backup of offline DB2 log files. Data Protection for SAP for DB2 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. A disk-tape storage hierarchy is recommended for backing up log files, each DB2 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 DB2 log 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 “Multiple DB2 Log File Copies” on page 69.

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 partial and log file backups, are automatically deleted.

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 DB2 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). 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 DB2 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. 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.

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

Planning for using IBM HACMP™ for AIX

This section provides information about Data Protection for SAP for DB2 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:

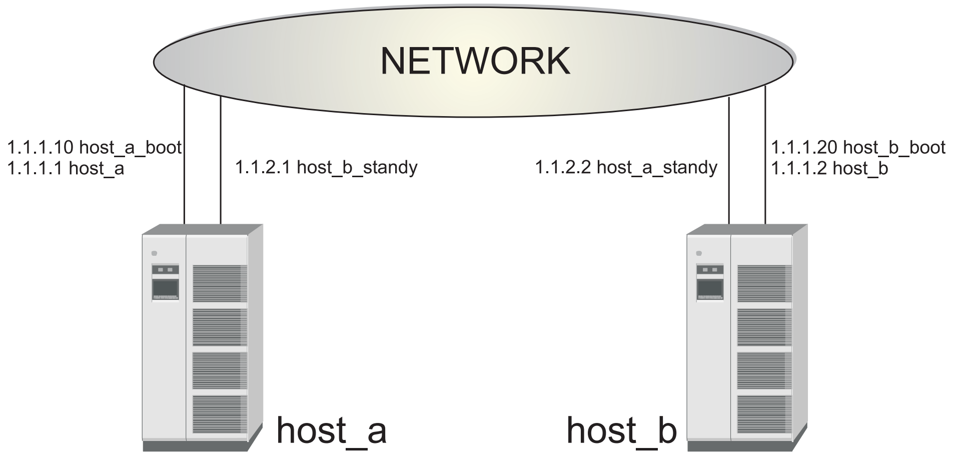


Figure 9. Sample Environment for HACMP Takeover

HACMP impact on Data Protection for SAP for DB2

A list of Data Protection for SAP for DB2 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`.
- 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`) . These files are located in a directory specified during the installation process.

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

The Data Protection for SAP dynamic library connects to `prole` using the following procedure:

- Retrieves the IP address for localhost (should be 127.0.0.1 for IPv4).
- Retrieves the `tdpr3db264` service (should be 57324).
- Connects to 127.0.0.1: `tdpr3db264` service>.

Digital Signing of Executable Files for Windows Systems

Data Protection for SAP for DB2 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-TSMERPDB2-WinIA64.exe
  - *version*-TIV-TSMERPDB2-WinX64.exe
- The Data Protection for SAP application executable files
  - backom.exe
  - createinfo.exe
  - prole.exe
  - tdpdb2.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 DB2 for V6.2

Information needed to install the various Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP for DB2 components is provided.

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

Note: 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 DB2 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 DB2 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 DB2 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 DB2 (base product) planning sheet" on page 152.
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 12.
5. Install Data Protection for SAP as described in "Installing Data Protection for SAP for DB2 on UNIX or Linux" on page 26 or "Installing Data Protection for SAP for DB2 on Windows" on page 27. See "Upgrade the Data Protection for SAP for DB2 V6.2 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 58.
7. Verify the installation completed successfully as described in "Verifying the Initial and Upgrade Installation" on page 30.

Installing the Data Protection for SAP for DB2 V6.2 base product

Information needed to install the Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP for DB2 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 DB2 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 about 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 of either upgrading from the product disc or image, or downloading the latest version from the IBM FTP server. See http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager_for_Enterprise_Resource_Planning. For the specific procedure for upgrading from an earlier version, refer to "Upgrade the Data Protection for SAP for DB2 V6.2 base product" on page 35.

These products must be installed before installing Data Protection for SAP:
- DB2
- SAP® R/3 or SAP e-business Solution, based on DB2

  The SAP Service Marketplace (http://service.sap.com/) provides current information relating 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 about configuring the Tivoli Storage Manager API client, see "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 DB2 in a Distributed File System" on page 50.

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 DB2 (base product) planning sheet" on page 152. 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 DB2 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-TSMERPDB2-platform.bin [-i console] -DRECORDFILE=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-TSMERPDB2–platform.bin -i silent -f properties file
   ```

   The *properties file* specification must contain a full path.

Sample properties file:

```
USER_INSTALL_DIR=//opt//tivoli//tsm//tdp_r3//db264
NAMEPORTAA_ADRESSE=AAServer
NAMEPORTAA_PORT=5126
RMANYES=
MANNO=
TSMUTL_SERVERADRESSE=TSMServer
TSMUTL_NODE=R3NODE
TSMUTL_BACKUPMGM=MDB
TSMUTL_ARCHIVEMGM=MLOG1 MLOG2
TSMUTL_YES=1
TSMUTL_NO=0
TSMAPI_DSMI_DIR=
TSMAPI_DSMI_CONFIG=
TSMAPI_DSMI_LOG=
TSMAPI_YES=
TSMAPI_NO=
SAP_BR_TOOL=
SAP_CFG_FILE=
TSM_CFG_FILE=
DBGSCRIPTS2=//dev//null
SID=SID
DB2_INSTANCE_NAME=DB2_INSTANCE_NAME
USER_MAGIC_FOLDER_1=//db2//DB2ERE//tdp_r3
LOGGING_NONE=0
LOGGING_LOGARCHMETH1=0
LOGGING_LOGARCHMETH2=0
LOGGING_BOTH=1
LOGGING_NR=12
```

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

Installing Data Protection for SAP for DB2 on UNIX or Linux

Data Protection for SAP for DB2 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-TSMERPDB2-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 6. File Extensions for Shared Libraries

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

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. Verify that the *DISPLAY* variable is set to view the installation prompts through a graphical X-Window.
3. Start the DB2 instance. The installation program makes the necessary updates to the DB2 configuration.
4. Invoke the Data Protection for SAP executable file and follow the installation prompts.
5. View the summary in the last page of the installation wizard. 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 the service tdpr3db264.
- Environment variable XINT_PROFILE specifies the Data Protection for SAP profile that is located in the path specified for configuration files during installation. The file name is `initSID.utl` where `SID` is the DB2 database SID specified during installation.
- Environment variable TDP_DIR points to the path where Data Protection for SAP configuration files and process logs reside. The default path is `profile path/tdplog` where `profile path` is the path specified for the Data Protection for SAP profile during installation.

- If the DB2 instance is running, the installation program sets the DB2 database configuration parameter *VENDOROPT* to the Data Protection for SAP vendor environment file. If *VENDOROPT* is already set (for example because of the installation of a previous version), the program will use its value and not set *VENDOROPT*. If DB2 log archiving is not to be managed by Data Protection for SAP, the corresponding database configuration settings are not modified. If DB2 log archiving is to be managed by Data Protection for SAP, the corresponding DB2 database configuration values are set based on the method selected during installation:

  ```
  LOGARCHMETHn  VENDOR:/path/library
  LOGARCHOPTn   /path/vendor.env
  ```

  If the DB2 instance was not running, you must complete these tasks manually, as described in “Specifying the VENDOROPT parameter” on page 44 and “Configuring the DB2 Log Manager” on page 44.

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

```
README
README_TSMERPversionlanguage.html
TIPHINTS
libtdpdb264.a (AIX)
libtdpdb264.so (Linux or Solaris)
ProLE
backom
createinfo
initSID.utl
SanFSsetupFS.sh (AIX only)
agent.lic (only after installation from disc or disc image)
```

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

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

```
initSID.utl
vendor.env
agent.lic (copy of file in installation directory)
```

Installing Data Protection for SAP for DB2 on Windows

Note: Data Protection for SAP for DB2 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-TSMERPDB2-platform
  ```

Complete 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 you want the installation program to make updates to the DB2 configuration, start the DB2 instance.
3. Invoke the Data Protection for SAP executable file, and follow the instructions of the installation dialog.
4. View the summary on the last page of installation wizard. 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 is installed and started.
- An entry is created in `%windir%\system32\drivers\etc\services` (`tdpr3db264`) .
- (Optional) The DSMI_DIR, DSMI_CONFIG, and DSMI_LOG environment variables are modified.
- The XINT_PROFILE environment variable specifies the Data Protection for SAP profile located in the path specified during installation. The file name is `initSID.utl` where *SID* is the DB2 database SID specified during installation.
- The TDP_DIR environment variable specifies the directory where Data Protection for SAP saves the configuration file and creates its process logs. Initially, this path is set to `profile path\tdplog` where <profile path> is the path for Data Protection for SAP profile specified during installation.
- If the DB2 instance is running, the installation program sets the DB2 database configuration parameter *VENDOROPT* to the Data Protection for SAP vendor environment file. If *VENDOROPT* is already set (for example because of the installation of a previous version), the program will use its value and not set *VENDOROPT*. If DB2 log archiving is not to be managed by Data Protection for SAP, the corresponding database configuration settings are not modified. If DB2 log archiving is to be managed by Data Protection for SAP, the corresponding DB2 database configuration values are set based on the method selected during installation:

  ```
  LOGARCHMETHn  VENDOR:path\tdpdb2.dll
  LOGARCHOPTn   drive:\path\vendor.env
  ```

  If the DB2 instance is not running, these tasks are not performed and must be performed manually at a later time as described in “Specifying the VENDOROPT parameter” on page 44 and “Configuring the DB2 Log Manager” on page 44.

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

```
README.txt
README_TSMERPversionlanguage.html
TIPHINTS.txt
tdpdb2.dll
ProLE.exe
backom.exe
createinfo.exe
initSID.utl
agent.lic (only after installation from disc or disc image)
```

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

These files are installed in the directory where the Data Protection for SAP profile resides:

```
initSID.utl ('SID' is replaced by the DB2 database SID provided during installation)
vendor.env
agent.lic (copy of file in installation directory)
```

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 Uniform Naming Convention (UNC) notation (\\server\path\filename). Data Protection for SAP for DB2 version 5.4 (or later) accepts UNC notation for the profile 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 DB2 under UNIX or Linux

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

1. Log in 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 DB2 is not running.
4. Invoke the uninstall executable file as shown here:

   installation path`/Uninstall_TIV-TSMERPDB2/Uninstall_TIV-TSMERPDB2`

   where `<installation path>` is the installation path documented in the summary at the end of the installation dialog. Follow the instructions of the uninstall dialog.

Uninstalling the Old Version of Data Protection for SAP for DB2 under Windows

Perform these tasks to uninstall a previous version of Data Protection for SAP for DB2 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.

Verifying the Initial and Upgrade Installation

In order to verify the installation of Data Protection for SAP for DB2, perform a full DB2 database backup and restore with the DB2 Control Center or DB2 command line processor (CLP). A complete restore or recovery of the entire SAP® database is also recommended. However, a complete offline backup should be performed first.

Installing the Administration Assistant function for Data Protection for SAP V6.2

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 V6.2 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 do not want to use the Apache Derby database already bundled with the Administration Assistant install package). 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 DB2 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 153 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 DB2 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 V6.2" 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 installing 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
Database	sdb.sh	sdb.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, up to three services are installed and automatically started. These services start the Adminstration Assistant components: `server`, `dbagent`, and `database`. The `database` component only runs if the Apache Derby database is used.
- 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
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 DB2 for V6.2

Information needed to upgrade to Tivoli Storage Manager for Enterprise Resource Planning: Data Protection for SAP for DB2 V6.2 is provided.

Perform these tasks to upgrade to Data Protection for SAP for DB2 V6.2.

Upgrade the Data Protection for SAP for DB2 V6.2 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 DB2 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. Check the readme files and release notes for incompatibilities between your installed version and the new version. Make sure that data backed up with an older version of Tivoli Data Protection for R/3 or Data Protection for SAP can still be restored with the version to be installed. For example, data that was backed up with Tivoli Data Protection for R/3 Version 3.1, 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 DB2 under UNIX or Linux” on page 29 or “Uninstalling the Old Version of Data Protection for SAP for DB2 under Windows” on page 30.
7. Install the new version of Data Protection for SAP as described in “Prerequisites” on page 24.
8. Update the Data Protection for SAP profile as described in “Migrate the Data Protection for SAP for DB2 profile” on page 36.
9. Create the configuration file(s) as described in “Creating the configuration files” on page 46.

10. Perform the necessary configuration tasks as described in “Configure the Tivoli Storage Manager client options” on page 54.
11. Verify the installation as described in “Verifying the Initial and Upgrade Installation” on page 30.
12. A full backup should be performed after upgrading to the new version.

Migrate the Data Protection for SAP for DB2 profile

The license file, the profile, and the configuration files are not deleted when Data Protection for SAP for DB2 is uninstalled. These files can be used by the new version of Data Protection for SAP. To reuse the existing configuration and connection to the Tivoli Storage Manager server, choose not to change the profile when you are prompted during installation.

Upgrade the Administration Assistant function for Data Protection for SAP V6.2

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 30. Note that the Data Protection for SAP for DB2 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 30.
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” on page 37.
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. Preparing a secure connection” on page 47.
8. Set up the Administration Assistant client as described in “2. Configuring the Administration Assistant function for Data Protection for SAP Client” on page 48.
9. Verify the installation as described in “3. Verifying the Administration Assistant function for Data Protection for SAP installation” on page 49.

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 DB2 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 DB2 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. The script guides you through the export process.

      The directory that you specify in this step is the same directory from which you can later import data to the latest version of the product during the installation process.
2. **From Administration Assistant function for Data Protection for SAP v5.5 or higher:**

   If you want to be able to access data from the currently running Administration Assistant database in a newer version of the Administration Assistant database of the same type, ensure that you do not uninstall the currently running database during the Administration Assistant uninstallation process. When you are asked which components to uninstall, specify only Administration Assistant server and Database Agent.

When you install the newer version of the Administrative Assistant database, you are asked if you want to update an existing database. If you choose this option, and are using the Apache Derby database, specify the directory that contains the existing database. (The default directory is *AA_install_dir*/aaDBSupport.) If you are using DB2, you do not need to specify an import directory.

If you want to keep performance data that is not kept in the database, back up the complete history directory, including its subdirectories, before uninstalling the old version. After installing the new version, copy the performance data into the new installation 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 box 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 DB2

Instructions about how to configure Data Protection for SAP for DB2 are provided.

Data Protection for SAP for DB2 requires certain configuration tasks to be performed for these applications:

- Data Protection for SAP base product
- Administration Assistant
- DB2 Log Manager and related DB2 files
- HACMP
- Distributed File System
- Tivoli Storage Manager backup-archive client
- Tivoli Storage Manager server

Configuration tasks for the Data Protection for SAP for DB2 base product

Instructions about how to configure the Data Protection for SAP for DB2 base product are provided.

Data Protection for SAP for DB2 requires that you complete certain configuration tasks before it performs a backup operation. Optional configuration tasks are identified in their description.

Verification tasks

Data Protection for SAP for DB2 requires these verification tasks to be performed as part of the product configuration.

Profile tasks

Data Protection for SAP for DB2 requires these tasks to be performed in the Data Protection for SAP profile as part of the product configuration.

Setting the SERVER statement in the Data Protection for SAP for DB2 profile

The SERVER statement is specified in the Data Protection for SAP for DB2 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 DB2 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 DB2 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 DB2 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
```

DB2 tasks

Data Protection for SAP for DB2 requires these DB2 tasks to be performed as part of the product configuration.

Reviewing DB2 and Data Protection for SAP for DB2 configuration guidelines

Data Protection for SAP for DB2 data transfer functions are implemented in a shared library that is accessed by DB2 whenever a backup or restore, and a log archive or log retrieve command, are issued. The shared library requires information on the path of the Data Protection for SAP profile and the path of the log files that are written by Data Protection for SAP. If an action is initiated using the DB2 commands `BACKUP DATABASE` or `RESTORE DATABASE`, the information required must be specified in a vendor environment file. The name of the vendor environment file is sent to DB2 through either the *OPTIONS* parameter of the `BACKUP DATABASE` or `RESTORE DATABASE` commands, or it can be stored persistently in the database configuration parameter *VENDOROPT* (for log archive or log retrieve, this can be stored either in the database configuration parameter *LOGARCHOPT1* or in *LOGARCHOPT2*). In the case of `BACKUP DATABASE` or `RESTORE DATABASE`, use of the `OPTIONS` keyword for this purpose is no longer necessary. It is strongly recommended that you keep the settings in the vendor environment file and in the system variables synchronised at all times. For an example of a Data Protection for SAP vendor environment file, see “Sample DB2 Vendor Environment File” on page 151. If `BACKUP DATABASE` or `RESTORE DATABASE` is triggered using the `backom` utility, the information required must be specified in the environment.

Consider these additional adjustment rules for Data Protection for SAP:

- To select a different set of Data Protection for SAP environment settings for a DB2 backup or restore, specify the full path of the vendor environment file in the *OPTIONS* parameter of the `BACKUP DATABASE` or `RESTORE DATABASE` commands. For details, refer to *DB2 Command Reference.*
- To select a different Data Protection for SAP profile, modify the environment variable *XINT_PROFILE* to denote the new profile in the vendor environment file.
- To select a different Data Protection for SAP profile for future calls to the `backom` utility, modify the environment variable *XINT_PROFILE* to denote the new profile.
- To select a different Data Protection for SAP profile for a call to the `backom` utility, specify the path of the new profile in option `–e` of the `backom` command.
- To change the path for Data Protection for SAP process log files for a call to DB2 commands `BACKUP DATABASE` or `RESTORE DATABASE`, modify the environment variable *TDP_DIR* in the vendor environment file and specify the file path in the *OPTIONS* parameter of the `BACKUP DATABASE` or `RESTORE DATABASE` commands.
- To change the path for Data Protection for SAP process log files for future calls to the `backom` utility, modify the environment variable *TDP_DIR* to denote the new profile.

Specifying the VENDOROPT parameter

In order to select a default set of Data Protection for SAP for DB2 environment settings for DB2 commands `BACKUP DATABASE`, `RESTORE DATABASE` and for the DB2 Log Manager, modify the DB2 database configuration to denote a file containing the settings:

```
db2 update db cfg for SID using LOGARCHOPT1|2 vendor environment file
```

where `<vendor environment file>` is the fully qualified path of the file containing Data Protection for SAP environment settings for DB2. Make sure that the environment settings of your system match the settings in this file.

This command can be used as an alternative to the db2set command and provides these advantages:

- There is no need to restart the DB2 instance.
- You can define default values for the OPTIONS parameter of the `BACKUP DATABASE` and `RESTORE DATABASE` commands in the DB2 configuration, thus making the OPTIONS parameter of these commands optional. (You can still override the default setting of the database configuration by specifying the OPTIONS parameter.)
- The same settings apply to database backup/restore and to log file archive/retrieve.

When using the `BACKUP DATABASE` and `RESTORE DATABASE` commands with the USE SNAPSHOT option for snapshot-based backup and restore by DB2 ACS or FlashCopy Manager, the VENDOROPT parameter is ignored. In this case, any options other than the default values must be set using the OPTIONS keyword.

Configuring the DB2 Log Manager

The following database configuration parameters are applicable to DB2 database backup and restore, and log archive and retrieve with Data Protection for SAP:

Table 8. Configuration parameters for DB2 database backup and restore, and log archive and retrieve

Parameter	**Description**	**Default**
LOGARCHMETH1	Media type of the primary destination for archived log files	Off
LOGARCHOPT1	Options field for the primary destination for archived log files (if required).	NULL
LOGARCHMETH2	Media type of the secondary destination for archived log files. If this path is specified, log files will be archived to both this destination and the destination specified by LOGARCHMETH1.	Off
LOGARCHOPT2	Options field for the secondary destination for archived log files (if required).	NULL

Table 8. Configuration parameters for DB2 database backup and restore, and log archive and retrieve (continued)

Parameter	Description	Default
FAILARCHPATH	If DB2 is unable to archive log files to both the primary and secondary (if set) archive destinations due to a media problem, then DB2 will try to archive log files to this path. This path must be a disk.	NULL
NUMARCHRETRY	Number of retries to archive a log file to the primary or secondary archive destination before trying to archive log files to a failover directory. This is only used if FAILARCHPATH is set. If NUMARCHRETRY is not set, DB2 will continuously retry archiving to the primary or secondary log archive destination.	5
ARCHRETRYDELAY	Number of seconds to wait after a failed archive attempt before trying to archive the log file again. Subsequent retries will only take affect if NUMARCHRETRY is at least set to 1.	2

To activate log archival or retrieval with the DB2 Log Manager facility, modify the DB2 database configuration during the installation. The following two changes to the database configuration are the minimum changes necessary to use the DB2 Log Manager with Data Protection for SAP:

1. Update one of the LOGARCHMETH database configuration parameters (this example uses LOGARCHMETH1):
   - (UNIX and Linux):

     ```
     db2 update db cfg for SID using LOGARCHMETH1 VENDOR:/path/shared library
     ```

   - (Windows):

     ```
     db2 update db cfg for SID using LOGARCHMETH1 VENDOR:drive:\path\tdpdb2.dll
     ```

2. Update the Data Protection for SAP environment. A file that contains the environment settings must be made available to DB2 to allow DB2 to provide this environment for Data Protection for SAP archive or retrieve requests. This file is an additional requirement. This example shows the setup needed by Data Protection for SAP for LOGARCHMETH1:
   - (UNIX and Linux):

     ```
     db2 update db cfg for SID using LOGARCHOPT1 /path/vendor.env
     ```

   - (Windows):

```
db2 update db cfg for SID using LOGARCHOPT1 drive:\path\vendor.env
```

The update to LOGARCHMETH takes effect during the next log file archive.

The database configuration parameters *LOGRETAIN* and *USEREXIT* are still available but are mapped to the parameter *LOGARCHMETH1*. For further description of the DB2 Log Manager, see the DB2 *Administration Guide*. Configure Data Protection for SAP so that at least one Tivoli Storage Manager session (one for the database backup and one for the log archives) is available for each of these operations.

Creating the configuration files

The configuration files can be created using either of the following methods:

When setting the Tivoli Storage Manager password with the backom utility, the configuration files for all DB2 partitions are automatically created in the paths `path/%DB2NODE/,` where `path` is the directory denoted by the value of keyword `CONFIG_FILE` in the profile and the string **`%DB2NODE`** is replaced automatically by a DB2 partition name referenced in the DB2 configuration file `db2nodes.cfg`. If the directory denoted by the value of keyword `CONFIG_FILE` is not located in the same network file system where the DB2 configuration file `db2nodes.cfg` is located, this procedure must be repeated for each machine where a partition of the database resides. If the database is not partitioned, `NODE0000` is used as the only DB2 partition name.

If you do not want to set the Tivoli Storage Manager password, you can manually create the required paths by performing these tasks:

1. For each database partition, create directory `path/%DB2NODE/,` where `path` is the directory denoted by the value of keyword `CONFIG_FILE` in the profile and the string **`%DB2NODE`** is replaced by one existing node (partition) found in the DB2 configuration file (`db2nodes.cfg`). The naming convention for a name to be built from the node (partition) number is a string starting with 'NODE' followed by a four digit partition number. For example, the name for partition 0 is NODE0000.
2. Copy the existing file `initSID.bki` into each of these paths. If the directory denoted by the value of keyword `CONFIG_FILE` in the profile is not located in the same network file system where file `db2nodes.cfg` is located, this procedure must be repeated for each machine where a partition of the database resides. If the database is not partitioned, `NODE0000` must be used as the only DB2 node name.

Optional: Setting backup object segmentation

Environments that contain large databases that rapidly increase in size might encounter problems when transferring data to the Tivoli Storage Manager server. For example, you might encounter the following problems when backing up or restoring large databases:

- Canceling a running backup session takes an unacceptably long time. This behavior is due to multiple internal processing activities on the Tivoli Storage Manager server.
- The recovery log for the Tivoli Storage Manager internal database might become unavailable when processing large databases. This unavailability prevents immediate access to important recovery data.

To avoid potential problems related to transferring large objects, use the Data Protection for SAP SEGMENTSIZE profile keyword. This keyword specifies the upper bound of the segments that are split from large backup objects during backup and restore processing. For more information about the SEGMENTSIZE keyword, see "Data Protection for SAP for DB2 profile parameter descriptions" on page 134.

Administration Assistant function for Data Protection for SAP tasks

Data Protection for SAP for DB2 requires these Administration Assistant function for Data Protection for SAP tasks to be performed as part of the product configuration.

1. Preparing 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. Configuring the Administration Assistant function for Data Protection for SAP Client" and "4. Configuring a scheduling client to create reports" on page 49.

2. Configuring 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 30.
- 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. Verifying 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 DB2 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 87.

4. Configuring 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 30.
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 147 or “Sample Command File for Scheduling a Report from a Windows Scheduling Client” on page 148for 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 DB2 requires these tasks to be performed to configure Data Protection for SAP in a distributed file system.

Configuring Data Protection for SAP for DB2 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 db2*SID* user ID instead of root. Perform these tasks to set up the ProLE service to run with the db2*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:

```
pd64:345:respawn:/usr/tivoli/tsm/tdp_r3/db264/prole -p profile
```

with this entry:

```
pd64:345:respawn:su - db2SID -c /usr/tivoli/tsm/tdp_r3/db264/prole -p profile
```

SID must be the actual SID.

4. Refresh the `/etc/inittab` processes.
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 DB2 in a Distributed File System in an Adaptive Computing Environment

Certain setup tasks must be performed when Data Protection for SAP for DB2 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 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/db264 /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/db264/SanFSsetupSID.sh
   ```

   The following information must be provided to the script:
   a. The SID for the SAP system to be backed up.
   b. The path for the Data Protection for SAP profile and configuration file (`init`*`SID`*`.utl`, `init`*`SID`*`.bki`).
   c. 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.

HACMP tasks

Data Protection for SAP for DB2 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 DB2 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 DB2 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.

   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 DB2 to an HACMP Resource Group:

A final step in enabling Data Protection for SAP for DB2 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 might need to ensure that any backup or restore operation in progress can be stopped.

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                                                              #
#                                                                                     #

#                                                                                     #
# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #

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


# Function to update all disk information for Data Protection for SAP

STOP_BACKUP()
{
# 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_BACKUP

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 DB2 operation are provided.

Data Protection for SAP for DB2 requires that you complete certain configuration tasks for the Tivoli Storage Manager backup-archive client and server.

Tivoli Storage Manager client tasks

Data Protection for SAP for DB2 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 DB2.

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 149. 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 DB2 database backup.
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.
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.a` that points to the `libApiDS.a` file in the Tivoli Storage Manager API installation directory (`/usr/tivoli/tsm/client/api/bin64`).

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 following is the suggested setup for Data Protection for SAP for DB2 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 DB2 database name as returned by "echo $DB2DBDFT". 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 $HOME of the DB2 instance owner as *writeable_path*.
3. Create one user options file for each DB2 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 db2*SID* or *SID*adm, or both in case of doubt.

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

- environment variable DSMI_CONFIG is exported from the login shell
- environment variable DSMI_CONFIG points to client user options file /usr/tivoli/tsm/client/api/bin64/dsm_*SID*.opt
- client user option "SERVER *servername*" in dsm_*SID*.opt points to the "SERVER *servername*" stanza in /usr/tivoli/tsm/client/api/bin64/dsm.sys
- the "SERVER *servername*" stanza contains the option "ERRORLOGName /*writeable_path*/dsierror_*SID*.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 150. 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 DB2 database backup.
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.

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 DB2 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 Fast Ethernet and Gigabit Ethernet work well with the Tivoli Storage Manager server. Fast network topologies 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.

In the AIX: LPAR environment

An LPAR 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 DB2 profile.
2. Adapt the Tivoli Storage Manager options files as described in "8. Verify the Tivoli Storage Manager server name" on page 64.
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 (containers, offline log 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 containers: `define stgpool sap_db` *`device_class_name`* `maxscr=20`
3. Define a storage pool for the offline log files: `define stgpool sap_log1` *`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 log files and copies of offlinelog files:

   ```
   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 DB2 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.

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 DB2 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:

```
backom -c password [-x]
```

(See “Password Command (Verify and Save Tivoli Storage Manager Password)” on page 129).

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

```
backom -e full path/initSID.utl
   -c password  serverA:nodeA:passwordA serverB:nodeB:passwordB [-x]
```

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 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

```
backom -c password [-x]
```

(See “Password Command (Verify and Save Tivoli Storage Manager Password)” on page 129).This method is recommended for an automated production environment.

Set the Tivoli Storage Manager password:

Data Protection for SAP for DB2 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 DB2 with the password for the Tivoli Storage Manager node by entering this command:

```
backom -c password
```

For more information on the password, refer to “7. Determine the Tivoli Storage Manager password method” on page 61.

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 9. 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	ON *n days* (see note 2)	ON *n days*
2	dsm.sys	PASSWORDACCESS PASSWORDDIR (see note 5) NODENAME	Unavailable	PROMPT Unavailable Unavailable.	GENERATE *path* *nodename*
3	Tivoli Storage Manager admin	UPDATE NODE (see notes 1, 6)	Unavailable	*password*	*password*
4	Data Protection for SAP for DB2 profile (init*SID*.utl)	For each SERVER statement specify:PASSWORDREQUIRED ADSMNODE	NO *nodename*	YES *nodename*	NO (see note 4)
6	Command line	`backom -c password`	Unavailable	*password* (see notes 3,7)	*password* (see notes 3,7

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 `SIDadm` and `db2SID` must have read and write permission for the `path` specified.
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 PASSWORDACCESS GENERATE, the operations must always be performed 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 10. 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	ON *n days* (see note 2)	ON *n days*
2	*server*.opt	PASSWORDACCESS PASSWORDDIR (see note 5) NODENAME	Unavailable	PROMPT Unavailable Unavailable	GENERATE *path* *nodename*
3	Tivoli Storage Manager admin	UPDATE NODE (see notes 1,6)	Unavailable.	*password*	*password*
5	Data Protection for SAP profile init*SID*.utl	For each SERVER statement specify:PASSWORDREQUIRED ADSMNODE	NO *nodename*	YES *nodename*	NO (see note 4)
6	Command line	`backom -c password`	Unavailable	*password* (see notes 3,7)	*password* (see notes 3,7)

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 `SIDadm` and `sapserviceSID` must have read and write permission for the `path` specified .
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 `initSID.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 `initSID.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 DB2 V6.2

Information needed to back up and restore 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 132 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.

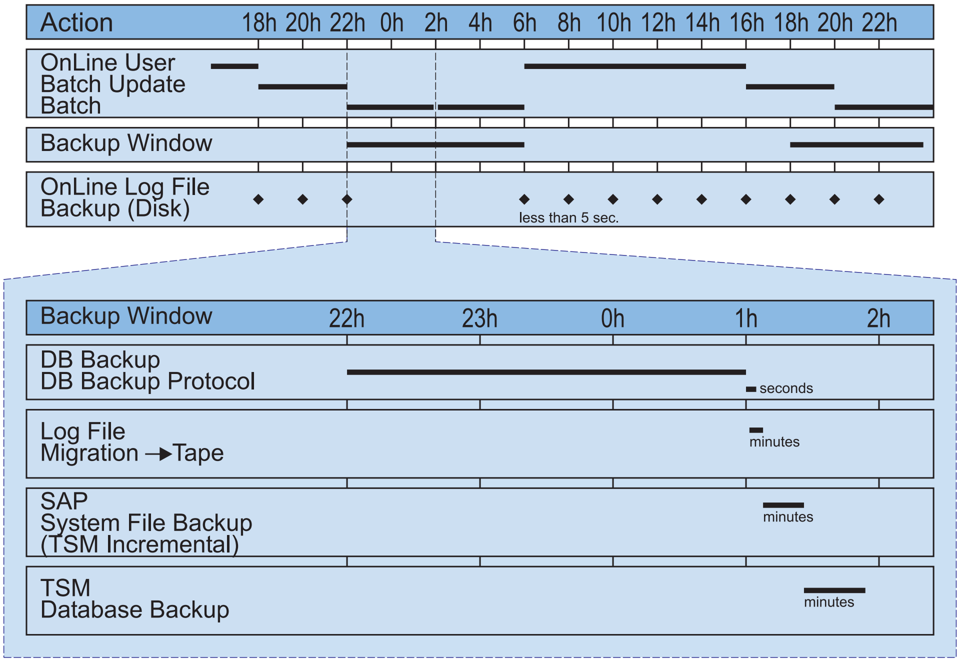


Figure 10. Production Backup Example

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 log files 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 c::\db2\C21\sapscripts\backup.cmd
```

Starting Backups in a Non-Partitioned Database Environment

The following examples show how you can start DB2 database/tablespace backups from the command line using DB2 CLP.

To start a DB2 backup or restore with Data Protection for SAP for DB2, log on as user `db2SID` or `SIDadm`. In these examples, the variable *shared library* represents the full path of the Data Protection for SAP shared library (UNIX and Linux) or DLL (Windows). DB2 database and tablespace backups are performed as follows:

- Full online backup (database parameter LOGRETAIN has to be activated):

```
db2 backup db dbname online load shared library
```

- Online tablespace backup (database parameter LOGRETAIN has to be activated):

```
db2 backup db dbname online tablespace (tablespace_name#1, ...)
        load shared library
```

Using DB2 Single System View for Backup

DB2 Version 9.5 (or later) provides the Single System View (SSV) function which allows backing up multiple database partitions at once. In earlier releases, partitioned databases needed to be backed up one partition at a time which can be time consuming and prone to errors. Backing up a partitioned database one partition at a time also failed to include the log files in the backup image. These log files are required to restore and recover the data. Restoring multiple partitions that were backed up individually is complicated as well, because the backup timestamp for each partition is slightly different. Because of this, identifying all database partitions belonging to the same backup is difficult, and determining the minimum recovery time for the backup that contains these partitions is difficult. Use of **db2_all** simplifies the backup of partitioned databases. However, backup and restore operations restrictions still exist that complicate these tasks. More information is available in “Backups and Restores in Partitioned Database Environments” on page 123.

With DB2 Version 9.5 (or later), when you perform a backup operation of a partitioned database, you can specify which partitions to include in the backup, or specify that all the database partitions should be included. The specified partitions are backed up simultaneously and the backup timestamp associated with all specified database partitions is the same. Also, by default, database logs are included in an SSV backup image. Finally, when you restore from an SSV backup image, you can specify to roll forward to end of logs, which is the minimum recovery time calculated by the database manager. See the DB2 *Command Reference* for additional information.

Multiple DB2 Log File Copies

Backing up multiple copies of a log file in a single archive operation helps protect against this data in the event of a storage hardware failure 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 for DB2 automatically switches to another copy and continues restoring the log file from that copy. The description of the profile keyword REDOLOG_COPIES on page “Data Protection for SAP for DB2 profile parameter descriptions” on page 134 provides detailed information about creating and using DB2 Log Copies.

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 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 DB2 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:\db2\C21\sqllib\scripts\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:\db2\C21\sqllib\scripts\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 DB2 backup batch file for 3264bit environments
rem -------------------------------------------------------------------------
rem Task:
rem Invokes a DB2 backup in order to perform a full offline backup of
rem all DB2 tablespaces
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 DB2 database
rem is assumed to be "C21".
rem
rem ------------------------------COMMAND------------------------------------
db2 backup db C21 load 'C:\Program Files\tivoli\tsm\tdp_r3\db264\tdpdb2.dll'
```

Full Offline Backup Shell Script Sample

```
#!/bin/ksh
# --------------------------------------------------------------------------
# backup.ksh:
# Sample DB2 backup shell script for 3264bit environments
# --------------------------------------------------------------------------
# Task:
# Invokes a DB2 backup in order to perform a full offline backup of
# all DB2 tablespaces
# --------------------------------------------------------------------------
#      *****     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 (alias) of the DB2 database is
# assumed to be 'C21'.
#
# --------------------------------COMMAND------------------------------------
su - db2c21 -c "db2 backup db C21
     load /usr/tivoli/tsm/tdp_r3/db264/libtdpdb264.a"
```

Segmenting large backup objects

To assist backing up and restoring of database objects that are larger than 1 TB, use the Data Protection for SAP *SEGMENTSIZE* keyword parameter for each DB2 backup session to be partitioned into multiple segments. These segments are stored on Tivoli Storage Manager as individual backup objects. The value of the *SEGMENTSIZE* keyword parameter determines the maximum allowable size of a backup segment on Tivoli Storage Manager storage.

Each DB2 backup session is assigned its own backup segment group. A *backup segment group* is a collection of all segments of a backup session generated by Data Protection for SAP during a database backup operation. For example, two DB2 backup sessions (`s1, s2`) that contain two segments for each session (`seg1, seg2`), is assigned two backup segment groups (`sg1, sg2`). The first backup segment group (`sg1`) contains segments `s1:seg1, s1:seg2`. The second backup segment group (`sg2`) contains segments `s2:seg1, s2:seg2`.

When you specify segmentation, the session number substring of the backup image name is used to identify the backup object as part of a segmented data stream. The session number substring *segment number* is added to the backup image name, separated by a colon (:). For example:

```
DB2 instance.db alias.type.partition number.DB2 backup ID.
session number
:segment number
```

When Data Protection for SAP initiates a change of Tivoli Storage Manager objects, the segment number (for the new backup object segment) increases by one.

For integrity check processing of the backup segment group, an additional zero-byte backup object, the so-called commit object, is generated. This will be used by Data Protection for SAP(R) to check the integrity of the related backup segment group. The naming convention of the commit object is as follows:

```
DB2 instance.db alias.type.partition number.DB2 backup ID.
session number
:Clast segment number
```

The character `C` following the colon (`:`) character identifies the backup image as a committed object. These committed objects are stored on Tivoli Storage Manager at the very end of each participating backup session. Also, the *`last segment number`* identifies the number of segments that must exist on Tivoli Storage Manager for all segments for that session to be restored. As a result, this update to the backup image name ensures that the correct object is assigned to the correct DB2 backup session. However, when one or more committed objects are missing, the integrity of the backup segment group is not guaranteed. For this reason, the database restore will not be started by Data Protection for SAP®.

You can verify whether backup object segmentation was activated by using either of these methods:

Data Protection for SAP log entries
An information message that identifies that the maximum segment size is logged to this file. The session number substring `:`*`segment number`* is included in the backup image name, as well as in an information message indicating that a commit object (containing substring C*last segment number*) was generated.

DB2 Backup Object Manager
The session number substring `:`*`segment number`* is visible in the backup image that is displayed by the `q_all -m detailed`, `q_db -m detailed` or `q_raw` command.

Administration Assistant function for Data Protection for SAP®
The session number substring (`:`*`segment number`*) is visible in the backup image that is displayed in the operations monitoring or performance monitoring views.

Segmentation and backup processing

Review the following backup characteristics before applying segmentation to your DB2 backup operations:

- The data stream sent from DB2 is segmented during a DB2 database backup.
- When implemented, segmentation is applied to every participating DB2 backup session.
- Backup and restore sessions are isolated from each other. As a result, segments that are generated by Data Protection for SAP are isolated on a per session basis. Therefore, segments cannot be mixed between different sessions. All segments backed up within the same session are restored in the same session.
- DB2 logs are not partitioned into multiple segments.

Segmentation and restore processing

Review the following restore characteristics before applying segmentation to your DB2 restore operations:

- Metadata associated with the backup object indicates whether the object is part of a segmented data stream. If the backup object is part of a segmented data stream, Data Protection for SAP automatically joins the segments to the object DB2 expects to receive from Tivoli Storage Manager during the restore operation.

- Backup and restore sessions are isolated from each other. As a result, segments that are generated by Data Protection for SAP are isolated on a per session basis. Therefore, segments cannot be mixed between different sessions. All segments backed up within the same session are restored in the same session.

Restoring SAP® data

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

Perform the tasks required for your operating system.

Starting Restores in a Non-Partitioned Database Environment

The following examples show how you can start DB2 database/tablespace restores from the command line using DB2 CLP.

Every successful backup run generates a timestamp that is required for later restore operations. These timestamps are written to the DB2 Recovery History file (RHF), which can be queried with DB2 commands. The timestamps of backup images currently stored on the Tivoli Storage Manager server can be queried using the Backup Object Manager query commands. If no timestamp is specified in a restore command, the latest backup image found on Tivoli Storage Manager will be restored. See "Managing Backup Objects" on page 125 for details.

DB2 database and tablespace restores are performed as follows:

- Full restore to a certain point in time:

  ```
  db2 restore db dbname load shared library taken at timestamp
  ```

  or

  ```
  backom -c r_db -a dbname -t timestamp
  ```

- Online tablespace restore

  ```
  db2 restore db dbname tablespace (tablespace_name#1, ...) online
        load shared library taken at timestamp
  ```

  or

  ```
  backom -c r_ts -a dbname -t timestamp -O
  ```

- Recovery History File restore

  ```
  db2 restore db dbname history file online load shared library
  ```

  or

  ```
  backom -c r_hfile -a dbname
  ```

Data Protection for SAP for DB2 process results can be checked by analyzing the Data Protection for SAP log files. These log files may contain success, warning, and error messages. Refer to "Data Protection for SAP (DB2) Messages" on page 159 for more information.

Redirected Restore in Automatic Mode

Backup Object Manager provides an automatic cloning function which creates an exact copy of the original SAP® database in a different location. The physical database layout (tablespaces, tablespace number, and size of the tablespace containers) of the target database is identical to that of the source system. The path names of the new tablespace containers are constructed by replacing the original SID with the SID of the target system. In addition, modifications to the sizes of all or selected tablespace containers of the target database can be made to optimize the I/O performance. Backup Object Manager provides automated tablespace resizing and automated tablespace normalizing for these modifications as described in "Automated Tablespace Adaptations" on page 110. The Backup Object Manager automatic mode redirected restore function can be used to resize table space containers of the source database. This is accomplished by performing a redirected restore in automatic mode with the same SID set as both the original and the target SID and requesting scaling or normalizing (or both) during the operation.

Issue this command on the target system to perform a redirected restore in automatic mode:

```
backom -c rr_db_clone -a DB2 source alias,DB2 target alias -t timestamp
```

The complete command syntax is provided in "DB2 Backup Object Manager utility" on page 4.

Backup Object Manager performs these steps during a redirected restore in automatic mode:

1. Backup Object Manager retrieves the TDI for the requested backup from Tivoli Storage Manager into memory.
2. Backup Object Manager replaces the source database alias with the target database alias. If no target database alias is specified, Backup Object Manager uses the original database alias as the target database alias.
3. Using the modified TDI, Backup Object Manager performs basic plausibility checks as described in "Redirected Restore Plausibility Checks" on page 83.
4. Backup Object Manager uses the modified TDI to create the necessary tablespace containers on the target system. If the target database alias is the same as the original database alias, the database is restored to the original database alias and SID. When restoring to the original system, Backup Object Manager attempts to overwrite the original database. Overwriting the original database requires approval by the administrator.
5. Backup Object Manager calls the DB2 redirected restore function.

Tablespace Definition Information (TDI)

In order to automate a redirected restore as much as possible, Backup Object Manager requires information on the tablespaces and the tablespace containers used in the original database. This information is used to create the tablespace containers of the target database accordingly. This information is required for each tablespace:

- The ID and name of the tablespace.
- The type of the tablespace. For example, whether the tablespace is system (SMS) or database managed (DMS).
- The page size in bytes.
- The extent size in pages.
- The number of pages used. This number can help the administrator when resizing containers. Backup Object Manager also calculates the numbers of total pages and of usable pages from the data stored for each tablepspace container.

  Is automatic storage used?
- Information on the tablespace containers used for the tablespace.

This information must be available for each tablespace container:

- The ID of the tablespace container.
- The name of the tablespace container. For example, whether the directory contains an SMS container or the file contains a DMS container, respectively.
- The type of the tablespace container. For example, whether a database managed container is stored in a file or on a raw device.
- For DMS tablespaces, the total number of pages stored in the container.

The TDI and the DB2 backup images are stored together on the Tivoli Storage Manager server. They are associated using the combination of the instance name of the database, the database alias, the database node number, and the timestamp of the backup. The name of the TDI is constructed in this format: *`DB2 instance`*`-<DB2 alias>-`*`DB2 node numbertimestamp`*`.tdi`. The TDI can be retrieved from Tivoli Storage Manager separately with the Backup Object Manager command `'r_tdi'` and can be stored as an ASCII file in a specified file system. The availability of TDI in the filesystem is a prerequiste for the Backup Object Manager redirected restore in batch mode.

These changes can be done to the TDI file to prepare for a batch-mode redirected restore:

- add or remove of tablespace containers from dedicated tablespaces
- modify names (locations) of tablespace containers
- modify the size of a DMS tablespace container, whereby the sum of container sizes has to have at least the number of pages used plus `((number of containers + 1) * extent)`, where `extent` is the extent size in pages.
- add an automatic storage path, if at least one automatic storage path is already present
- change the location of an existing automatic storage path
- remove one or more existing automatic storage paths, whereby in any case at least one automatic storage path needs to exist

```
tablespace
```

The following is a sample TDI file:

```
;    IBM Tivoli Storage Manager for Enterprise Resource Planning
;                    Data Protection for SAP(R) for DB2
;                - Tablespace Definition Information (TDI) -
;
; The following TDI sections can be modified manually:
;  - Automatic_Storage_Path
;  - Container
;
; An automatic storage path section consists of the following format:
;
;  Automatic_Storage_Path = path#1
;  ...
;  Automatic_Storage_Path = path#n
;
; It is possible to add or remove an automatic storage path entry. For already existing
; automatic storage path entries the assigned path can be updated.
;
; A tablespace section consists of the following format:
;
;  [Tablespace ID "tbsp. name" type page size extent size in pages
;                                                     used pages yes|no]
;  Container[ID 1] = definition ;
   . . .
;  Container[ID n] = definition
;
; where the definition of a container statement is characterized by its tablespace:
; - SMS tablespace: "path"
; - DMS tablespace: file | "path/container name" | size in pages
;
; If the tablespace containers are modified manually (add or remove container,
; adjust container path or size) at least the following conditions have to be
; guaranteed for ensuring the TDI integrity:
; 1) Any new container specified requires empty brackets '[]'. The ID is calculated
;    internally.
;
; 2) Each tablespace block has to have at least one container specification
;
; 3) The sum of container sizes of a DMS tablespace has to have at least the number
;    of used pages plus ((number of containers + 1) * extent).
;
; !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
; ! DO NOT EDIT ANYTHING ELSE EXCEPT THE SECTIONS !
; !      - Automatic_Storage_Path (if present)    !
; !      - Container                              !
; !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[TDI]
Version = 1.1
Generator = Data Protection for SAP(R) 6100

[Backup]
Alias = T01
Instance = db2t01
Node = 0
Timestamp = 20081130094352
Database_Path = /db2/T01/sapdata1/db2t01/NODE0000/SQL00001/
Automatic_Storage_Path = /db2/T01/sapdata1
Automatic_Storage_Path = /db2/T01/sapdata2

[Tablespace 0 "SYSCATSPACE" dms 16384 4 9264 yes]
Container[0] = file | "/db2/T01/sapdata1/db2t01/NODE0000/T01/T0000000/C0000000.CAT" | 8192
Container[1] = file | "/db2/T01/sapdata2/db2t01/NODE0000/T01/T0000000/C0000001.CAT" | 8192

[Tablespace 1 "TEMPSPACE1" sms 16384 32 1 no]
Container[0] = "/db2/T01/saptemp1"

[Tablespace 10 "T01#USER1D" dms 16384 2 540 no]
Container[0] = file | "/db2/T01/sapdata1/NODE0000/T01#USER1D.container000" | 448
Container[1] = file | "/db2/T01/sapdata2/NODE0000/T01#USER1D.container001" | 448

[Tablespace 11 "T01#USER1I" dms 16384 2 540 no]
Container[0] = file | "/db2/T01/sapdata1/NODE0000/T01#USER1I.container000" | 448
Container[1] = file | "/db2/T01/sapdata2/NODE0000/T01#USER1I.container001" | 448
```

Be aware of the following considerations regarding the TDI file:

- The "[TDI]" header block is used to identify the data as TDI and holds some meta-information about it. The "Version" key holds the version of the TDI syntax. The "Generator" key denotes some product information.
- The [Backup] block holds various kinds of information about the database backup the TDI is associated with. This information must be kept within the TDI file so that it is available even when the file has been renamed.

  [Backup] additionally includes the database path where database meta data is stored as well as all automatic storage paths the database provides for tablespaces supporting automatic storage. It is possible to add or remove an automatic storage path entry in that section. Optionally, for already existing automatic storage path entries the assigned path can be updated.
- The [Tablespace] block marks the start of the container definitions of a specific tablespace.
- The block header contains the following items in exactly this order: the ID of the tablespace, its name, its type, the page size in bytes, the extent size in pages and the number of used pages in the tablespace. Do not change any data within the tablespace block header.
- Each container statement defines one container of a tablespace according to the following rules:
  - The ID is denoted in square brackets if the line was written by the system. If a new container is to be added to a tablespace, the ID is not yet known. Therefore, the administrator specifies a new container without an ID, just entering consecutive brackets.
  - For an SMS tablespace, only the fully qualified path is specified.
  - For a DMS tablespace, the type, location and size of the container are specified, in this order, and separated by a vertical bar ("|"). The type is given by one of the strings "file" or "device". The size will be interpreted as a number of pages unless a unit is specified. In this case, the unit is used.
  - Names of tablespaces and paths must be quoted strings.

Redirected Restore in Batch Mode

Backup Object Manager provides a redirected restore batch mode function where the TDI for the target database is modified before starting the redirected restore. The TDI image to be used must be available as an ASCII file in the file system. For example, a TDI image created during an interactive redirected restore can be used as target TDI for a redirected restore in batch mode. Batch mode can also be used for multiple redirected restores to different locations with identical changes of the physical database structure. As with the interactive mode, the original TDI is used to test whether the changes of tablespace container sizes and locations made are valid. In addition, modifications to the sizes of all or selected tablespace containers of the target database can be made to optimize the I/O performance. Backup Object Manager provides automated tablespace resizing and automated tablespace normalizing for these modifications as described in “Automated Tablespace Adaptations” on page 110. A sample TDI file and modification guidelines are available in “Tablespace Definition Information (TDI)” on page 75.

Before beginning a redirected restore in batch mode, the TDI for the target database must be available. This is accomplished by providing the target TDI image of a previous interactive redirected restore as a file in the file system or by retrieving the original TDI from Tivoli Storage Manager. Issue the following command to retrieve a TDI image from Tivoli Storage Manager into the file system:

```
backom -c r_tdi -a DB2 source alias -t timestamp -d target directory of TDI
```

This original TDI image can be renamed and modified. The complete command syntax is provided in "DB2 Backup Object Manager utility" on page 4.

Issue the following command on the target system to perform a redirected restore in batch mode:

```
backom -c rr_db_batch -a DB2 source alias,DB2 target alias -t <timestamp,...
...-f full qualified path and name of target TDI file
```

Backup Object Manager performs these steps during a redirected restore in batch mode:

1. Backup Object Manager replaces the alias specified in the target TDI file with the alias of the target database. If no target database alias is specified, Backup Object Manager uses the original database alias as the target database alias.
2. Backup Object Manager retrieves the original TDI from Tivoli Storage Manager and verifies whether the target TDI defines tablespace containers that are sufficient to replace the original tablespace containers.
3. Backup Object Manager uses the target TDI and the original TDI, to perform basic plausibility checks as described in "Redirected Restore Plausibility Checks" on page 83.
4. Backup Object Manager uses the target TDI to create the necessary tablespace containers on the target system. If the target database alias is the same as the original database alias, the database is restored to the original database alias and SID. When restoring to the original system, Backup Object Manager attempts to overwrite the original database. Overwriting the original database requires approval by the administrator.
5. Backup Object Manager calls the DB2 redirected restore function.

Redirected Restore in Interactive Mode

Backup Object Manager interactive mode is a menu-driven dialog where the table space container layout is redefined by adding, deleting, moving, or resizing items. Backup Object Manager compares the tablespace definitions entered in the menu dialog with the original database layout (as documented in the original TDI) and provides immediate feedback regarding potential configuration problems. In addition, modifications to the sizes of all or selected tablespace containers of the target database can be made to optimize the I/O performance. Backup Object Manager provides automated tablespace resizing and automated tablespace normalizing for these modifications as described in "Automated Tablespace Adaptations" on page 110.

Issue this command on the target system to perform a redirected restore in interactive mode:

```
backom -c rr_db_interactive -a DB2 source alias,DB2 target alias...
...-t timestamp -f target TDI file
```

The complete command syntax is provided in "DB2 Backup Object Manager utility" on page 4.

Backup Object Manager performs these steps during a redirected restore in interactive mode:

1. Backup Object Manager retrieves the TDI for the requested backup from Tivoli Storage Manager into memory.
2. Backup Object Manager replaces the source database alias with the target database alias. If no target database alias is specified, Backup Object Manager uses the original database alias as the target database alias.
3. Backup Object Manager determines if specific containers need to be redefined.
4. Backup Object Manager displays the main menu which show a list of sorted tablespaces for the database to be restored. A '!' mark in front of a tablespace or tablespace container indicates a warning regarding a potential problem. Although the redirected restore can still begin, the problem should be resolved before proceeding. A '!!' character in front of a tablespace or tablespace container indicates an error was detected, such as a problem concerning their location or size. The redirected restore will not succeed until the error is first resolved.
5. The administrator can select tablespaces or tablespace containers to be changed by using their IDs. When all modifications of the physical database layout are completed and no more errors ('!!') are displayed, the redirected restore can be started by entering 'c' from the main menu. The administrator can also end the redirected restore from any menu dialog by entering 'a'.
6. When the -f option is specified during the redirected restore, the modified physical database layout of the target database is stored in an ASCII file in the file system. This file can be used afterwards as input for a redirected restore in batch mode at another location, where the same physical changes to the restored database must be applied.
7. Backup Object Manager uses the modified TDI and the original TDI to perform basic plausibility checks as described in "Redirected Restore Plausibility Checks" on page 83.
8. Backup Object Manager uses the modified TDI to create the necessary tablespace containers on the target system. If the target database alias is the same as the original database alias, the database is restored to the original database alias and SID. When restoring to the original system, Backup Object Manager attempts to overwrite the original database. Overwriting the original database requires approval by the administrator.
9. Backup Object Manager calls the DB2 redirected restore function.

Sample Work Flow for Redirected Restore

This is a sample work flow for a redirected restore with Data Protection for SAP for DB2 Backup Object Manager. In order to clone the SAP® production database (PRD) to a test system (TST) on a different machine, apply the following procedure:

1. Make sure that the administrator account to be used has the appropriate rights on the target system, such as permission to allocate files of a size greater than 2 GB.
2. Verify that the source database PRD meets the prerequisites for a redirected restore operation as identified in "Redirected Restore Prerequisites" on page 86.
3. Set up Data Protection for SAP for DB2 on the target machine. Verify that these environment variables specify these values:
   - XINT_PROFILE specifies the Data Protection for SAP profile.

- DB2_VENDOR_LIB specifies the Data Protection for SAP shared library.
- TDP_DIR specifies the path for the Data Protection for SAP process log files.

4. For the restore process, customize the Data Protection for SAP profile (initTST.utl) on the test system with these settings:
   - Use BACKUPIDPREFIX as specified on the source system: PRD___.
   - Use the Tivoli Storage Manager server specified on the source system. This may include adding the appropriate Tivoli Storage Manager server stanza to the client system options file (`dsm.sys`) on the test system.
   - Use the ADSMNODE specified on the source system.
   - Use BRBACKUPMGTCLASS as specified on the source system.
5. Issue the following command to record the password of the appropriate node on the Tivoli Storage Manager server:

   ```
   backom -c password
   ```

   This creates or updates the Data Protection for SAP configuration file `initTST.bki`.
6. Issue the following command to check the Data Protection for SAP database backup images on Tivoli Storage Manager:

   ```
   backom -c q_db
   ```

   Verify that the TDI flag is set to yes for the backup image to be restored. Information regarding how to create Tablespace Definition Information is provided in “Create Tablespace Definition Information” on page 85.
7. Issue the following command with the -C option to call the BackOM built-in check routine:

   ```
   backom -c rr_db_clone -a PRD,TST -t timestamp -C
   ```

   This checks for logical and physical integrity of the test system.
8. Issue the following command to start the redirected restore:

   ```
   backom -c rr_db_clone -a PRD,TST -t timestamp
   ```

9. If the database is in rollforward pending mode and needs to be recovered, there are two possibilities for retrieving the required logs.
   - automatically by the DB2 Log Manager during the recovery process, or
   - manually with BackOM before the DB2 rollforward process is started.

   The automatic log file retrieval requires some extra configuration parameters to enable Data Protection for SAP to find the logs on the TSM server, because the logs were archived under a different database name (the source database) but the rollforward process tries to find them based on the target database name. Therefore, two additional Data Protection for SAP configuration parameters help to find and retrieve the required logs.

   The configuration parameters are:
   - SRC_DB_INSTANCE
   - SRC_DB_ALIAS

where SRC_DB_INSTANCE specifies the name of the DB2 instance of the source database and SRC_DB_ALIAS the name of the source database itself. These two parameters must be added to the DB2 vendor environment file, which will be used as the option (DB2 database configuration parameter LOGARCHOPT1 or LOGARCHOPT2) for the appropriate activated DB2 log archive method, for example:

```
XINT_PROFILE=/db2/TST/tdpr3/initTST.utl
TDP_DIR=/db2/TST/tdpr3/tdplog
BACKOM_LOCATION=/usr/tivoli/tsm/tdp_r3/db264/backom
SRC_DB_INSTANCE=DB2PRD
SRC_DB_ALIAS=PRD
```

Activate the DB2 Log Manager on the test system (if not already done) in combination with Data Protection for SAP (here, log archive method 1 is used to service log requests):

```
db2 update db cfg for TST using LOGARCHMETH1 VENDOR:/<fully qualified name
          of shared library>
```

Set LOGARCHOPT1 to the modified DB2 vendor environment file (vendor.env) created during the Data Protection for SAP installation:

```
db2 update db cfg for TST using LOGARCHOPT1 <fully qualified name of
         DB2 vendor environment file>
```

The logs required for the database recovery can be either retrieved automatically, which required the Data Protection for SAP® parameters SRC_DB_INSTANCE and SRC_DB_ALIAS set in the DB2 vendor environment file or they can be retrieved manually with BackOM. In the latter case, the TSM server must first be checked for the logs already archived, where logs of a database will be lgrouped by their associated log chain number. Issue the following command:

```
backom -c q_log -a PRD
```

10. In order to retrieve the log files, issue:

```
backom -c r_log -a PRD -l log number range -k log chain number
             -d destination directory
```

The database log directory or a different location may be specified for the destination directory.

11. Start the DB2 rollforward process. In case the log files were retrieved manually by BackOM to a location other than the database log directory, start the DB2 rollforward procedure and use the overflow log path option to specify the location of the retrieved log files.
12. After the redirected restore completes successfully and before backing up the new test system, modify the Data Protection for SAP profile `initTST.utl` to match the values of the new test system. This modification might involve these keywords:
    - BACKUPIDPREFIX
    - SERVER
    - ADSMNODE

   - BRBACKUPMGTCLASS
   - BRARCHIVEMGTCLASS

   If the DB2 vendor environment file was updated using the parameters SRC_DB_INSTANCE and SRC_DB_ALIAS for recovery purposes, remove those parameters from that file.

   Attention: Be sure not to back up the test system with the BACKUPIDPREFIX of the production system.

13. Perform the following tasks to update the DB2 database configuration of the test system:
   - Set VENDOROPT to the vendor environment file created during the Data Protection for SAP installation.

     ```
     db2 update db cfg for TST using VENDOROPT
      fully qualified name of DB2 vendor environment file
     ```

   - If the DB2 Log Manager is used in combination with Data Protection for SAP and is not yet configured, set the appropriate log archive method and its assigned option field in the database configuration as follows::

     ```
     db2 update db cfg for TST using LOGARCHMETH1 VENDOR:
        fully qualified name of shared library
     db2 update db cfg for TST using LOGARCHOPT1
        fully qualified name of DB2 vendor environment file
     ```

Redirected Restore Plausibility Checks

Regardless of the mode of the redirected restore operation (automatic, interactive, batch), Backup Object Manager performs these checks before the DB2 redirected restore operation begins:

- All paths of tablespace containers must be fully qualified.
- On Windows, all drives used for storing tablespace containers must be available.
- On UNIX or Linux, the volumes used for storing tablespace containers must be available.
- There must be sufficient space in the various locations of the tablespace containers in the target system for storing them.
- Backup Object Manager tests whether there exist other files or directories at the desired locations of the tablespace containers. A warning is issued when a directory for an SMS container already exists but is not attached to a different database. An error is issued when one of these situations is detected:
  - A directory for an SMS container already exists and is attached to a different database.
  - A file for a DMS container already exists in the target location.
- The tablespace containers must be provide sufficient storage space for the restored data.

For all modes of redirected restore, Backup Object Manager provides a test-only option that performs validation checking without actually starting a restore. This option is used to determine in advance whether a specific redirected restore will succeed. The Backup Object Manager test-only option is activated by adding the command option -C to a redirected restore command. For example, issue this command to test whether a redirected restore in batch mode will succeed with the provided target TDI file:

```
backom -c rr_db_batch -a DB2 source alias,DB2 target alias -t timestamp...
...-f full qualified path and name of target TDI file -C
```

If the test determines that the redirected restore will not succeed, check the Backup Object Manager log for error and warning messages.

DB2 Redirected Restore Using Backup Object Manager

The DB2 Backup Object Manager provides redirected restore functions such as these:

- Restore a DB2 database to a different location.
- Change the physical database layout of a restored database, including the location of tablespace containers, the number of tablespace containers, their names, and their sizes.
- Clone a database, changing both the name and the location of the database.

Backup Object Manager uses a simple set of commands to perform a redirected restore of a database and also performs some plausibility checks before actually starting the operation.

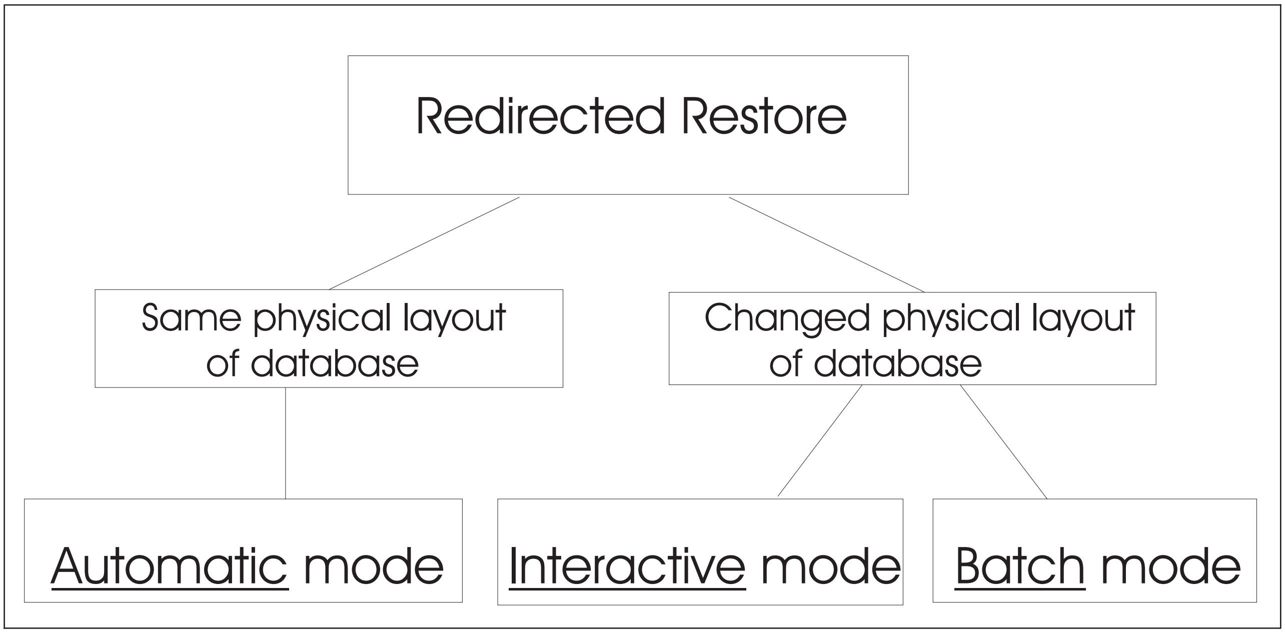

Redirected Restore
Same physical layout of database
Changed physical layout of database
Automatic mode
Interactive mode
Batch mode

Figure 11. Redirected Restore Overview

Backup Object Manager provides these redirected restore modes:

Automatic
Restore a database to a different name and location while keeping the general database layout. However, scaling and normalizing of tablespace containers can be requested with an automatic redirected restore.

Batch Restore a database to a different location and database layout that is defined in a configuration file.

Interactive
Restore a database to a location and database layout specified by the administrator in a dialog.

In all modes, Backup Object Manager can also perform additional automated adaptations to tablespaces. For example, perform tablespace scaling to provide tablespaces with appropriate free space or perform tablespace normalizing to optimize the parallel I/O performance of the restored database.

Create Tablespace Definition Information

A TDI image is created after a full database backup completes successfully and is stored on the Tivoli Storage Manager server with the database backup image. Only database backups for which a corresponding TDI is available can be used for redirected restore with Backup Object Manager.

The Backup Object Manager must be used in order to create a TDI for an offline database backup image. For example, this command starts an offline database backup using two sessions:

```
backom -c b_db -a database alias -S 2
```

A TDI is not created when using the DB2 command line interface to perform an offline database backup.

There are two methods available to create a TDI for an online database backup image:

- One method is to use the Backup Object Manager backup function. For example, this command starts an online database backup using two sessions:

  ```
  backom -c b_db -a database alias -S 2 -O
  ```

- Another method is to use the DB2 command line interface to start an online backup with the BACKOM_LOCATION parameter set in the vendor environment file. When the value of this parameter specifies the `backom` executable, the TDI is stored on the Tivoli Storage Manager server after the backup completes successfully. This statement must be included in the DB2 vendor environment file:

  ```
  BACKOM_LOCATION=fully qualified path and name of the backom executable
  ```

  The DB2 backup command can then be issued on the DB2 command line interface:

  ```
  db2 backup db database alias online load shared library open 2 sessions
  ```

Use the Backup Object Manager query function to verify whether a TDI image is available for a Data Protection for SAP for DB2 backup image.

Redirected Restore Prerequisites

These requirements must be met in order for the Backup Object Manager to successfully perform a redirected restore:

- A TDI image must be available for the backup to be restored.
- The database must not have a tablespace container that is a raw device.
- DMS tablespace containers of the original system are available in these locations:
  - UNIX or Linux:`/db2/SAPSID/sapdatan`
  - Windows: `drive:\db2\SAPSID\sapdatan` (*n* is an integer)
- *SAPSID* must be the database alias (*SAPSID*) and must consist of all upper case characters or digits
- SMS tablespace containers of the original system are available in these locations:
  - UNIX or Linux: `/db2/SAPSID/...`
  - Windows: `drive:\db2\SAPSID\...`

Tablespace Definition Information

In order to perform a redirected restore, Backup Object Manager requires information about the physical layout of the original database, such as the tablespace containers used by the original database. In particular, the size of database managed containers (DMS) must be available in order to create new tablespace containers with sufficient space. Backup Object Manager keeps information on all tablespaces of a database backed up for every backup image on Tivoli Storage Manager. The following information is collected for each tablespace:

- The ID and name of the tablespace.
- Whether the tablespace type is system (SMS) or database managed (DMS).
- Whether the tablespace is managed by automatic storage.
- The page size in bytes.
- The extent size in pages.
- The number of pages used.
- The tablespace containers used for the tablespace:
  - The ID of the tablespace container.
  - The name of the tablespace container (the directory containing an SMS container or the file containing a DMS container, respectively).
  - Whether the tablespace container type is a database managed container stored in a file or on a raw device.
  - For DMS tablespaces, the total number of pages stored in the container.

This information about the physical database layout is referred to as the Tablespace Definition Information (TDI) and is stored along with the production data. The TDI is required for Backup Object Manager redirected restore operations. A TDI image is identified with its corresponding DB2 backup by the combination of DB2 instance name, database alias, database node number, and the timestamp of the backup as shown here:

```
DB2 instance-DB2 alias-DB2 node number-timestamp.tdi
```

The TDI is stored in ASCII format to allow for read and edit usability. For example, the number of used pages recorded in the TDI image can help identify the correct sizes to request when resizing containers as described in “Automated Tablespace Adaptations” on page 110. Backup Object Manager also calculates the number of total pages and used pages from the data stored for each tablespace container. Editing may be necessary when requesting a redirected restore in batch mode, as described in “Redirected Restore in Batch Mode” on page 78. A sample TDI file is provided in “Tablespace Definition Information (TDI)” on page 75.

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 DB2

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 tdpr3db264 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 DB2 (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 tdpr3db264  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. Configuring a scheduling client to create reports" on page 49.

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. Configuring a scheduling client to create reports" on page 49. 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 DB2 built-in utilities or commands 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.

Chapter 7. Performance tuning for Data Protection for SAP for DB2

Information needed to fine-tune Data Protection for SAP for DB2 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.

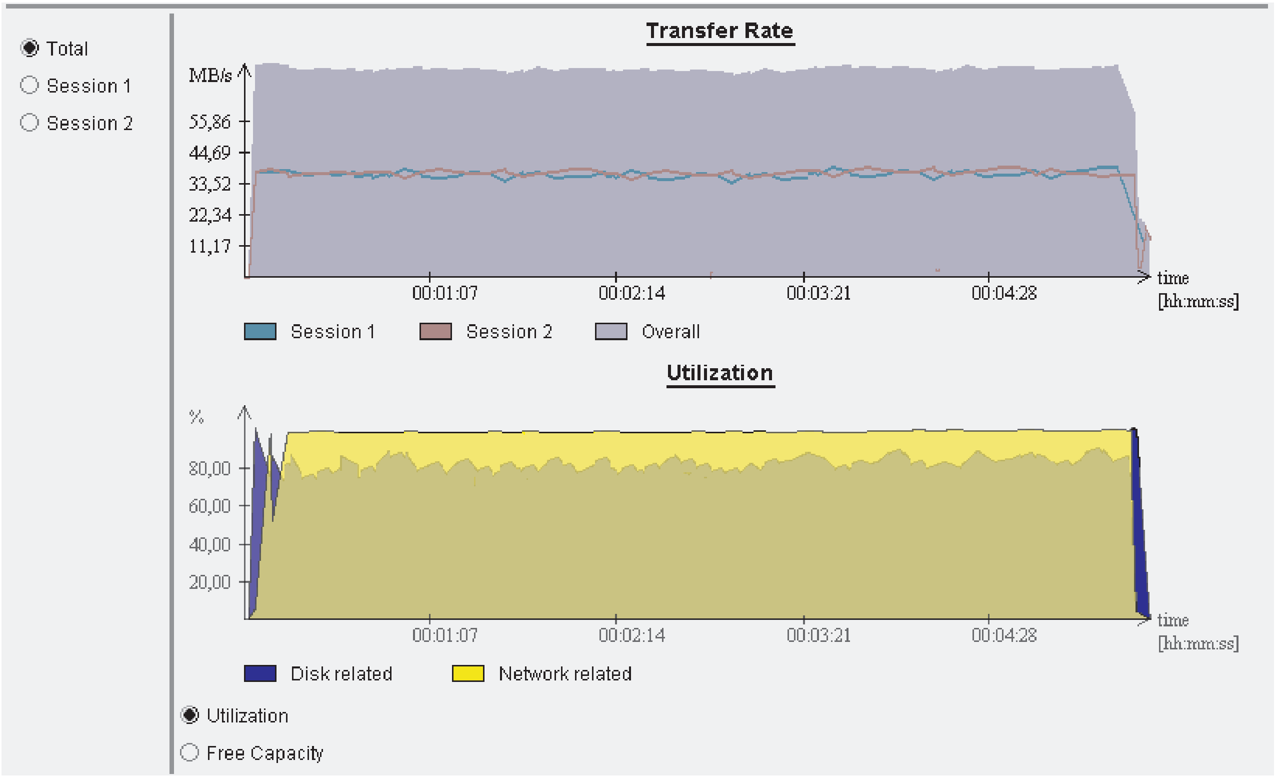


Figure 12. Indicating a Balanced Configuration

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

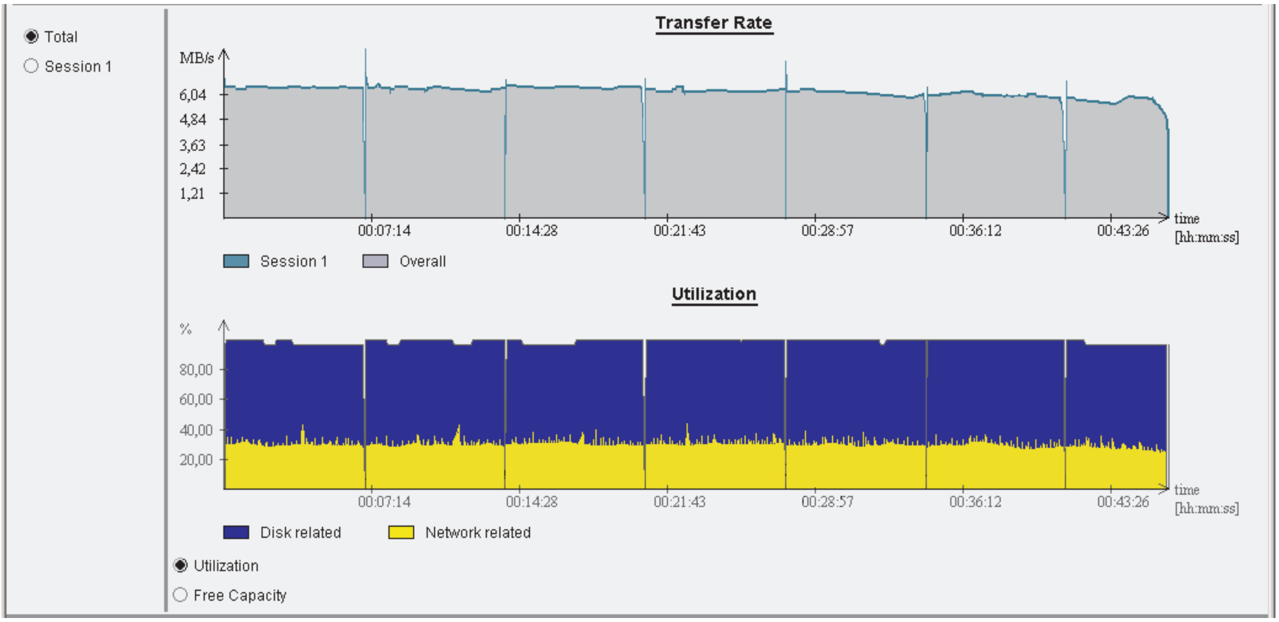


Figure 13. Indicating a Disk Bottleneck

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.

Example of a network or Tivoli Storage Manager bottleneck

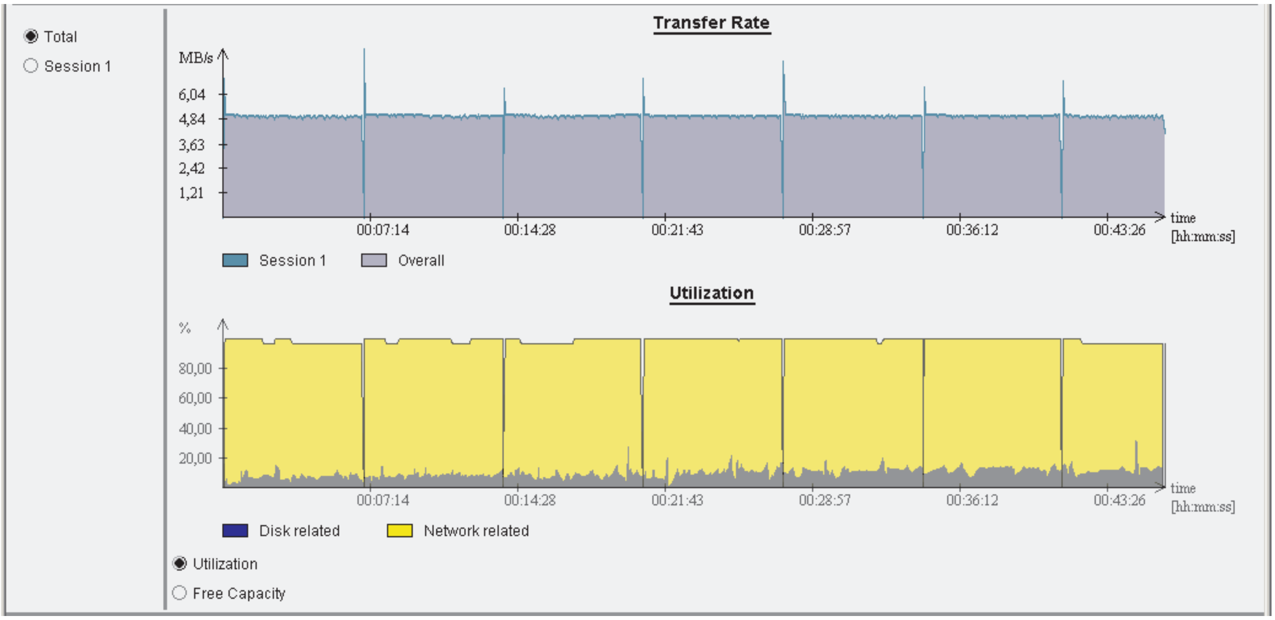


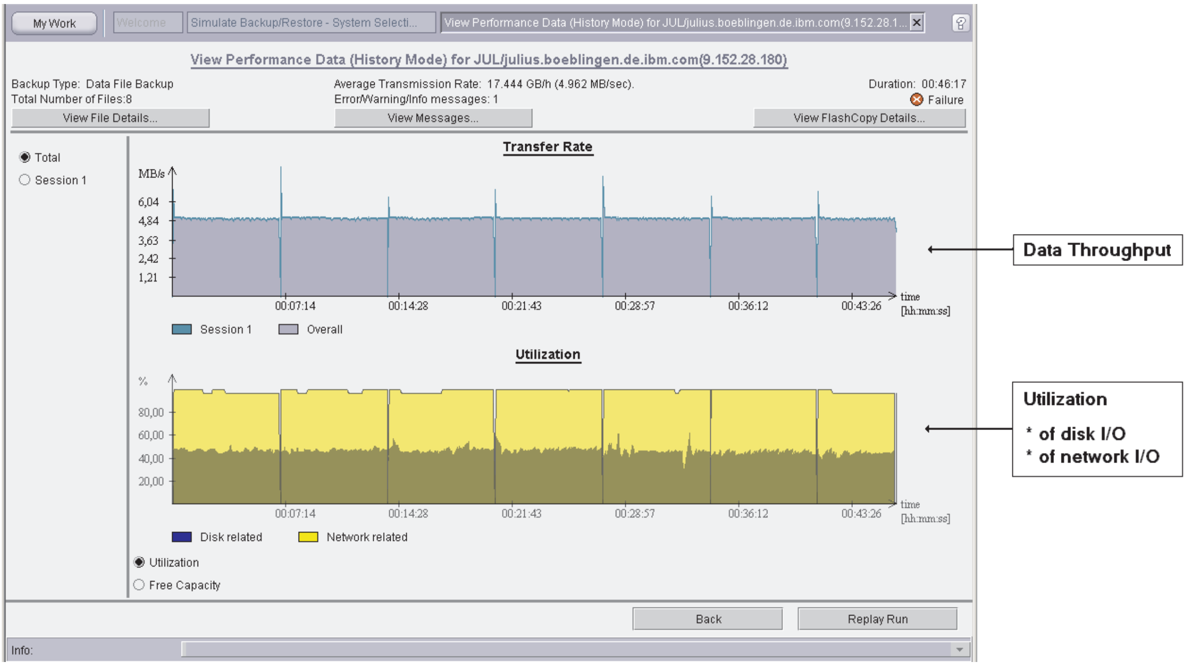
Figure 14. Indicating a Network or Tivoli Storage Manager Bottleneck

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 DB2 performance analysis. 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.

Viewing performance data


My Work
Welcome
Simulate Backup/Restore - System Selecti...
View Performance Data (History Mode) for JUL/julius.boeblingen.de.ibm.com(9.152.28.1...

View Performance Data (History Mode) for JUL/julius.boeblingen.de.ibm.com(9.152.28.180)

Backup Type: Data File Backup
Total Number of Files:8
Average Transmission Rate: 17.444 GB/h (4.962 MB/sec).
Error/Warning/Info messages: 1
Duration: 00:46:17
Failure

Data Throughput

Utilization
* of disk I/O
* of network I/O

Figure 15. 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 DB2 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 DB2 creates a report that contains statistical information such as the number of bytes transferred and the effective data throughput. 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 DB2 Activities" on page 101.

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. Performance optimization is discussed in detail in "Overview of a balanced system" on page 91.

Tracing

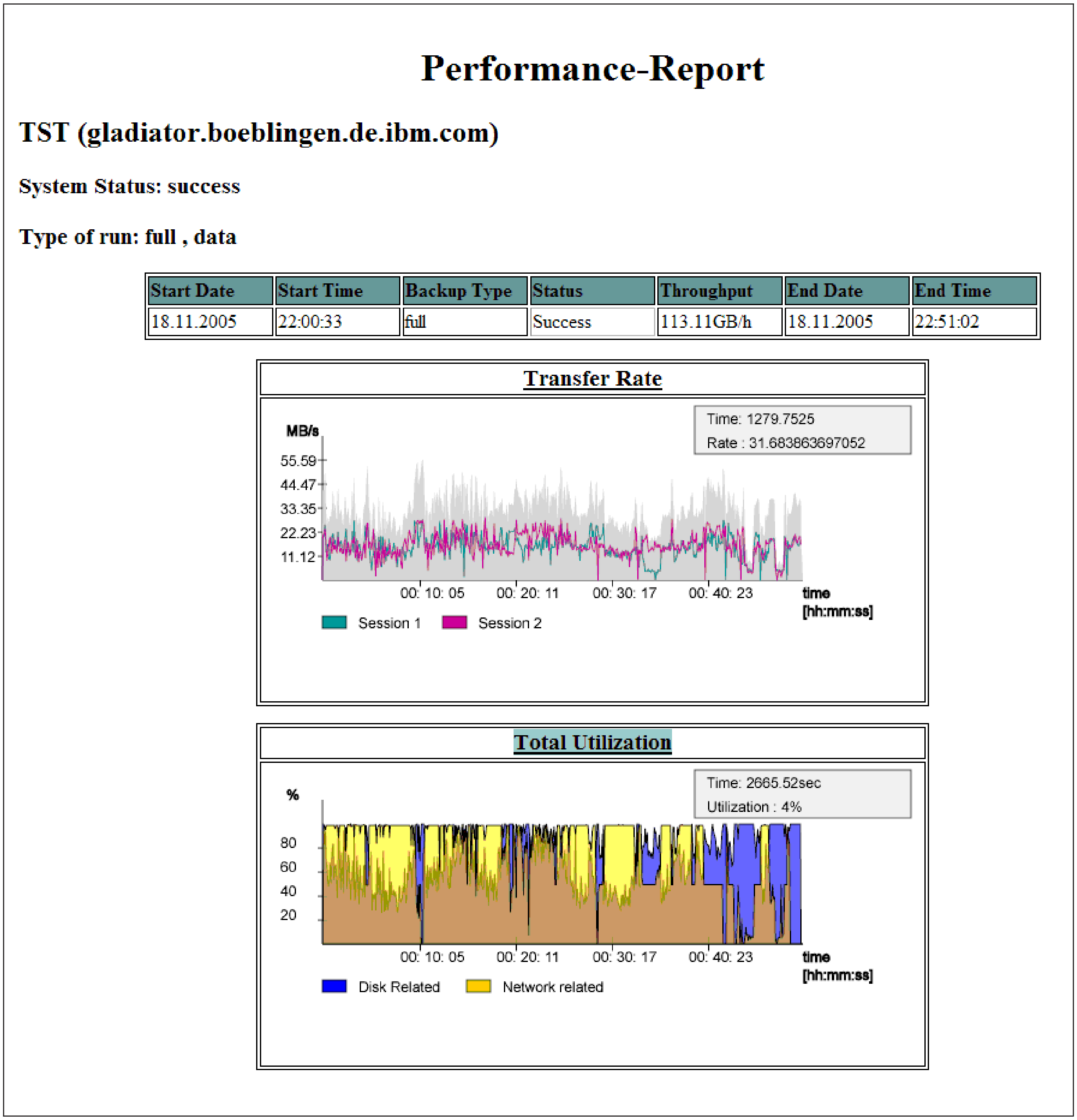
Trace information can be recorded in a file to help analyze problems that occur. However, contact your Data Protection for SAP support before attempting to use this function.

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 97 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

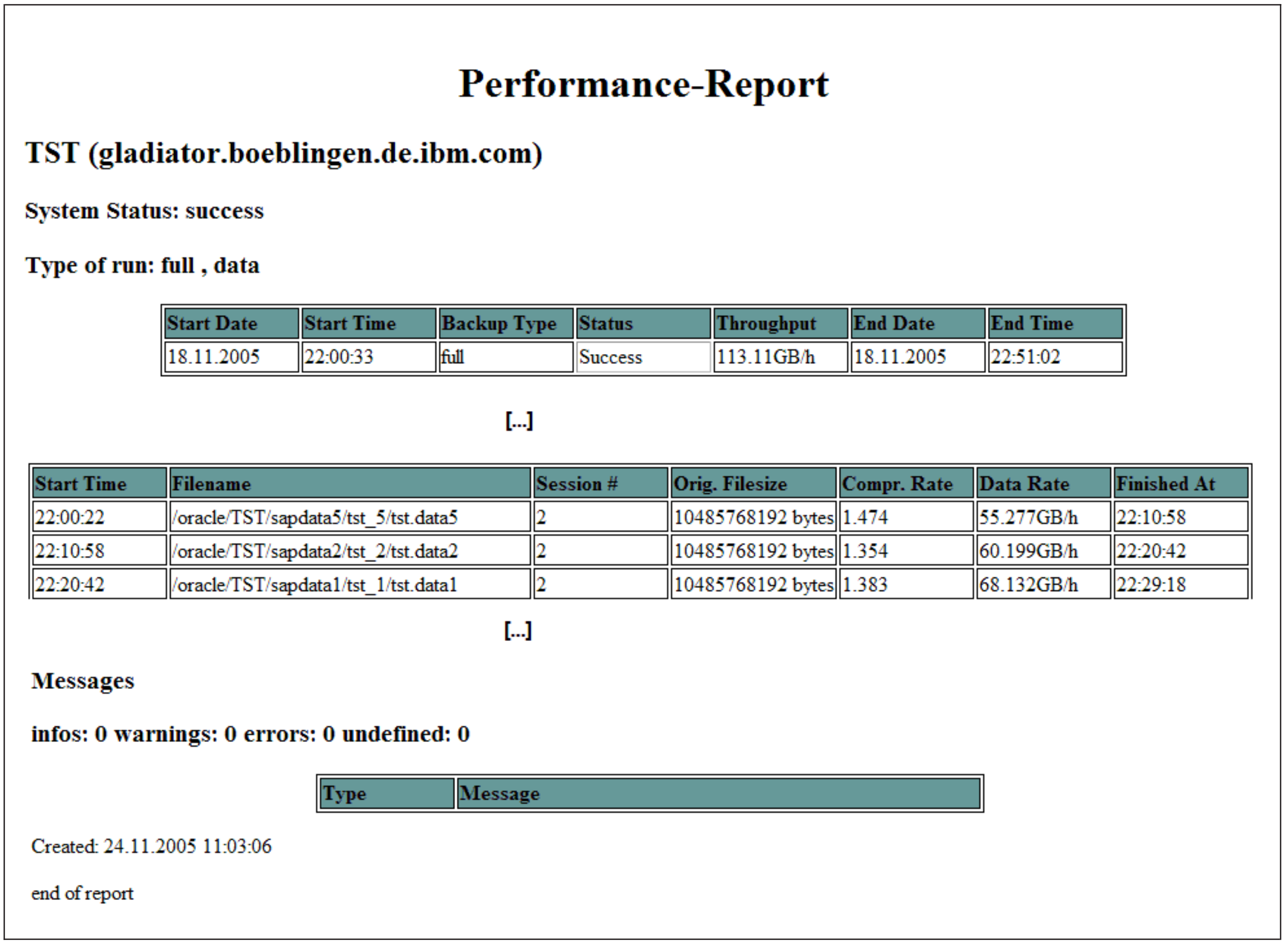
Type of run: full , data

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

Transfer Rate

Total Utilization

Figure 16. 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

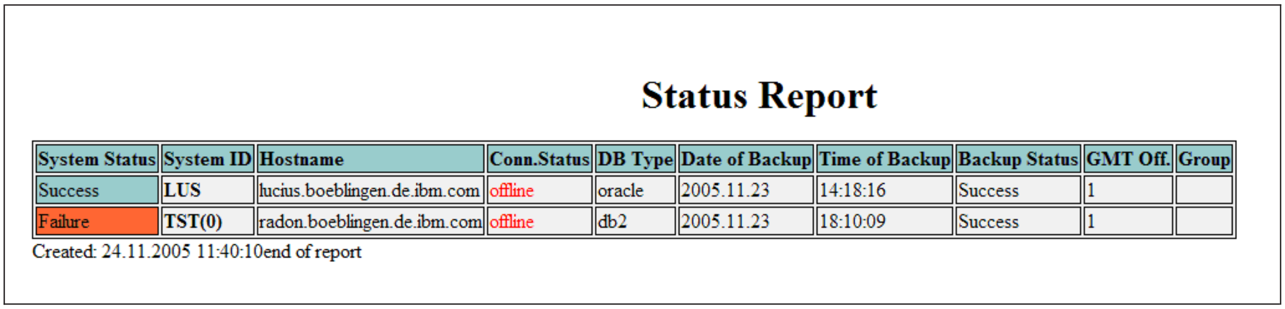
Created: 24.11.2005 11:03:06

end of report

Figure 17. 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 18. Status Report

Creating a Report

Consider this information when planning to create a report:

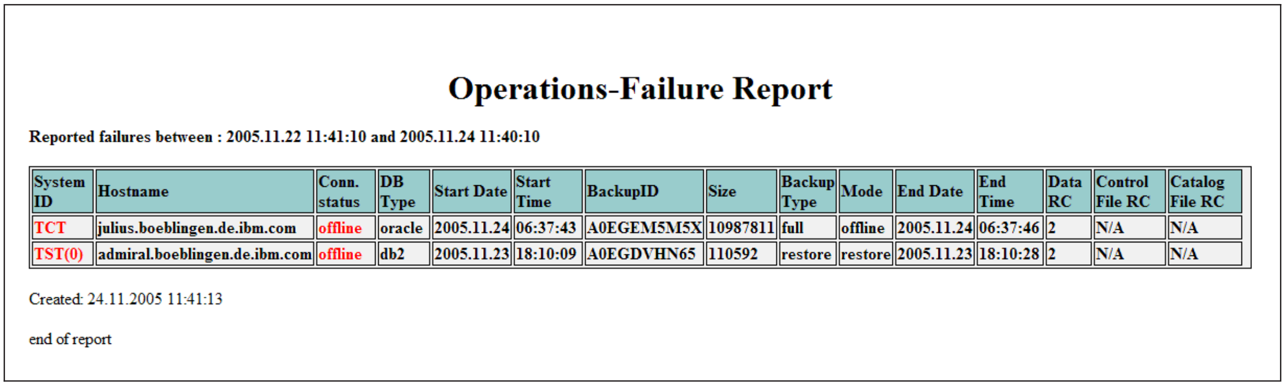
- Reports are requested from the Administration Assistant function for Data Protection for SAP client using the graphical user interface panels that contain the information to be included.
- Reports can also be generated from a scheduling client using a command line interface without any user interaction.
- 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 19. Operations - Failure Report

Modifying Report Output

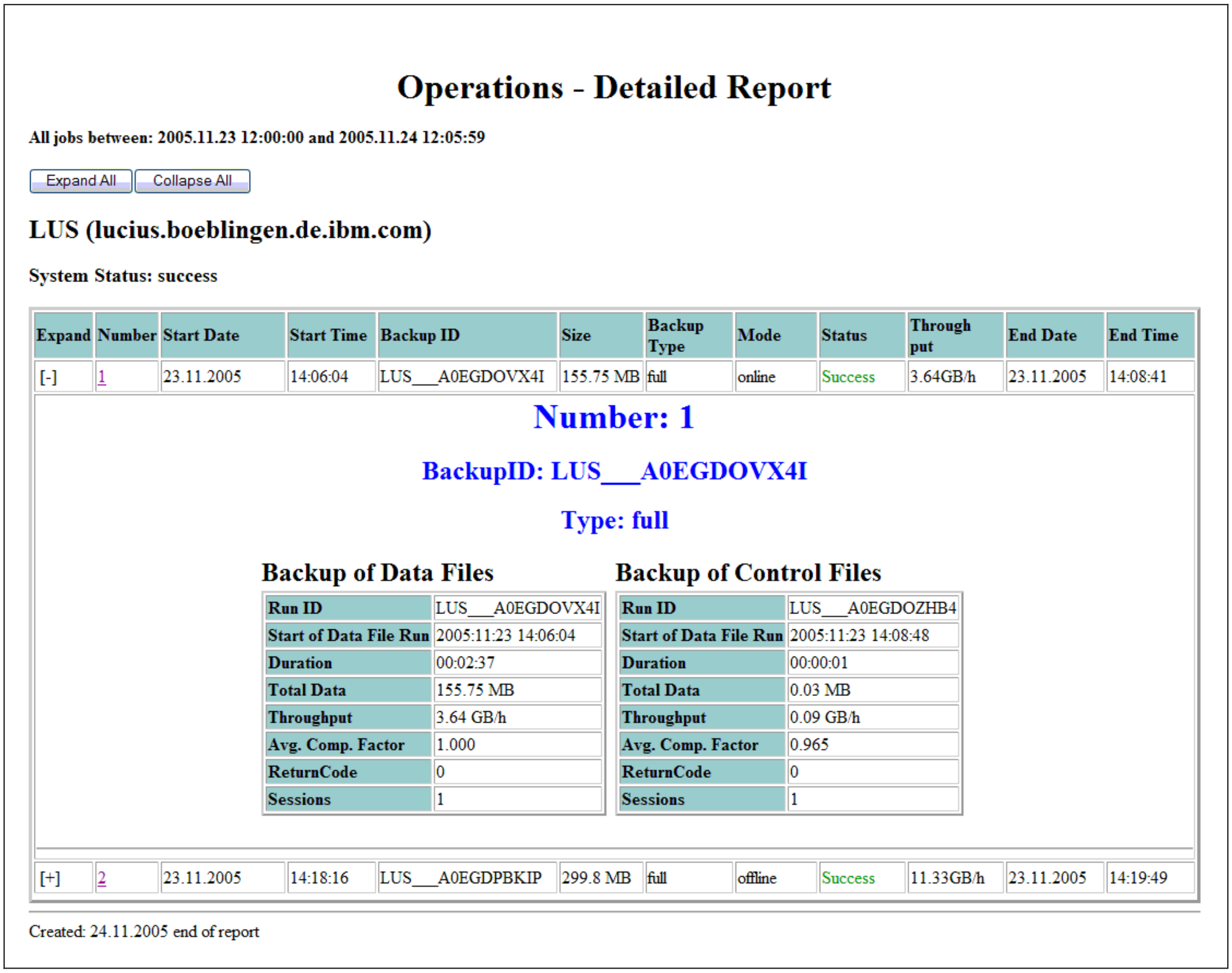
Consider this information when modifying a report:

- 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, and View Performance Data (History Mode). 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

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

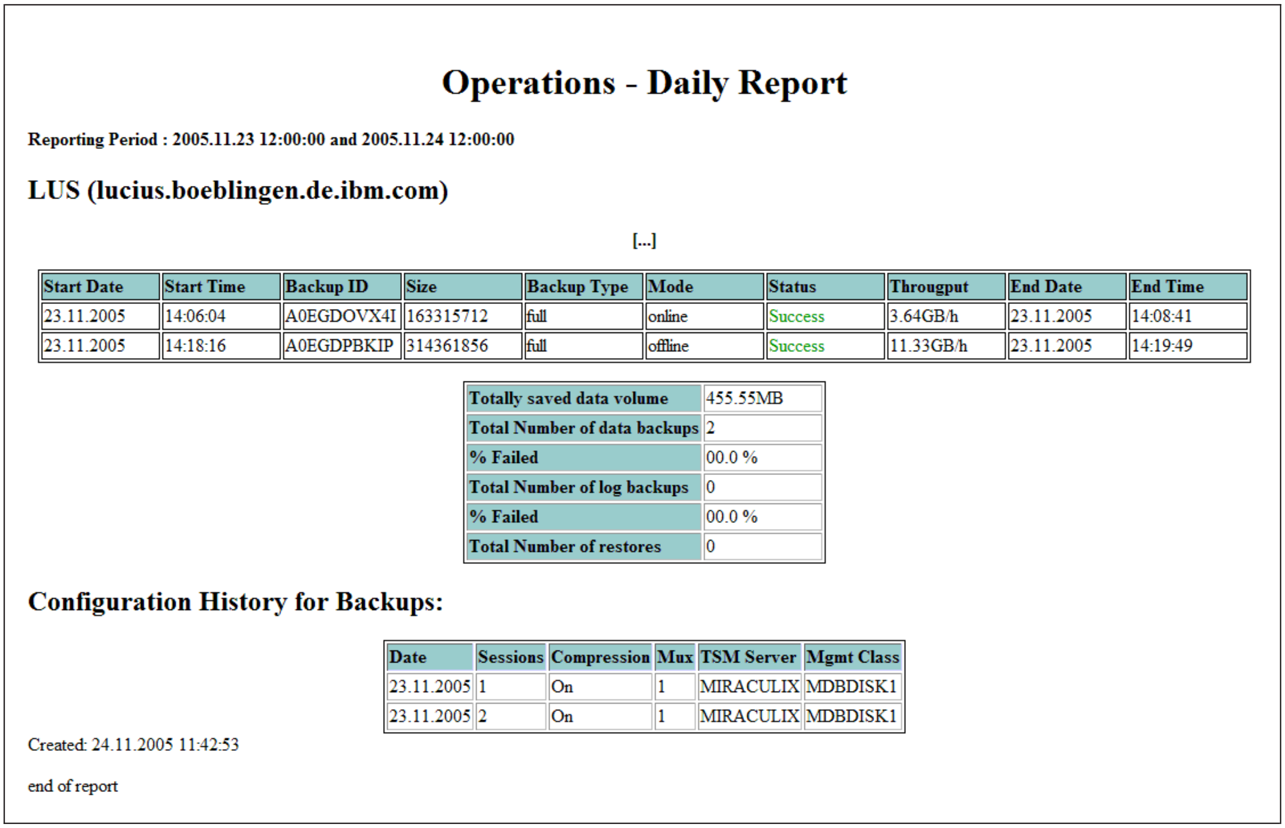
[+]	2	23.11.2005	14:18:16	LUS___A0EGDPBKIP	299.8 MB	full	offline	Success	11.33GB/h	23.11.2005	14:19:49

Created: 24.11.2005 end of report

Figure 20. 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 21. Operations Daily Report

Reporting on Data Protection for SAP for DB2 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 DB2 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 and View Performance Data 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

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

Managing Data on the Backup Server

The Data Protection for SAP for DB2 Backup Object Manager can search for backup objects on the Tivoli Storage Manager server in order to restore or delete them. Complete information is located in "DB2 Backup Object Manager utility" on page 4.

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 DB2 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 DB2 profile parameter descriptions" on page 134). 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 DB2 profile parameter descriptions" on page 134.

Options

Performance Options of Data Protection for SAP for DB2

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 DB2 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 108.

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 109 and “Multiple Servers” on page 107.

Incremental and Delta Backup

Data Protection for SAP supports incremental and delta backups of DB2 databases. Depending on the system environment, incremental backups might decrease backup processing time.

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 104 for complete details.

Adjustments to Data Protection for SAP for DB2 for Improving Performance of Data Transfer

Data Protection for SAP for DB2 is configured (by default) to send uncompressed data to the Tivoli Storage Manager server using a single session.

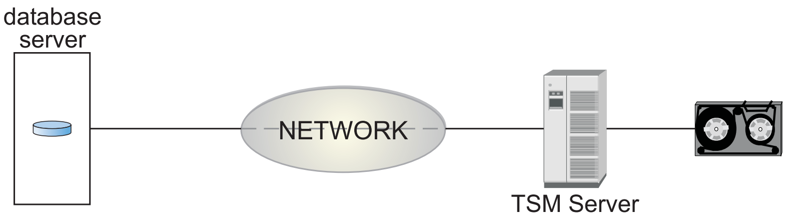


Figure 22. Data Transfer for a Backup / Restore

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 91.

Buffer Copies

Data Protection for SAP for DB2 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 DB2 profile parameter descriptions” on page 134 for more information.

Buffer Size

Data Protection for SAP for DB2 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 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 DB2 profile parameter descriptions” on page 134 for more information.

Compression

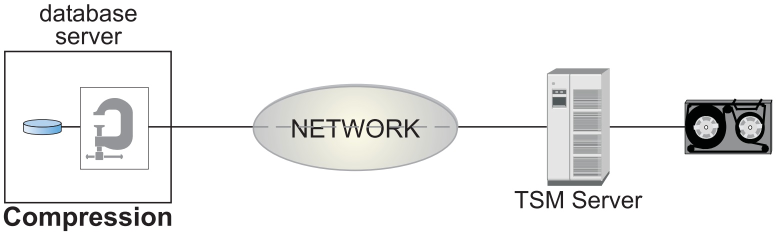


Figure 23. Null Block Compression

Data Protection for SAP for DB2 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 DB2 profile parameter descriptions” on page 134 for details on how to activate Data Protection for SAP compression.

Automation Options for Data Protection for SAP for DB2

Administrative productivity can be improved by using these Data Protection for SAP for DB2 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 DB2 log files to a disk storage pool. Multiple management classes can also be specified to use in conjunction with multiple DB2 log files. The profile keywords BRARCHIVEMGTCLASS and BRBACKUPMGTCLASS in “Data Protection for SAP for DB2 profile parameter descriptions” on page 134 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 specified number, the oldest version is deleted.

Retaining backups keeps track of all DB2 log files, and all incremental and delta 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 DB2 profile parameter descriptions” on page 134 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 DB2 profile parameter descriptions” on page 134.

Data transfer

Observations on the Data Protection for SAP for DB2 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.

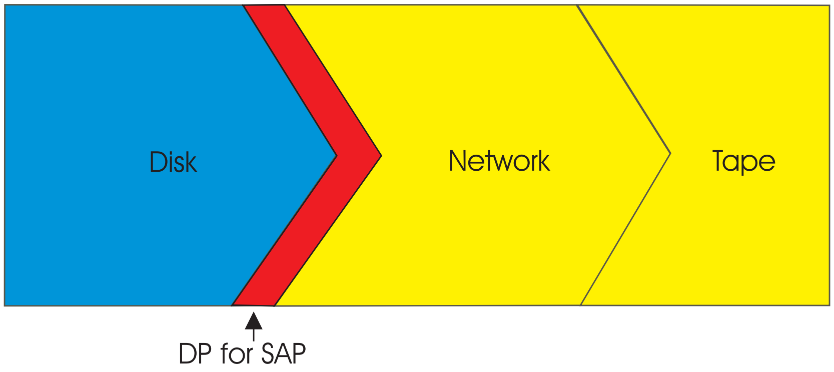


Figure 24. High-level View of the Data Flow During Backup

From a high-level view, the data packages need to send these elements when doing a backup with Data Protection for SAP for DB2: 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 DB2" on page 102. Additional performance issues are available in "General Performance Considerations" on page 107.

Data Protection for SAP for DB2 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.

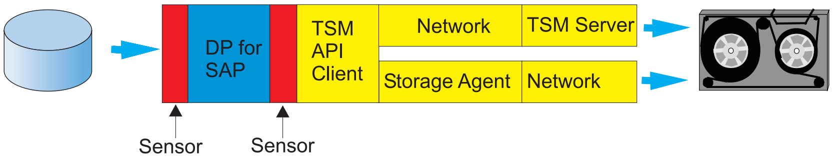


Figure 25. Performance Optimizing by Using Sensors

Data Protection for SAP for DB2 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 26 provides a high level overview of these three main components involved during a Data Protection for SAP for DB2 data transfer:

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

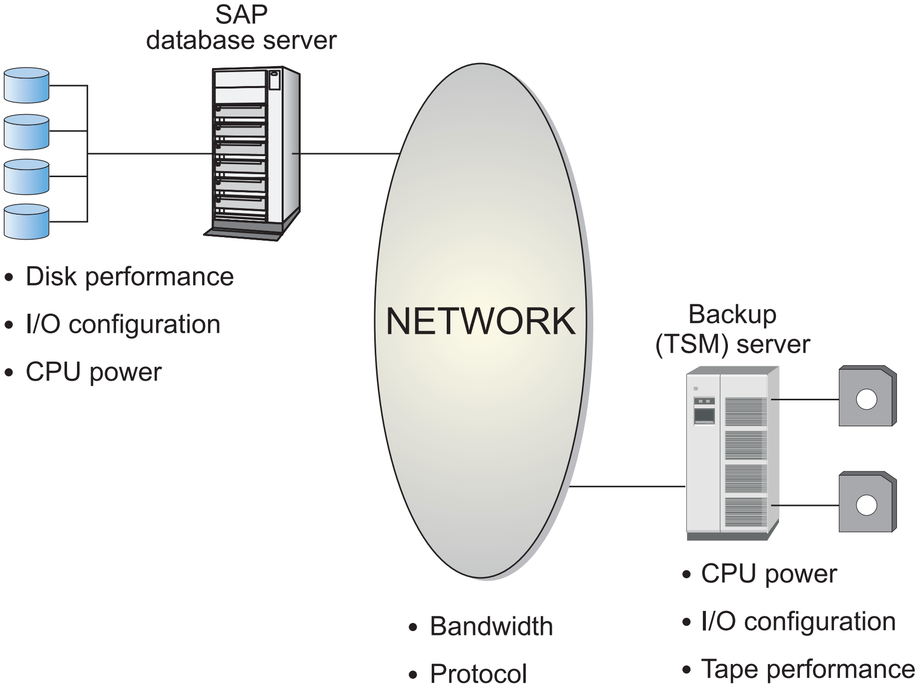


Figure 26. Data Protection for SAP Data Transfer

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 DB2 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.

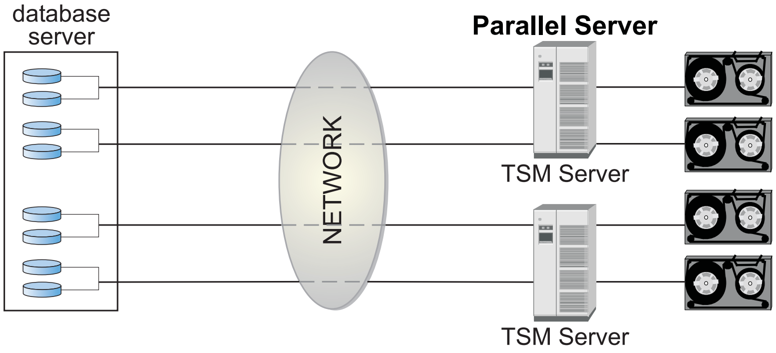


Figure 27. Multiple Servers

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 DB2 profile parameter descriptions” on page 134. The value of the MAX_SESSIONS keyword is not greater than the sum of all SESSION values specified for the SERVER statements used concurrently.

Multiple Sessions

Data Protection for SAP for DB2 allows use of multiple tape drives simultaneously in order to increase the transfer rate to or from the Tivoli Storage Manager server. The keyword MAX_SESSIONS is 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 this keyword, see page “Data Protection for SAP for DB2 profile parameter descriptions” on page 134. 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 DB2 profile parameter descriptions” on page 134.

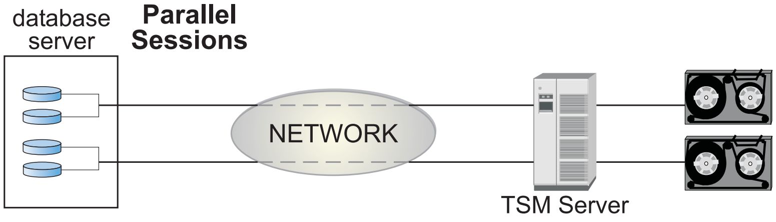


Figure 28. Parallel (Multiple) Sessions

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 DB2 log backups are running, 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, this consideration for database backups also applies to disk storage pools:

Several DB2 log archive sessions can simultaneously utilize one or two independent disk storage pool(s).

The number of storage pools that are required depends on the number of backup copies requested for a DB2 log file. See keyword REDOLOG_COPIES in "Data Protection for SAP for DB2 profile parameter descriptions" on page 134.

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.

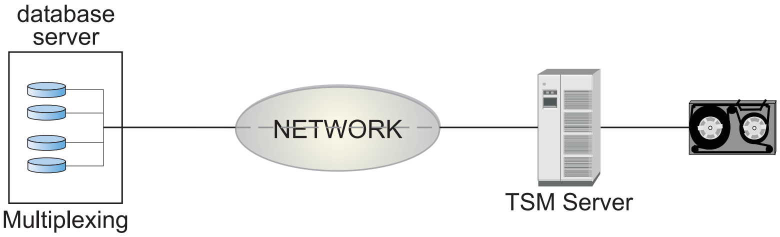


Figure 29. Multiplexing

This feature is provided by the PARALLELISM parameter available with the BACKUP DATABASE and RESTORE DATABASE commands. Refer to your *DB2 Command Reference* for details about these commands and the PARALLELISM parameter.

Multiple Network Paths

Data Protection for SAP for DB2 allows you to use multiple network connections (paths) for data transfer between the database server and the backup server.

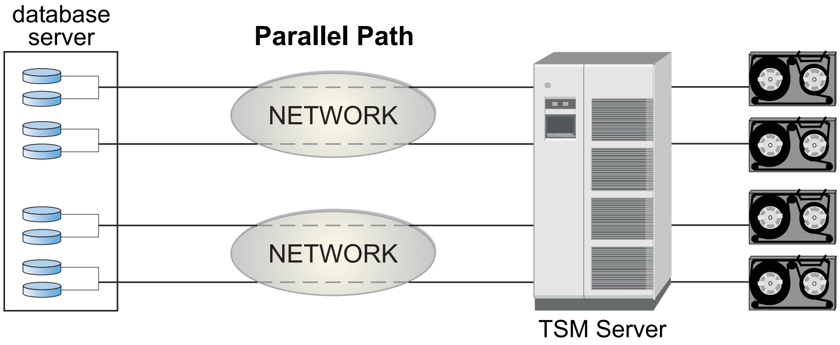


Figure 30. Parallel (Multiple) Paths

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 DB2 profile parameter descriptions" on page 134. 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 18.

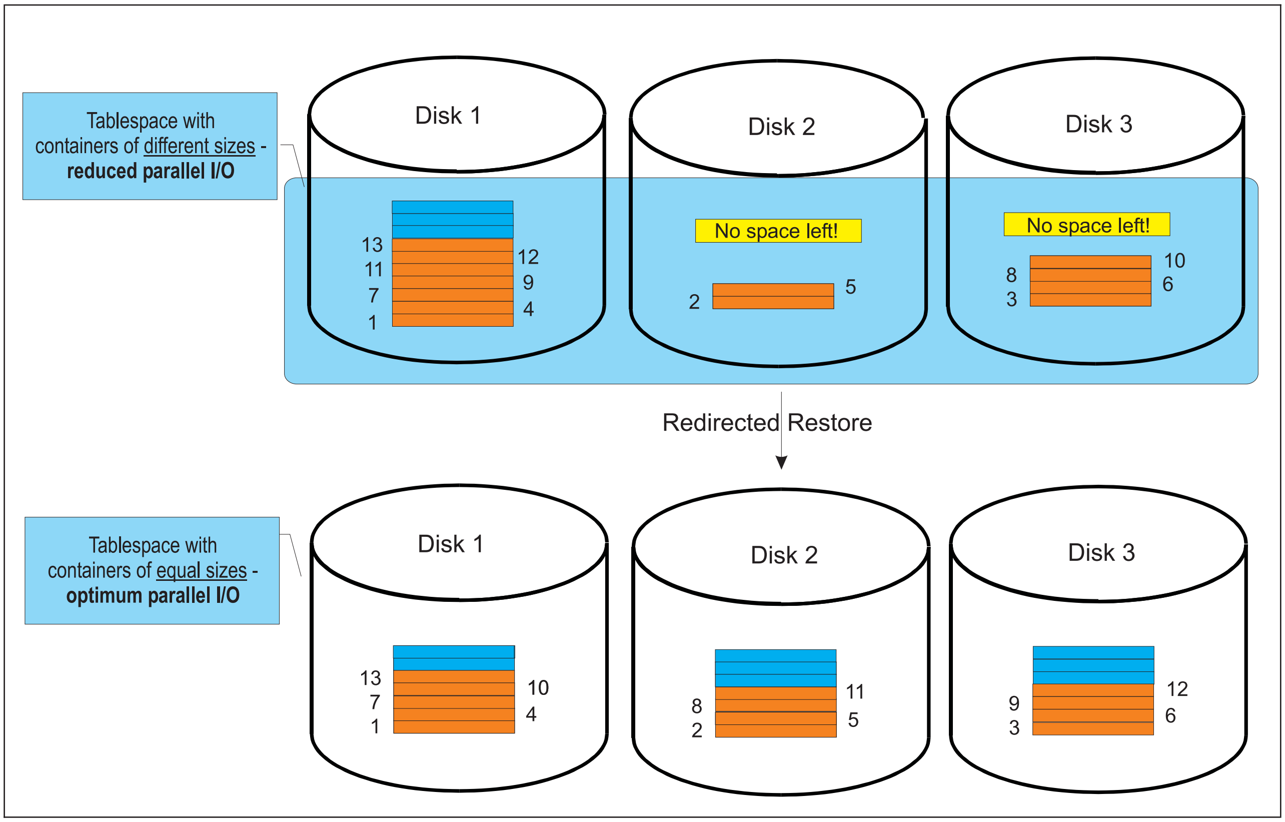
Storage space

Automated Tablespace Adaptations

Backup Object Manager can adapt the sizes of tablespace containers when creating the containers of the target databases during a redirected restore operation. For example, tablespace container sizes might be increased in order to provide more space or decreased in order to use storage more efficiently. Tablespaces can also be allocated with similar sizes in order to make parallel I/O operations more efficient. These features are supported by Backup Object Manager resizing and normalizing functions.

Tablespace Normalizing

In order to achieve optimal parallel I/O operation performance for a database, all containers of a tablespace should be the same size. During tablespace maintenance, containers may be added or extended which creates different container sizes. As a result, data is unevenly distributed among the containers which can result in decreased parallel I/O operation performance during table scans (sequential prefetching). Backup Object Manager provides an automated tablespace normalizing function that allows the location and size of tablespace container to be redefined. This also helps prevent I/O-intensive tablespace rebalancing that can be detected by DB2.



Tablespace with containers of different sizes - reduced parallel I/O
Disk 1
13
11
7
1
12
9
4
Disk 2
No space left!
2
5
Disk 3
No space left!
8
3
10
6
Redirected Restore
Tablespace with containers of equal sizes - optimum parallel I/O
Disk 1
13
7
1
10
4
Disk 2
8
2
11
5
Disk 3
9
3
12
6

Figure 31. Tablespace Normalizing

This graphic shows that the original system tablespace consists of different sized containers. Even though sequential prefetching allows three processes to simultaneously read the data during table scans, the different container sizes and uneven data distribution prevent parallel I/O during part of the scan. The degree of parallelism decreases over time. To counteract this, adjust the containers for each tablespace so that they are the same size. This type of adjustment, in combination with a redirected restore operation, requires no further resizing tasks for the tablespace containers after the restore completes.

Backup Object Manager simplifies the tablespace container resizing process by providing an automatic tablespace normalizing function. It can be used in combination with any mode of redirected restore facility by specifying the -N option. Issue this command to resize each container of a tablespace to the average size of all containers within the same tablespace during a redirected restore:

```
backom -c rr_db_type -aDB2 source alias,DB2 target alias -t timestamp -N
```

After the redirected restore completes successfully, all containers of a tablespace of the target database are the same size. As a result, the continuous parallel I/O performance of the physical layout of the restored database is optimized.

Tablespace Scaling

Sufficient free space must be available in a tablespace for the database to function properly. Backup Object Manager provides an automated tablespace scaling function that allows the location and size of tablespace container to be redefined. This also helps prevent I/O-intensive tablespace rebalancing that can be detected by DB2.

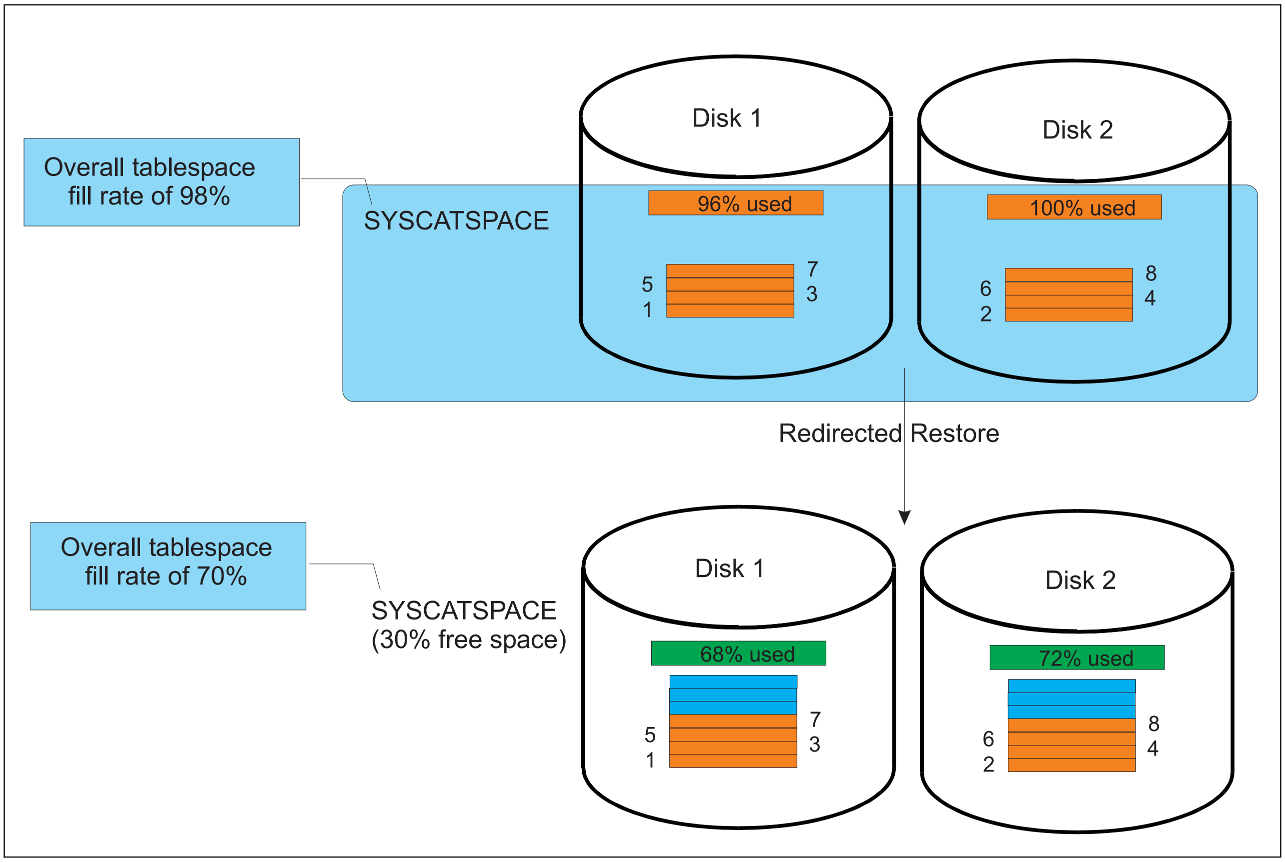


Figure 32. Tablespace Scaling

This graphic shows that 98% of the SYSCATSPACE tablespace of the original system is being used. Disk 1 has 4% free space while 100% of the second container is used. The free space available in a tablespace can be increased as part of the redefinition feature during a redirected restore. The goal is to achieve an overall filling rate for the target side of 70%. This can be achieved by manually increasing the amount of free space the first container must provide at 20% and 40% for the second container. This type of adjustment, in combination with a redirected restore operation, requires no further resizing tasks for the tablespace containers after the restore completes.

Backup Object Manager simplifies the tablespace resizing process by providing an automatic tablespace scaling function. It can be used in combination with any mode of redirected restore by specifying the -S option with a floating point sizing factor. Consider these factors when resizing tablespaces:

- A value of '1' indicates that the target tablespace is 100% the size of the original (nothing is changed).
- A value greater than 1 increases the target tablespace. For example, a value of 1.1 increases the target tablespace by 10% to a target value of 110% of the original.
- A value less than 1 decreases the target tablespace. For example, a value of 0.9 decreases the target tablespace by 10% to a value of 90% of the original.

Therefore, manual adaptation of the tablespace containers described above can be replaced by the following procedure using Backup Object Manager redirected restore:

1. Issue this Backup Object Manager query to determine the original fill rate of the tablespace:

   ```
   backom -c q_tdi -a DB2 source alias -t timestamp -m detailed
   ```

2. Calculate the tablespace scaling factor using this formula:

   ```
   scaling factor = original fill rate / new fill rate
   ```

   For example:

   ```
   scaling factor = 0.98 / 0.7 = 1.4
   ```

3. Issue this command to begin the Backup Object Manager redirected restore:

   ```
   backom -c rr_db_type -a DB2 source alias,DB2 target alias -t timestamp ...
   ...-T SYSCATSPACE -s 1.4
   ```

   After the redirected restore has completed successfully, the SYSCATSPACE tablespace on the target side is increased by 40% during tablespace container redefinition. The new overall fill rate of the SYSCATSPACE in the target database is now 70%.

Chapter 8. Troubleshooting IBM Tivoli Storage Manager for Enterprise Resource Planning

Information on how to resolve errors that might occur during IBM Tivoli Storage Manager for Enterprise Resource Planning operations is provided.

Troubleshooting IBM Tivoli Storage Manager for Enterprise Resource Planning common problems

Information on how to resolve errors that might occur during IBM Tivoli Storage Manager for Enterprise Resource Planning 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 ((`tdpdb2.`*`SID`*`.`*`nodename`*`.log`, `db2diag.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 DB2 setup changed.
- One (or more) of the DB2, 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 `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 `tdpdb2.`*`SID`*`.`*`nodename`*`.log`.
  - 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 (`vendor.env`, `init`*`SID`*`.utl`, `dsm.sys`, `dsm.opt`, `/etc/services`, `/etc/inittab`, `...`).. This UNIX 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 DB2 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:

  ```
  pd64:2:respawn:/usr/tivoli/tsm/tdp_r3/db264/prole -p tdpr3db264
  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 DB2 port `tdpr3db264` for connections with the shared library 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:

  ```
  tdpr3db264      57324/tcp
  ```

  These lines are added to the `/etc/services` file by the installer.

See Figure 33 on page 117 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:

```
tdpr3db264      57324/tcp
```

- Make sure the Data Protection for SAP configuration file `init`*`SID`*`.utl` is located in the directory to pointed by the TDP_DIR environment variable.
- The vendor environment file `vendor.env` must contain the fully qualified path and file name of the `init`*`SID`*`.utl` file.
- The vendor environment file `vendor.env` should contain the path of the location where the Data Protection for SAP run logs are written. If this location is not specified, temporary directory of the machine is used.

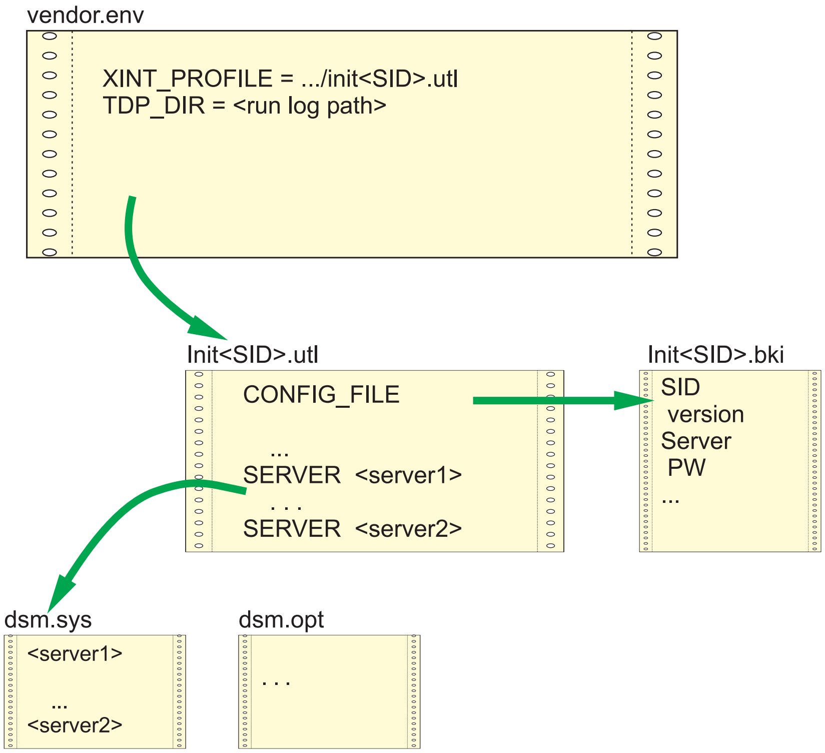


Figure 33. SAP® and Data Protection for SAP configuration files on UNIX or Linux

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 Tivoli Storage Manager API message text file resides. This is typically the `c:\Program Files\Tivoli\tsm\api64` directory.

Providing information to IBM or Tivoli support

Provide this information when contacting IBM or Tivoli support:

- The Data Protection for SAP for DB2 version.
- The operating system level and patches that were applied.
- The DB2 version
- The Tivoli Storage Manager server version.
- The Tivoli Storage Manager server operating system level.
- Data Protection for SAP configuration file (`vendor.env`, `initSID.utl`) including Tivoli Storage Manager client configuration files (`dsm.sys`, `dsm.opt`)
- Data Protection for SAP profile (`initSID.utl`)
- 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 DB2 problems

Information on how to resolve errors that might occur during Data Protection for SAP for DB2 operations is provided.

General problem resolution

The following graphic (Figure 34 on page 119) will help you to isolate problems that occur when backing up or restoring of your DB2 database.

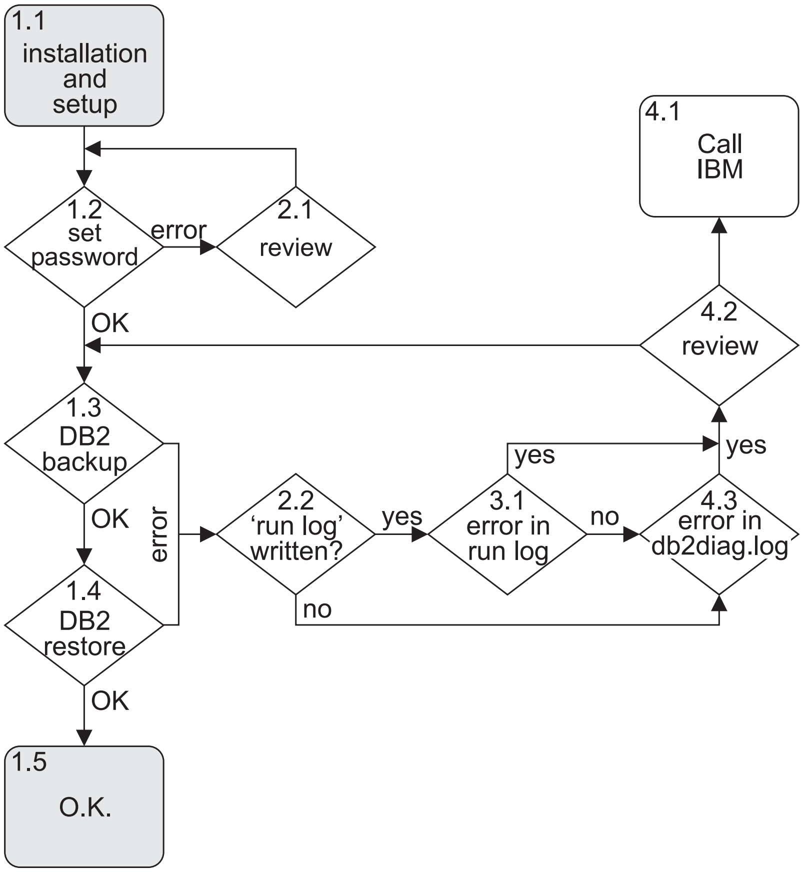


Figure 34. General Problem Isolation

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 backom again.

`BKI5001E: Tivoli Storage Manager Error: Server not found in configuration file`
On UNIX or Linux, the Tivoli Storage Manager server defined in the `initSID.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 backom 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 the DB2 backup command to verify the settings are correct as described in "Backing up SAP® data" on page 67. If the backup was successful you will see a message from DB2:

```
Backup successful. The timestamp for this backup image is: timestamp
```

If an error message displays, view the error description in "Data Protection for SAP (DB2) Messages" on page 159 for information regarding how to resolve it.

When an error occurs, always view the Data Protection for SAP run log `tdpdb2.SID.nodename.log` first. This log file is located in the directory specified by the TDP_DIR environment variable. If the variable is not specified, the log file resides in the system temporary directory. If the `tdpdb2.SID.nodename.log` file does not exist (Step 2.2), then either DB2 was unable to load the shared library that contains the DB2 connector for Data Protection for SAP or an error was encountered before calling the Data Protection for SAP library. In both cases, a DB2 error message should display on the command line that begins with the `SQL` prefix and is also written in the DB2 diagnostic log `db2diag.log` (Step 4.3). DB2 provides detailed error descriptions by issuing this command:

```
db2 ? SQLnumber
```

Replace *number* with the appropriate message number. Try to resolve this problem using the DB2 documentation.

If the `tdpdb2.SID.nodename.log` file exists, search for a message beginning with `BKIXXXXY` where *XXXX* is a four digit number and *Y* is the letter I, W, or E. When such a message occurs, the DB2 connector for Data Protection for SAP loaded correctly was called by DB2. In Step 3.1, the `tdpdb2.SID.nodename.log` file is created and an error message starting with `BKI` is recorded.

Location of log files

Text displayed on the screen during DB2 backup, DB2 restore, and BackOM operations are typically written to log files. DB2 also writes messages of internal operations, events, or status in the administration notification log file (`db2SID.nfy`) and diagnostic log file (`db2diag.log`). These log files reside in the directory specified with the DB2 database management configuration parameter DIAGPATH. Query the DB2 database management configuration with this command:

```
db2 get dbm cfg
```

Information about how to locate these log files is available in "How to find files containing message output (log files)" on page 159.

DB2 vendor reason codes

Data Protection for SAP for DB2 uses these reason codes which might also be displayed or logged by DB2 in the case of problems.

Table 11. DB2 Vendor Reason Codes

Reason Code	Explanation	User Response
1	The library specified could not be loaded.	Check the DB2 diagnostic log for further details.
2	Communication error between shared library and ProLE	Check the Data Protection for SAP run log file `tdpdb2.SID.nodename.log` for further details.
6	Object specified cannot be found on Tivoli Storage Manager.	There is no backup image on Tivoli Storage Manager matching the given search criteria.
10	Invalid options specified with the options parameter of the DB2 backup/restore command.	Check the options string specified and check theData Protection for SAP run log file `tdpdb2.SID.nodename.log` for further details.
11	Initialization procedure for shared library failed.	Check the Data Protection for SAP run log file `tdpdb2.SID.nodename.log` and the DB2 diagnostic log file for further details.
17	During end processing of either backup/archive or restore/retrieve session(s), an error occurred.	Check the Data Protection for SAP run log file `tdpdb2.SID.nodename.log` for further details.
18	An error occurred during reading or writing data from or to Tivoli Storage Manager.	Check the Data Protection for SAP run log file `tdpdb2.SID.nodename.log` for further details.

Table 11. DB2 Vendor Reason Codes (continued)

Reason Code	Explanation	User Response
26	An error occurred during deleting data from Tivoli Storage Manager.	Check the Data Protection for SAP run log file `tdpdb2.`*`SID.nodename`*`.log` for further details.
29	An abort request from DB2 could not be handled correctly.	Check the Data Protection for SAP run log file `tdpdb2.`*`SID.nodename`*`.log` and the DB2 diagnostic log file for further details.
30	A severe error occurred.	Check the DB2 diagnostic log file for further details.

Chapter 9. Data Protection for SAP for DB2 reference information

Data Protection for SAP for DB2 reference information is provided here.

Commands used with Data Protection for SAP for DB2

A list of various commands that are used with Data Protection for SAP for DB2 operations is provided.

Backups and Restores in Partitioned Database Environments

DB2 Version 9.5 (or later) provides the Single System View (SSV) function, which allows the backup of all partitions to be triggered with a new dedicated DB2 backup command option ON ALL DBPARTITIONNUMS (see "Using DB2 Single System View for Backup" on page 69 for more information). Furthermore, partitioned database backups and restores can be made by using the already established DB2 framework for partitioned databases called db2_all. A requirement of DB2 is to back up and restore the catalog partition separately from all other DB2 partitions. Thus, backup and restore operations of a partitioned database are two-step scenarios, whereby the first step is to backup/restore the catalog partition and the second step to backup and restore all other partitions in parallel. Data Protection for SAP uses the DB2 command `db2_all` for separation and parallelization of the backup and restore commands. The `db2_all` command provides special characters for handling partitions and for running commands in parallel or sequentially. The DB2 *Administration Guide* contains further information.

The DB2 `db2_all` command supports the following special characters or character combinations:

- `<<+N<` Runs a command only on partition N
- `<<-N<` Runs a command on all partitions except on partition N
- `"` Substitute occurrences of () by the machine index and substitute occurrences of ## by the partition number
- **;** Runs the commands in parallel in the background and terminates the command after all remote commands are completed.

By using these characters, each partition of the database can be backed up or restored with its special adapted environment.

This list presents possible partitioned database backups and restores using Data Protection for SAP for DB2:

Full offline backup

Full offline backup of all database partitions with two sessions, starting with the catalog partition (shown as partition 0) followed by all other partitions in parallel:

```
db2_all '<<+0< db2 backup db SID load shared library open 2 sessions'
db2_all '<<-0<; db2 backup db SID load shared library open 2 sessions'
```

Full restore of latest backup

Full restore of latest backup starting with the catalog partition (shown as partition 0) followed by all other partitions (shown with three partitions) in parallel using different number of sessions for some of the partitions. Before starting the restore, a temporary environment script (this example uses `/db2/SID/EEEenv.sh`) has to be created. The `/db2/SID` directory must be an NFS share between all hosts where the partitions reside. For this example, it would contain the following:

```
export SESSION0=2
export SESSION1=2
export SESSION2=4
export SESSION3=4
```

This means that partitions 0 and 1 will be restored with two sessions, and partitions 2 and 3 will be restored with four sessions. As a result, this is the restore command:

```
db2_all '<<+0<" ./db2/SID/EEEenv.sh; db2 restore db SID load shared library open
$SESSION##'
db2_all '<<-0<" ./db2/SID/EEEenv.sh; db2 restore db SID load shared library open
$SESSION##'
```

The string '$SESSION##' in the db2_all command will be replaced while running it with the value provided by the environment variables SESSION0 to SESSION3.

Full online backup

Full online backup of all database partitions, starting with the catalog partition (shown as partition 1) followed by all other partitions in parallel using different Data Protection for SAP profiles for each partition. To support this scenario, one Data Protection for SAP profile (`initSID.utl`) must be created and maintained for each partition. Each profile can have different settings for the Tivoli Storage Manager node and management class. These are the profiles needed for this example:

- `initSID.utl.1` (profile for partition 1)
- `initSID.utl.2` (profile for partition 2)
- `initSID.utl.3` (profile for partition 3)
- `initSID.utl.4` (profile for partition 4)

In addition, a Data Protection for SAP vendor environment file (`vendor.env`) must be created and maintained for each partition. Each vendor environment file has an XINT_PROFILE entry which refers to the corresponding Data Protection for SAP profile. For example:

```
vendor.env.1 (environment for partition 1 ->
XINT_PROFILE=/db2/SID/vendor.env.1)
```

```
vendor.env.2 (environment for partition 2 ->
XINT_PROFILE=/db2/SID/vendor.env.2)
```

```
vendor.env.3 (environment for partition 3 ->
XINT_PROFILE=/db2/SID/vendor.env.3)
```

```
vendor.env.4 (environment for partition 4 ->
XINT_PROFILE=/db2/SID/vendor.env.4)
```

As a result, this is the backup command:

```
db2_all '<<+1<" db2 backup db SID online load shared library options
/db2/SID/vendor.env.##'
db2_all '<<-1<;" db2 backup db SID online load shared library options
/db2/SID/vendor.env.##'
```

The string `vendor.env.##` in the `db2_all` command will be replaced while executing it with the values `vendor.env.1` - `vendor.env.4`, whereby the special characters '`##`' will be substituted by the corresponding partition number.

Managing Backup Objects

This is the Backup Object Manager syntax:

`backom [ -? ]` displays the syntax help.

Note: For the C shell, enclose the option string in quotes (`backom '-?'`).

`backom -h [password|query|backup|restore|delete]` displays the `command` online help.

```
backom -c command [ command option ...]
```

where '`command`' is one of:

for Password: `password`

for Query: `q_all` | `q_db` | `q_ts` | `q_log` | `q_tdi` | `q_raw`

for Backup: `b_db`

for Restore: `r_db` | `r_ts` | `r_log` | `r_hfile` | `r_raw` | `r_tdi` | `rr_db_interactive` | `rr_db_batch` | `rr_db_clone`

for Delete: `d_db` | `d_ts` | `d_log` | `d_raw`

where '`command option`' is one of:

```
-i    instance
-a    alias name
-n    node number
-u    userid
-p    password -t    timestamp | timerange
-l    log number | log number range
-k    log chain | log chain range
-f    file name
-d    destination directory
-e    execution profile
-b    buffer size
-s    scaling factor
-N
-S    sessions
-B    number of buffers
-P    parallelism
-D    target database
-T    tablespace
-R    full | incremental | delta
-O
-L
-C
-x
-v
-m    output mode
```

Backup Object Manager Commands

Details regarding these six types of Backup Object Manager commands are provided:

- Password command
- Query commands
- Backup command
- Restore commands
- Delete commands

Details regarding these commands and their syntax requirements are provided in this section. Optional command options are listed in brackets [ ], parameter descriptions, that must be replaced, are listed in angle brackets .

Backup Object Manager Command Options

The following options may be specified together with Backup Object Manager commands:

- `-a` *`database alias`* or `-a` *`original database alias`*`,`*`target database alias`*. Denotes the name of the database for which an operation is requested. In the case of a redirected restore to a different database or of database cloning, the database aliases of both the original and the target databases must be specified and separated by a comma. When a redirected restore is requested that specifies a single database alias, the database is restored to the original database.
- `-b` *`buffer size`* Denotes the size of DB2 backup or restore buffers, in 4 KB allocation units (pages). The minimum is 8 units. The buffer size is limited by the memory available.
- `-B` *`number of buffers`* Denotes the number of DB2 buffers to be used for backup or restore. The minimum number is 2. The number of buffers is limited by the available memory.
- `-C` If specified for a redirected restore, this option indicates that the Backup Object Manager should only run a test of the setup but not start copying data.
- `-d` *`destination directory`* Denotes the destination path for restoring a file to the file system.
- `-D` *`target database directory`*For a redirected restore, this option denotes the fully qualified name of the target database directory. This command option is ignored when the database alias of the target database is the same as the database alias of the original database.
- `-e` *`execution profile`* Denotes the complete path of the Data Protection for SAP for DB2 profile to be used with the Backup Object Manager. This option overrides the profile name set in the XINT_PROFILE environment variable.
- `-f` *`file name`* Denotes the name of a file in the file system. Unless the file denotes a TDI image, the following wild card characters are accepted:? denotes any single character * denotes any number of any characters.
- `-i` *`DB2 instance`* Used in query commands to limit the database or tablespace data to be displayed to a specific DB2 instance. With all other commands, this command option is used to override the DB2 instance name defined in the DB_INSTANCE environment variable.
- | `-k` *`log chain`* `|` *`log chain range`* where `<log chain range>` = *`chain1`* `-`
| *`chain2`*.Denotes the log chain number(s) of DB2 log file(s). DB2 log chains can be
| specified either in the format C*nnnnnnn*, where *nnnnnnn* is a string of 7 decimal

digits or in the format *mmmmmmm*, where *mmmmmmm* is a string of up to 7 decimal digits denoting the log chain number.

- `-l` *`log number`* `|` *`log number range`*`where<log number range> =` *`log number 1 - log number 2`* Denotes the log serial numbers of DB2 log files. DB2 log numbers can be specified either in the format Snnnnnnn.log (DB2 log file name), where nnnnnnn is a string of 7 decimal digits, or in the format mmmmmmm, where mmmmmmm is a string of up to 7 decimal digits denoting the log serial number.
- `-L` If specified for a database backup, the DB2 log files are saved to Tivoli Storage Manager with the database backup.
- `-m` *`output mode`* where `<output mode> = short | normal | detailed` Denotes the detail of information requested with a query command. The default is "short" for information related to DB2 log files, "normal" for all other kinds of information.

  If you need to override the default values generally, you may set environment variables FULL_OUTPUT (for information on database backups), TABLESPACE_OUTPUT (for information on tablespace backups) and LOG_OUTPUT (for information on DB2 log file backups) to the values desired.
- `-N` If specified, this command option causes all containers of a tablespace to be allocated with the same size during a redirected restore.
- `-n` *`node number`* Denotes the DB2 node number. For the password command in a DB2 partitioned environment: If for only one DB2 node/partition the password has to be set/changed, specify the command option -n <node number>.If the node/partition number is not specified, the new password is saved to all available node/partitioned based Data Protection for SAP configuration files. For all other commands: If the node number is not specified, node NODE0000 is assumed.
- `-O` If specified when requesting a backup or tablespace restore operation, an online backup or an online tablespace restore is performed.
- `-p` *`password`*The password of the user ID specified in option -u.
- `-P` *`parallelism`* Denotes the degree of parallelism within DB2, i.e. the number of buffer manipulator processes reading from or writing to tablespaces at the same time. The minimum parallelism is 1, the maximum is 1024.
- `-R` *`backup type`* where `<backup type> = full | incremental | delta` . Denotes the type of backup requested. If no backup type is specified a full backup is performed.
- `-S` *`sessions`*Denotes the number of I/O sessions that are to be started by DB2. The value of this command option must be less than or equal to the value of the keyword MAX_SESSIONS in the Data Protection for SAP profile.
- `-s` *`scaling factor`*Denotes the positive floating point factor to be used for resizing all containers of a tablespace during redirected restore. The default is 1, indicating that the new tablespace is exactly the size of the original.
- `-t <timestamp | time range>` where `time range =` *`timestamp1-timestamp2`* Denotes the time when a backup object was created. For database and tablespace backups, this timestamp matches the timestamp listed in the DB2 Recovery History File. It consists of 14 decimal digits and has the format: yyyymmddhhmmss where yyyy is the year mm is the month of the year, 01 through 12 dd is the day of the month, 01 through 31 hh is the hour of the day, 00 through 23 mm is the minute of the hour, 00 through 59 ss is the second of the minute, 00 through 59. For restore commands, an **exact** timestamp must be given. For query and delete commands, a time range can be specified, or the timestamp might contain wild card characters. The following wild card characters are accepted:

  - ? denotes any single digit
  - * denotes any number of any digits.

  If a timestamp is not specified for a query, the result will contain all eligible backup object available on the Tivoli Storage Manager server. If a timestamp is not specified for a restore, the newest object is retrieved from Tivoli Storage Manager.
- `-T` *tablespace list* where `<tablespace list> =` *tablespace*`[,`*tablespace list*`]` For a backup request, denotes the names of the tablespace(s) to be backed up. Tablespace names are separated by commas. If there is no tablespace list specified, a full database backup is performed.
- `-u` *userid* Denotes the DB2 user ID used for backing up or restoring a DB2 database, tablespace, or recovery history file if it is different from the current login user ID.
- `-v` If set, all log messages will also be displayed on STDOUT.
- `-x` If specified, this option suppresses all confirmation requests. Otherwise, confirmation requests will be issued for restore commands that would overwrite existing data, and for delete requests.

  In conjunction with the "-c password" option, `-x` causes the password to be changed on all database partitions.

Backup Command (Backup Database Data)

With the Backup Object Manager backup command, you can backup a complete database or selected tablespaces of a database. (For a detailed description of the command options, refer to “Backup Object Manager Command Options” on page 126.)

- Backup the database data denoted by the command options:`backom -c b_db -a <database alias [-T` *tablespace list*`][-R <backup type>][-i` *instance*`] [-n` *node number*`] [-u` *userid*`][-p` *password*`] [-b` *buffer size*`][-B <number of buffers] [-S` *sessions*`][-P` *parallelism*`] [-e` *execution profile*`] [-O] [-L] [-v]`

Delete Commands (Remove Backup Objects from Tivoli Storage Manager)

The Backup Object Manager delete commands remove backup objects from Tivoli Storage Manager that were sent to Tivoli Storage Manager by Data Protection for SAP for DB2. (For a detailed description of the command options, refer to “Backup Object Manager Command Options” on page 126.)

- Delete the database backup(s) specified by the command options from Tivoli Storage Manager: `backom -c d_db -a <database alias> -t` *timestamp* `|` *time range*`[-i` *instance*`] [-n <node number>] [-e` *execution profile*`] [-x] [-v]`
- Delete the tablespace backup(s) specified by the command options from Tivoli Storage Manager: `backom -c d_ts -a` *database alias* `-t` *timestamp*`|`*time range* `[-i` *instance*`] [-n` *node number*`] [-e` *execution profile*`] [-x] [-v]`
- Delete the DB2 log file backup(s) specified by the command options from Tivoli Storage Manager: `backom -c d_log -a <database alias> -l` *log number*`|`*log number range*`[-n` *node number*`] [-t` *timestamp*`|`*time range*`] [-e` *execution profile*`][-x] [-v]`
- Delete the file(s) specified by command option -f from Tivoli Storage Manager:`backom -c d_raw -f` *file name* `[ -e <execution profile>] [-x] [-v]`

Password Command (Verify and Save Tivoli Storage Manager Password)

The password command connects to the backup server, prompts for a new password, and verifies the password entered with the backup server. If the verification is successful, the new password is encrypted and stored in the Data Protection for SAP for DB2 configuration file. Successful password verification requires that the password entered must be the active password for the corresponding node on the Tivoli Storage Manager server. Issue this command to verify and save a Tivoli Storage Manager password:

```
backom -c password [-x] [-a DB2 alias name] [-n DB2 node number]
[-e execution profile]
```

Information regarding when to use the password command is provided in "7. Determine the Tivoli Storage Manager password method" on page 61.

Query Commands (List Backup Objects)

The query commands list backup objects that were sent to Tivoli Storage Manager by Data Protection for SAP for DB2. The objects to be displayed can be filtered by using appropriate command options (see also "Backup Object Manager Command Options" on page 126).

- List all backup objects related to DB2 (database or tablespace backups and DB2 log file backups):`backom -c q_all [-i instance] [-a database alias]  [-n <node number>] [-t timestamp | time range] [-l <log number | log number range>][-e execution profile] [-m <output mode>] [-v]`
- List database backups:`backom -c q_db [-i instance] [-a database alias] [-n node number] [-t <timestamp | time range>] [-e execution profile] [-m output mode] [-v]`
- List tablespace backups:`backom -c q_ts [-i instance] [-a database alias] [-n <node number>] [-t timestamp | time range] [-e <execution profile>] [-m output mode] [-v]`
- List tablespace definition information (TDI) images related to a full DB2 database backup:`backom -c q_tdi -a <database alias> -t <timestamp [-i instance][-n node number] [-e execution profile] [-m output mode] [-v]`
- List DB2 log file backups: `backom -c q_log [-a <database alias>] [-n node number] [-t timestamp | time range] [-l log number | log number range] [-e execution profile] [-m output mode] [-v]`
- List backup objects available on Tivoli Storage Manager (database or tablespace backups, DB2 log file backups, and file backups): `backom -c q_raw [-f <file name>] [-e execution profile][-m output mode] [-v]`

Restore Commands (Restore Backup Objects)

With the Backup Object Manager restore commands, you can restore any backup object that was created by Data Protection for SAP for DB2. (For a detailed description of the command options, refer to "Backup Object Manager Command Options" on page 126.)

- Restore the database denoted by the command options:backom -c r_db -a *database alias* [-n *node number*] [-u *userid*][-p *password*] [-t *timestamp*] [-b *buffer size*] [-B <number of buffers>] [-S *sessions*] [-P *parallelism*] [-R <restore type>] [-O][-e *execution profile*] [-x] [-v]
- Restore the database denoted by the command options to a different location (redirected restore) in automatic mode: backom -c rr_db_clone -a <original database alias>,*target database alias* [-i *instance*] [-n <node number] [-u *userid*] [-p *password*][-t *timestamp*] [-b <buffer size>] [-B *number of buffers*] [-S *sessions*] [-P *parallelism*][-D <target database directory>][-e *execution profile*] [-s <scaling factor>] [-N] [-C] [-v]For a detailed discussion of the redirected restore function read "DB2 Redirected Restore Using Backup Object Manager" on page 84.
- Restore the database denoted by the command options to a different location (redirected restore) in batch mode:backom -c rr_db_batch -a <original database alias>,*target database alias* -f *TDI image* [-i *instance*] [-n *node number*] [-u *userid*][-p *password*] [-t *timestamp*][-b <buffer size>][-B *number of buffers*] [-S *sessions*] [-P *parallelism*][-D <target database directory>][-e *execution profile*][-s <scaling factor>] [-N][-C] [-v] For a detailed discussion of the redirected restore function read "DB2 Redirected Restore Using Backup Object Manager" on page 84.
- Restore the database denoted by the command options to a different location (redirected restore) in interactive mode:backom -c rr_db_interactive -a *original database alias*,*target database alias* [-i *instance*] [-n *node number*] [-u *userid*] [-p <password][-t *timestamp*] [-f <modified TDI image] [-b *buffer size*][-B *number of buffers*] [-S *sessions*][-P *parallelism*][-D <target database] [-e *execution profile*] [-s *scaling factor*][-N][-C] [-v] For a detailed discussion of the redirected restore function read "DB2 Redirected Restore Using Backup Object Manager" on page 84.
- Restore the tablespaces denoted by the command options: backom -c r_ts -a *database alias* [-n *node number*] [-u *userid*][-p *password*] [-t *timestamp*] [-b *buffer size*] [-B <number of buffers>] [-S *sessions*] [-P *parallelism*] [-R <restore type] [-O][-e *execution profile*] [-x] [-v]
- Restore the DB2 Recovery History File of the database denoted by the command options: backom -c r_hfile -a *database alias* [-n *node number*][-t *timestamp*] [-u *userid*] [-p *password*] [-b *buffer size*][-B <number of buffers>] [-S *sessions*] [-P *parallelism*][-e <execution profile>] [-x] [-v]
- Restore the tablespace definition information (TDI) denoted by the command options:backom -c r_tdi -t *timestamp* -a *database alias* [-d *destination directory*] [-e <execution profile>] [-x] [-v]
- Retrieve the DB2 log files denoted by the command options:backom -c r_log -a *database alias* -l *log number|log number range* -d *destination directory* [-n *node number*] [-t <timestamp|time range>] [-e *execution profile*] [-x] [-v]

- Retrieve the file(s) specified by command option -f to the path specified by command option -d:`backom -c r_raw -f <file name> -d` *`destination directory`* `[-e` *`execution profile`*`] [-x] [-v]`

BACKOM command examples

These examples show which commands can be used to perform certain tasks:

- Issue the following command to verify and save a Tivoli Storage Manager password:

```
backom -c password
```

- Issue the following command to create a list of all available backup objects sent to Tivoli Storage Manager by Data Protection for SAP for DB2:

```
backom -c q_all
```

- Issue the following command to create a list of all DB2 log files for database SAMPLE, with a log number greater than 123, and created in November 2002, with normal output detail level:

```
backom -c q_log -a SAMPLE -l 124-9999999 -t 200211* -m normal
backom -c q_log -a SAMPLE -l S0000124.log-S9999999.log -t 200211* -m normal
```

- Issue the following command to create a list of DB2 log files for log chains 5 to 15 for database SAMPLE with log numbers from 98 to 180, archived between 4 p.m. and 8.30 p.m.:

```
backom -c q_log -a SAMPLE -k C0000005-C0000015 -l 98-180 -t ????????16*-????????2030*
```

- Issue the following command to create a list of all tablespace backups for partition NODE0001, of database SAMPLE, that were created in November 2002 between 4 p.m. and 5 p.m.:

```
backom -c q_ts -a SAMPLE -n NODE0001 -t 200211??16*
```

- Issue the following command to backup online database SAMPLE using two I/O sessions and four backup buffers:

```
backom -c b_db -a SAMPLE -S 2 -B 4 -O
```

- Issue the following command to backup the tablespaces SYSCATSPACE and USERSPACE1 of database SAMPLE, using the execution profile 'initSAMPLE.utl' located at `/db2/SAMPLE/config`:

```
backom -c b_db -a SAMPLE -T SYSCATSPACE,USERSPACE1 -e /db2/SAMPLE/config/initSAMPLE.utl
```

- Issue the following command to restore a tablespace of database SAMPLE with the tablespace backup created on November 27, 2002, at 6:32:15 p.m.:

```
backom -c r_ts -a SAMPLE -t 20021127183215
```

- Issue the following command to restore database SAMPLE with the latest backup:

```
backom -c r_db -a SAMPLE
```

- Issue the following command to delete all DB2 log files for database SAMPLE that were created before June 2002:

```
backom -c d_log -a SAMPLE -t 1900*-20020601000000
```

- Issue the following command to delete all versions of files containing "tmp" in their path or file names that were sent to Tivoli Storage Manager by Data Protection for SAP:

```
backom -c d_raw -f *tmp*
```

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 DB2 `backup` 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 - db2c21 -c "/db2/C21/sapscripts/backup.ksh"
```

The content of `backup.ksh` is available in “Full Offline Backup Shell Script Sample” on page 71.

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 backup/archive commands
# and TSM 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 (alias) of the DB2 database
# is assumed to be 'C21' and the username 'db2c21'.
#
# ---------------------------------------------------------------------------
# Full database backup, scheduled every Friday at 8:00 p.m.
#
0  20    * * 5
#    /usr/bin/su - db2c21 -c "/db2/C21/sqllib/scripts/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 - db2c21 -c "/db2/C21/sqllib/scripts/archive.ksh"
```

The Data Protection for SAP for DB2 Profile

The Data Protection for SAP for DB2 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.

The profile is copied to the profile path (during installation) if no other profile exists there. Data Protection for SAP reads the profile pointed to by environment variable XINT_PROFILE (shared library, BackOM) or sent as a parameter (BackOM) immediately prior to a backup or restore operation.

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.
- Additional profile information is provided in “Enable ProLE to access configuration files on a remote share” on page 29.

Data Protection for SAP for DB2 profile parameter descriptions

The default value is underlined in these descriptions and applies if the parameter is not specified.

ADSMNODE *node_name*
: Specifies a *node_name* 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 DB2 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 DB2 after the backup function completed and before program control is returned to DB2. If *pgmname* is not a fully qualified path, the default search path is used to locate 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. If not specified, the default value is SAP___.All partitions of a partitioned DB2 database should have the same BACKUPIDPREFIX.

BRARCHIVEMGTCLASS *management_class [management_class...]*
: Specifies the Tivoli Storage Manager management class(es) that Data Protection for SAP uses to back up offline DB2 log files. 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 log file copies (keyword REDOLOG_COPIES on page "Data Protection for SAP for DB2 profile parameter descriptions." This parameter must be defined in conjunction with the respective SERVER statement, as shown in the sample profile.

To use different Tivoli Storage Manager 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 to back up the DB2 database. 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 when communicating with DB2. 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 sessions (keyword SESSIONS). By activating RL_COMPRESSION, the number of buffers is doubled.

CONFIG_FILE *path/SID>.bki*

Specifies the configuration file `initSID.bki` for Data Protection for SAP to store all variable parameters such as passwords and the date of the last password change. During processing, the string `%DB2NODE` is replaced automatically by the current DB2 node of a partitioned database or by 'NODE0000' otherwise. 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.

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*

Specifies the maximum number of parallel Tivoli Storage Manager client sessions that Data Protection for SAP establishes 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.

MAX_VERSIONS *n*|**0**

The *n* value defines the maximum number of database backup versions to be kept in backup storage. The default setting for this value is 0, meaning that backup version control is disabled. Every time a full backup completes successfully, the version count is increased by an increment of 1 and stored in the Data Protection for SAP configuration file. This value is also assigned to the tablespace files and to all subsequent DB2 log file backups. If the number of versions kept in backup storage is larger than the specified maximum number of backup versions (stored by the parameter *MAX_VERSIONS*), the oldest version is deleted, together with the corresponding tablespace, incremental and log file backups until only the specified maximum number of most recent versions remain. For partitioned DB2 databases, backup version control is done on a partition basis. Therefore, full backups should always be initiated for all partitions at the same time, for example by the DB2 script `db2_all`. For details on the `db2_all` script, see your DB2 documentation. 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 Tivoli Storage Manager 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.
- Every database partition needs its own configuration file. Partitions of a partitioned database should have the same BACKUPIDPREFIX.

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 60.

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 DB2 log file. The valid range is from 1 to 9. If not specified, Data Protection for SAP stores one copy of each log file. The number of different management classes for archived logs (keyword BRARCHIVEMGTCLASS specified must be greater than or equal to the number of log file copies specified. The number of different management classes specified must be greater than or equal to the number of log file copies specified.

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 was started. The offline log files are not compressed.

SEGMENTSIZE *size***[GB|TB]**

This keyword specifies the maximum size of the segments that are split from large backup objects. The required *size* value must be a positive integer equal to or greater than 1. Consider these characteristics when specifying this parameter:

- The scale units (GB or TB) are not required. GB is the default value.
- When specifying the scale units (GB or TB), you can use lower case letters, upper case letters, or a combination of both cases. However, you cannot specify single-character abbreviations (G or T).
- When this parameter is not specified, one backup object per DB2 backup session is transferred to Tivoli Storage Manager.
- If the specified segment size is less than the DB2 block size specified during the backup, the specified segment size is ignored at runtime. The specified DB2 backup block size is used instead.

The following example sets the maximum size of the backup objects segments on Tivoli Storage Manager to 100 GB:

```
SEGMENTSIZE   100 GB
```

You can also specify the command in the following way:

```
SEGMENTSIZE   100
```

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 Tivoli Storage Manager 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.

TCP_ADDRESSIP *address of server*

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. This parameter 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. The valid range is 4096 (4MB) to unlimited. 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. This parameter must be defined in conjunction with the respective SERVER statement, as shown in "Example of SERVER statement with alternate servers" on page 42. The parameter USE_AT has no effect on actions other than backup.

Sample Data Protection for SAP for DB2 Profile for UNIX or Linux

The sample profile (`initSID.utl`) is included in the Data Protection for SAP for DB2 installation package. Although the UNIX, Linux, and Windows versions are similar, all example versions are provided.

```
#-------------------------------------------------------------------------
#
# Data Protection for SAP (R) interface for DB2 UDB
#
# Sample profile for Data Protection for SAP (R) Version 6.2
#
#-------------------------------------------------------------------------
#
# 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 is stored in the description field of
# the Tivoli Storage Manager archive function.
# Maximum 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 backup copies of the DB2 log files.
# The valid range of REDOLOG_COPIES is from 1 to 9.
# Default: 1.
#--------------------------------------------------------------------------
#REDOLOG_COPIES  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
# only activated if the parameter MAX_VERSION 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


#--------------------------------------------------------------------------
# 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                 # NO is default


#--------------------------------------------------------------------------
# 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
#TRACEFILE           /db2/C21/sqllib/log/tdpr3.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          /db2/C21/sqllib/%DB2NODE/initSID.bki


#--------------------------------------------------------------------------
# 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


#*************************************************************************
# 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 DB2 Profile for Windows

```
#--------------------------------------------------------------------------
#
# Data Protection for SAP (R) interface for DB2 UDB
#
# Sample profile for Data Protection for SAP (R)
# Version 6.2 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 is used for communication with the
# SAP® 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 backup copies of the DB2 log files.
# The valid range of REDOLOG_COPIES is from 1 to 9.
# Default: 1.
```

```
#--------------------------------------------------------------------------
#REDOLOG_COPIES  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 parameter MAX_VERSION is not 0.
# The valid range of MAX_VERSIONS is from 0 to 9999.
# Default: 0
#--------------------------------------------------------------------------
#MAX_VERSIONS  4


#--------------------------------------------------------------------------
# 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


#--------------------------------------------------------------------------
# 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
#TRACEFILE              c:\sqllib\tdp_r3\log\tdpr3.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          c:\sqllib\tdp_r3\%DB2NODE\initSID.bki


#--------------------------------------------------------------------------
# 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


#**************************************************************************
# 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

sqlSQL statement/sqldescription ... /param
sqlSQL statement/sqldescription ... /param
...
```

As an aid to explaining the entry structure, it is shown in the following with each tag set in a separate line:

```
sqlSQL statement/sql
descriptionDescription of the SQL statement/description
programid0/programid
actionid0/actionid
displaygroup1,3/displaygroup
backuptype2/backuptype
executionmode0/executionmode
paramparameter-value1/param
paramparameter-value2/param
...
paramparameter-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

Table 12. Contents of the Custom SQL File (continued)

Tag	Definition
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
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)

Table 13. Tags for Defining Thresholds in the Custom SQL File (continued)

Tag	Value
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
#
sqlselect * from AdminAssistant.tsmrun where amount > 500000000000/sql
descriptionAmount over 500 GB/description
programid0/programid
actionid0/actionid
displaygroup1/displaygroup
backuptype2/backuptype
executionmode0/executionmode
paramemailAdress@email.com/param
#
```

Data Protection for SAP for DB2 files and samples

Use these file samples to assist with Data Protection for SAP for DB2 operations.

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 DB2 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 DB2
#
# 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 DB2 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 DB2
#
# 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

```
************************************************************************
* Tivoli Storage Manager                                               *
*                                                                      *
* Sample Client User Options file for Unix platforms                   *
************************************************************************

SErvername       server_a
Replace          On
Tapeprompt       No
DOM              /usr/sap /sapmnt/C21 /usr/sap/trans /db2/C21
```

Client User Options File Sample (dsm.opt) Windows

Data Protection for SAP for DB2 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 UNIX 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. Consequently, you can exclude at least the following
*       directories:
*
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 DB2 backup techniques and the SAP utility brarchive.
*
exclude /db2/C21/log_archive/C21/*
* exclude /db2/C21/sapreorg/.../* (There may be important scripts
*                                   located, check it out and decide.)
exclude /db2/C21/sapdata*/.../*
exclude /db2/C21/sapraw*/.../*
* ----------------------------------------------------------------------------
*
* With the above include/exclude list we implicitly include everything not
* excluded above. Especially for DP for SAP, this means including:
*      /sapmnt/C21     > 300 MB
*      /usr/sap        >  50 MB
*      /db2/C21        > 200 MB
* and UNIX related     > 350 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 DB2 from routine Tivoli Storage Manager incremental backups. Typically, such files are Windows system files and DB2 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 DB2 database is done by
* Data Protection for SAP(R) and not by Tivoli Storage
* Manager command-line backup client, the DB2 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 DB2 database files:
*
Exclude *:\db2\C21\log_archive\C21\...\*
Exclude *:\db2\C21\sapreorg\...\*
Exclude *:\db2\C21\sapdata*\...\*
```

Client Options Files Sample (*server*.opt)

Data Protection for SAP for DB2 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
COMPression        OFF
*NODEname           C21
TCPPort            1500
TCPServeraddress   xxx.xxx.xxx.xxx
PASSWORDACCESS     PROMPT
TCPBUFFSIZE        31
TCPWINDOWSIZE      32
```

Sample DB2 Vendor Environment File

A DB2 vendor environment file (`vendor.env`) is created from the information entered in the installation dialog panels during installation. A sample DB2 vendor environment file is included in the Data Protection for SAP for DB2 installation package.

Note

Ensure that there are no blanks within the paths specified for the vendor-specific environment variables of the vendor environment file. DB2 is currently unable to handle embedded blanks. Note that in the case of a standard Windows installation, the Data Protection for SAP profile is located at

`c:\Program Files\Tivoli\tsm\tdp_r3\db264\initSID.utl`

Sample DB2 vendor environment file for UNIX or Linux:

```
XINT_PROFILE=/db2/C21/tdpr3/initC21.utl
TDP_DIR=/db2/C21/tdpr3/tdplog
BACKOM_LOCATION=/usr/tivoli/tsm/tdp_r3/db264/backom
```

Sample DB2 vendor environment file for Windows:

```
XINT_PROFILE=c:\db2\C21\tdpr3\initC21.utl
TDP_DIR=c:\db2\C21\tdpr3\tdplog
BACKOM_LOCATION=c:\tivoli\tsm\tdp_r3\db264\backom.exe
```

Data Protection for SAP for DB2 planning sheets

Uses these planning sheets to assist with installing and configuring Data Protection for SAP for DB2.

Data Protection for SAP for DB2 (base product) planning sheet

Collect the information in this planning sheet before installing Data Protection for SAP for DB2. This table is also provided in file form as `planning_sheet_db2` for UNIX and Linux and `planning_sheet_db2.txt` for Windows.

Table 14. Installation Parameters for Data Protection for SAP

UNIX or Linux	Windows	Installation Parameter
X	X	DB2 database SID:
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 61.
X	X	Tivoli Storage Manager management classes for database and log file backups. Management classes configured for the database backup and for the backup of log files. For details, refer to "4. Define a policy" on page 60. Default: MDB for database backups, MLOG1 and MLOG2 for log file 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\db264

Table 14. Installation Parameters for Data Protection for SAP (continued)

UNIX or Linux	Windows	Installation Parameter
X	X	Options: • Use of the Administration Assistant (see "Administration Assistant function for Data Protection for SAP" on page 9 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. • Use of DB2 Log Manager for log archiving.

Administration Assistant function for Data Protection for SAP planning sheet

Collect the information in this planning sheet before installing 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 DB2 (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 (DB2) 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 DB2 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 DB2 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.

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* .

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.

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.

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

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.

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`

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.

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.

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.

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: The backup library 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.

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.

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 subsequent 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.

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.

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.

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.

BKI8301E *Product_name***: Exception caught in function** *function_name***. Error information: '***error_information***'**

Explanation: The named product implementing the DB2 Advanced Copy Services API received an error in the named API function. The error information is shown.

User response: Analyze the error information to find the cause of the problem. Resolve any problems indicated.

BKI8302E *Product_name***: Exception caught in function** *function_name***. More information may be available in file** *log_file_name***. Error information: '** *error_information***''**

Explanation: The named product implementing the DB2 Advanced Copy Services API received an error in the named API function. The error information is shown.

User response: Analyze the error information and the appropriate log files to find the cause of the problem. Resolve any problems indicated.

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.

BKI8305E Invalid option *option* **in options string: '***options_string***'.**

Explanation: An invalid option was found while parsing the options string specified in the 'db2' command.

User response: Correct the command and try again.

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.

BKI8313E *Product_name*: interface problem in function *function_name*: Invalid value of *parameter: value*

Explanation: The named product detected an interface problem in the named API function. An invalid value was found for *parameter* in one of the API data structures.

User response: Contact your IBM support personnel.

BKI8314E *Product_name*: interface problem in function *function_name*: The session is already in use by a different operation.

Explanation: The named product detected an interface problem in the named API function. Either the session handle is used for various operations simultaneously, or the functions are called in an order not supported by the current version of the library.

User response: Contact your IBM support personnel.

BKI8315E *Function_name*: The following object is not under the control of *product_name*: *path*

Explanation: The named product implementing the DB2 Advanced Copy Services API detected a problem in the named API function: The path passed by the database is not under the control of the product.

User response: Make sure the database to be backed up meets the requirements for employing snapshot backups.

BKI8316E *Product_name*: interface problem in function *function_name*: Empty group list passed by DB2.

Explanation: The named product detected an interface problem in the named API function: The database passed a group list containing no elements.

User response: Contact your IBM support personnel.

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.

BKI8318E *Product_name*: interface problem in function *function_name*: Not enough space provided to write meta data.

Explanation: The named product detected an interface problem in the named API function: The buffer provided by the database is too small to contain the requested meta data.

User response: Contact your IBM support personnel.

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.

BKI8323E *Product_name***: Problem occurred while processing** *function_name***. Please check log file** *log_file_name* **for more information. Error information: '***error_information***'**

Explanation: The named product implementing the DB2 Advanced Copy Services API received an error in the named API function. The error information is shown.

User response: Analyze the error information and the appropriate log files to find the cause of the problem. Resolve any problems indicated.

BKI8324E *Product_name***: Problem occurred while processing** *function_name***: Device agent returned code** *return_information***.**

Explanation: The named product implementing the DB2 Advanced Copy Services API received an error from the device agent in the named API function. The device agent's return information is given.

User response: Check the appropriate log files to find the cause of the problem. Resolve any problems indicated.

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.

BKI8344E **Path** *path* **is listed more than once for partitioning.**

Explanation: This is a DB2 - TSM interface problem.

User response: Contact your IBM support personnel.

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.

BKI8511I **The command is:** *command name***.**

Explanation: This is an information message echoing the command.

User response: None.

BKI8512I **Return code is:** *return code***.**

Explanation: This message shows the return code of the Backup Object Manager.

Valid return codes:

0	The requested action was performed successfully.
1	The requested action was performed successfully; however, some warnings were issued.
2 or greater	The requested action could not be performed due to errors. In this case, an error message should be logged, too.

User response: None if the return code is 0.

If the return code is greater than 0, analyze the error and/or warning messages. Resolve errors before starting the action again.

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.

BKI8514W **'TDP_DIR' is not set correctly. The temporary path will be used.**

Explanation: The variable TDP_DIR is set but contains an invalid path. All run logs will be written to the machines temporary directory instead.

User response: Check and reset the environment variable TDP_DIR.

BKI8520E **No command was specified.**

Explanation: `backom` was called without a command line.

User response: Check the command syntax and correct the call.

BKI8521E **Command option** *command option* **requires an argument.**

Explanation: A command option requiring an argument was specified without an argument.

User response: Check the command syntax and correct the call.

BKI8522E **Invalid command** *command***.**

Explanation: backom was called with an invalid command.

User response: Check the command syntax and correct the call.

BKI8523E **Error during** *action***.**

Explanation: An error occurred while performing the named action.

User response: Look for other error messages in order to analyze the problem.

BKI8524E **Table space online restore is not allowed.**

Explanation: Either the database setup or the kind of backup prevents an online table space backup.

User response: If you need to do a table space restore it must be done offline.

BKI8525E The DB2 instance name can consist of at most 8 characters.

Explanation: The name given for the DB2 instance does not comply with the DB2 naming conventions.

User response: Correct the DB2 instance name.

BKI8526E The DB2 database alias can consist of at most 8 characters.

Explanation: The name given for the DB2 alias does not comply with the DB2 naming conventions.

User response: Correct the DB2 alias name.

BKI8527E Invalid node. Specify it in the format ***node format*****.**

Explanation: The name given for the DB2 node does not comply with the DB2 naming conventions. Node numbers must be specified in the displayed format, for example 'NODE0000' or '0000'.

User response: Correct the DB2 node number.

BKI8528E Invalid timestamp. It must consist of 14 digits with format yyyymmddhhmmss or digits and wildcards * or ?.

Explanation: Specify digits in the format 'yyyymmddhhmmss' or mixed with wildcards '*' or '?'.

where:

- yyyy is the year, specified as four digits,
- mm is the month, specified as two digits, with leading zero for the months January to September,
- dd is the day of the month, specified as two digits, with leading zero for days 1 to 9,
- hh is the hour of the day, 00 to 23, with leading zero for hours 0 to 9,
- mm is the minutes of the hour, 00 to 59, with leading zero for minutes 0 to 9,
- ss is the second of the minute, 00, to 59, with leading zero for seconds 0 to 9.

Any digits can be replaced by wildcards '*' or '?', where

- * means any number of any digits,
- *?* means exactly one digit of any value.

User response: Correct the timestamp.

BKI8529E Invalid log sequence number. Specify it in the format ***log sequence format*****.**

Explanation: The information on the log sequence number(s) does not comply with the expected format. Accepted log sequence numbers are for example '123' or 'S0000123.LOG'.

User response: Correct the log sequence number(s).

BKI8530E Profile ***file name*** **does not exist or cannot be accessed.**

Explanation: Either an existing file could not be opened, or a file could not be created.

User response: Check the attributes of the file and/or its directory. For backup processing, read access is required for the files to be backed up. For restore processing, write access is required for the target location of the files to be restored.

BKI8531E Directory ***file path*** **does not exist or cannot be accessed.**

Explanation: A file path cannot be accessed.

User response: Check the attributes of the file and/or its directory. For backup processing, read access is required for the files to be backed up. For restore processing, write access is required for the target location of the files to be restored.

BKI8532E Invalid log chain number. Specify it in the format ***log chain format*****.**

Explanation: The information on the log chain number(s) does not comply with the expected format. Accepted log chain number(s) are for example '123' or 'C0000123'. *file path*

User response: Correct the log chain number(s).

BKI8533E A timestamp range is not allowed for the command ***command*** **.**

Explanation: A timestamp range is not allowed for command `restore database`, `restore tablespace`, `restore tablespace online` and `restore DB2 history file`. Only a single timestamp argument can be used.

User response: Correct the timestamp command option.

BKI8534E Command option ***command option*** **is missing.**

Explanation: A command was issued without specifying a required command option.

User response: Check the command syntax and correct the call.

BKI8535E Invalid output mode. Specify one of the keywords ***keyword list*****.**

Explanation: Only the listed keyword values are allowed with the output mode command option `-m`.

User response: Correct the output mode command option.

BKI8536E **Wildcard characters are not allowed for command** *command***.**

Explanation: For the BackOM commands 'restore database', 'restore tablespace', 'restore tablespace online' and 'restore DB2 history file' it's not allowed to specify the wildcard characters '*' and '?' in a timestamp command option.

User response: Correct the timestamp command option.

BKI8537E **The path** *path* **is not absolute.**

Explanation: A command line argument requires a fully qualified path which was not given.

User response: Specify the fully qualified path.

BKI8538E **The TDI** *file name* **cannot be processed.**

Explanation: The TDI file could not be parsed because of errors. There are more specific parser error messages before this message occurs.

User response: Check for and respond to preceding error messages in the Backup Object Manager log.

BKI8540I **Using** *component_name* **at** *host name***:***port number***.**

Explanation: The *component_name* service named is used for the current action.

User response: None.

BKI8541I **Using profile** *profile path***.**

Explanation: The profile named is used for the current action.

User response: None.

BKI8542E **Profile** *profile path* **cannot be read.**

Explanation: The Backup Object Manager tried to use the profile named but the profile was not available or could not be read. The location of the profile is specified via command line as argument to option '-e' or in environment variable 'XINT_PROFILE'.

User response: Make sure that the profile is available at the location specified in option '-e' on the command line or in environment variable 'XINT_PROFILE'.

Check the attributes of the profile and the corresponding directory and make sure that the file can be accessed.

BKI8543I **Querying TSM for file(s)** *file list***.**

Explanation: The Backup Object Manager checks if the files listed are available on the TSM server(s) specified in the corresponding profile.

User response: None.

BKI8545I **No** *image type* **image(s) found.**

Explanation: A request could not be satisfied because the files to be processed are not available on the TSM server.

User response: Check if the file(s) were specified correctly in the request.

BKI8546E **Environment variable** *environment variable* **is not set or not set correctly.**

Explanation: A required environment variable is not set at all or has a value that is not allowed.

User response: Check the documentation for the appropriate values of the environment variable named and set its value accordingly.

BKI8548I **Elapsed time:** *time value***.**

Explanation: After restore and delete, the time elapsed during the action is displayed.

User response: None.

BKI8549E **Unable to create file** *file name***.**

Explanation: During restore, the file to be restored cannot be created in the target location.

User response: Check if there is sufficient space available for the file to be restored.

Check the attributes of the target directory; write access is required.

If the target file already exists, check that write access is granted

BKI8550W **Environment variable** *environment variable* **for output mode has wrong value. Using default.**

Explanation: The default output mode can be overridden by the named environment variable. Accepted values are "short", "normal", or "detailed". The system default is "short" for actions on DB2 log files, "normal" otherwise.

User response: Specify an appropriate value for the environment variable named, or remove the environment variable.

BKI8551E Not all data written to *file path*.

Explanation: Restoring raw or DB2 log file data ended before all data retrieved from TSM could be written to the file named.

The file is incomplete.

User response: Make sure there is sufficient space for the data to be restored.

BKI8552E File *file path* could not be closed.

Explanation: After restoring raw or DB2 log file data, the target file could not be closed.

User response: Retry the action.

BKI8555E Variable 'DB2DBDFT' or command option 'alias' is required.

Explanation: The password command needs the name/alias of the database, for which the Data Protection for SAP configuration file has to be adapted.

User response: Either set the environment variable DB2DBDFT or provide the command option 'alias' with the password command and try again.

BKI8556E Unable to get hostname.

Explanation: The machines hostname could not be determined.

User response: Check the TCP/IP configuration of the machine.

BKI8557E The config file *file name* could not be created.

Explanation: Data Protection for SAP tries to create the configuration file named if it is not present at the location specified by the Data Protection for SAP profile keyword CONFIG_FILE. However, the file cannot be created. This may either be caused by an incorrect path specified by keyword CONFIG_FILE, or the user may not have the appropriate permissions for creating the file.

User response: Make sure the path specified by keyword CONFIG_FILE is correct and the permissions are set appropriately.

BKI8558I Setting TSM password for partition *partition number* on host *host name*.

Explanation: The Data Protection for SAP TSM password is set on the host named for the DB2 partition indicated.

User response: None.

BKI8559W For partition *partition number* switch to host *host name* and issue the command again.

Explanation: When verifying the TSM password, the Data Protection for SAP configuration file is modified.

If the Data Protection for SAP profile keyword CONFIG_FILE points to an NFS mounted (UNIX or Linux) or a shared (Windows) path accessible to all hosts in a DB2 ESE (EEE) environment, for example the instance home, all configuration files of the various partitions can be modified simultaneously. If, in contrast, keyword CONFIG_FILE points to a local path, only the configuration files of the local partitions can be modified. In this case, the password verification needs to be done from each host. The message indicates the partitions whose associated configuration files are not accessible. In order to avoid this administrative overhead, it is recommended to place the Data Protection for SAP configuration files in a file system shared by all hosts hosting a partition of the database.

User response: Make sure to verify the TSM password(s) for all partitions of the database.

BKI8560E Partition *partition number* not found in the database configuration.

Explanation: The DB2 partition specified could not be found in the database configuration.

User response: Check the configuration of the DB2 ESE(EEE) environment (`db2nodes.cfg`, environment variable DB2NODE) and try again.

BKI8561W Database 'alias' not listed in the system database directory.

Explanation: The database 'alias' does not exist. Because there is a dependency between the alias and the settings for Data Protection for SAP there might be problems during database backup or restore runs. Nevertheless, the Data Protection for SAP configuration file (init<alias>.utl) will be created and adapted.

User response: Check if the alias specified does match to an entry in the DB2 system database directory. Further, check the argument for the Data Protection for SAP profile keyword CONFIG_FILE and if necessary adapt it appropriately.

BKI8584I Delete command completed successfully.

Explanation: The object(s) specified with the delete command were successfully deleted from the TSM server.

User response: None.

BKI8585W Delete command completed successfully, but had warning(s).

Explanation: The object(s) specified with the delete command were deleted with warning(s) from the TSM server.

User response: Check the Backup Object Manager log file for further detailed messages and if required, do the requested interventions manually.

BKI8586I Delete command was aborted.

Explanation: The delete command was aborted by the user. No object(s) were deleted from the TSM server.

User response: None

BKI8587E Delete command failed due to an error.

Explanation: The delete command failed during execution. Not all objects were deleted from the TSM server.

User response: Check the Backup Object Manager log file for further detailed messages and try to resolve the error which led to the delete failure. Retry the action. If the error still exists, contact the IBM Support.

BKI8588E Delete command has not been started or no delete result information is available.

Explanation: This message indicates that an operation did not complete successfully. Typically, some other error condition was detected before.

User response: Contact the IBM Support.

BKI8589E Query command failed due to an error.

Explanation: The query command failed during execution. Not all queried objects can be displayed.

User response: Check for and respond to preceding error messages in the Backup Object Manager log. In the absence of preceding error messages, contact IBM Support.

BKI8610I Restoring *type* ...

Explanation: The restore of *type* has started.

User response: None.

BKI8612I Continuing restore ...

Explanation: The database restore continues.

User response: None.

BKI8613E Terminating restore ...

Explanation: An error occurred, and the database restore terminates.

User response: Check for and respond to preceding error messages in the Backup Object Manager and the shared library run logs. Additional information may be found in the DB2 diagnostic log (db2diag.log).

BKI8615I Restore command completed successfully.

Explanation: The object(s) specified with the restore command were successfully restored from the TSM server.

User response: None.

BKI8616W Restore command completed successfully. Warning(s) encountered.

Explanation: The object(s) specified with the restore command were restored with warning(s) from the TSM server.

User response: Check the Backup Object Manager log file for further detailed messages and if required, do the requested interventions manually.

BKI8617I Restore command was aborted.

Explanation: The restore command was aborted by the user. No object(s) were restored from the TSM server.

User response: None.

BKI8618E Restore command failed due to an error.

Explanation: The restore command failed during execution. Not all objects were restored from the TSM server.

User response: Check the Backup Object Manager log file for further detailed messages and try to resolve the error which led to the restore failure. Retry the action. If the error still exists, contact the IBM Support.

BKI8619E Restore command has not been started or no restore result information is available.

Explanation: This message indicates that an operation did not complete successfully. Typically, some other error condition was detected before.

User response: Check for and respond to preceding error messages in the Backup Object Manager log.

BKI8621I Restoring file *file name*...

Explanation: The system started restoring the file indicated.

User response: None.

BKI8622I Deleting *type* ...

Explanation: The deletion of *type* has started.

User response: None.

BKI8623I Deleting file *file name* ...

Explanation: The system started deleting the file indicated.

User response: None.

BKI8626W The TDI *file name* could not be deleted.

Explanation: The system tried to remove the TDI image from TSM, but did not succeed.

User response: Try to remove the image manually using the Backup Object Manager raw delete facility.

BKI8630E The command option *option* must be a number.

Explanation: An invalid argument was specified for command option *option*.

User response: Correct the command syntax.

BKI8631I Backup command completed successfully.

Explanation: The backup operation completed successfully; the backup image can be used for restoring. In the case of a full database backup, the TDI image was generated and stored to TSM, too.

User response: None.

BKI8632W Backup command completed successfully. Warning(s) encountered.

Explanation: The backup operation completed successfully; the backup image can be used for restoring. However, some problems occurred.

User response: Check the warning messages and take corrective actions if necessary.

BKI8633I Backup command was aborted.

Explanation: The backup operation was cancelled by user interaction. No backup image was created.

User response: None.

BKI8634E Backup command failed due to an error.

Explanation: No backup was made due to previous errors.

User response: Check for and respond to preceding error messages in the Backup Object Manager log.

BKI8635E The command option *option* must be a floating point number.

Explanation: An invalid argument was specified for command option *option*.

User response: Correct the command syntax.

BKI8636E The command option *option* must be one of *values*.

Explanation: An invalid argument was specified for command option *option*.

User response: Correct the command syntax.

BKI8637I *Type online/offline* backup of *alias* started ...

Explanation: A backup operation of database *alias* of type *type* has started.

User response: None.

BKI8638I *Type online/offline* backup of table space(s) *tablespace#1,...,tablespace#n* of *alias* started ...

Explanation: A backup operation of table space(s) *tablespace#1 ... tablespace#n* of database *alias* of type *type* was started.

User response: None.

BKI8639I Including log files in backup image ...

Explanation: The DB2 log files are stored as part of the backup image.

User response: None.

BKI8640I Using *number* buffers with a size of *size* ...

Explanation: For backup or restore operations, the indicated number of buffers of the size displayed are used.

User response: None.

BKI8641I Using *number* session(s) ...

Explanation: For backup or restore operations, the indicated number of TSM sessions is used.

User response: None.

BKI8642I **Using a degree of parallelism of** ***number*** **...**

Explanation: For backup or restore operations, the degree of parallelism is displayed.

User response: None.

BKI8643I **Using vendor library at** ***lib path*** **...**

Explanation: For backup or restore operations, the named vendor library is used.

User response: None.

BKI8644W **Offline backups cannot include log files. The option -L is being ignored.**

Explanation: An offline backup operation was started, requesting the DB2 log files to be included. This is not possible with an offline backup. The backup is done without including DB2 log files.

User response: Make sure to backup DB2 log files separately.

BKI8652I **Detected DB2 version** ***version*** **with** ***number*** **bits.**

Explanation: The indicated DB2 version was detected by Backup Object Manager.

User response: None

BKI8653I **Using autonomic buffer size and number of buffers ...**

Explanation: The buffer size and the number of buffers used for backup or restore is automatically determined by DB2.

User response: None

BKI8654I **Using an autonomic buffer size with** ***number*** **buffers ...**

Explanation: The buffer size used for backup and restore is automatically determined by DB2. The number of buffers to be used was specified in the call to the Backup Object Manager.

User response: None.

BKI8655I **Using an autonomic number of buffers with a size of** ***size*** **...**

Explanation: The number of buffers to be used for backup and restore are determined by DB2. The buffer size to be used was specified in the call to the Backup Object Manager.

User response: None.

BKI8656I **Using an autonomic degree of parallelism...**

Explanation: The number of DB2 processes (UNIX or Linux) or threads (Windows) used for reading or writing data from/to table space containers during backup and restore is determined by DB2.

User response: None.

BKI8657W ***Number*** **is not a valid partition number. Assuming partition 0.**

Explanation: The partition number specified in the call to Backup Object Manager does not denote a valid partition of the database. Therefore, the default partition 0 will be used by DB2 and by Backup Object Manager.

User response: If your database is not partitioned do not specify the partition number for further actions.

BKI8658E ***Number*** **is not a partition number of the database or does not denote a partition on this host.**

Explanation: The partition number specified does not denote a valid database partition or is not the partition located on the system where Backup Object Manager is called. Backup Object Manager can only operate on partitions residing on the same host.

User response: Either change *number* to a partition number of a local partition, or start Backup Object Manager from the same host where the partition resides.

BKI8659I **Creating table space definition information ...**

Explanation: The table space definition information (TDI) is being created in memory.

User response: None.

BKI8660I **Saving table space definition information ...**

Explanation: The table space definition information (TDI) is being stored on the TSM server.

User response: None.

BKI8661W **Could not create TDI. The backup cannot be used for redirected restore with BackOM.**

Explanation: The system could not collect the table space definition information. The backup was made without TDI. As a result, the backup can be used for restoring the system, but it cannot be used for restoring to a different location.

User response: Ensure that your database is enabled to accept CLI connections.

BKI8662W **Could not save TDI. The backup cannot be used for redirected restore with BackOM.**

Explanation: The system could not save the TDI on TSM. The backup was made without TDI. As a result, the backup can be used for restoring the system, but it cannot be used for restoring to a different location.

User response: Check for and respond to preceding error messages in the Backup Object Manager log.

BKI8663W **The TDI contains device containers. The backup cannot be used for redirected restore with BackOM.**

Explanation: A backup of a database using device containers was requested. The backup was successful, it can be used to restore the system, but it cannot be used for restoring to a different location. Restoring to a different location is not supported with device containers.

User response: None.

BKI8664E **Connecting to** *alias* **using CLI failed. The return code was** *return code*.

Explanation: The system tried to connect to the database named via the CLI. The operation did not succeed and returned the error code indicated.

User response: Ensure that your database is enabled to accept CLI connections.

BKI8665I **The backup timestamp is:** *timestamp*.

Explanation: The DB2 backup finished successfully with the timestamp *timestamp*.

User response: None.

BKI8666I **Redirecting table space** *table space* **with ID** *id*.

Explanation: The named table space is restored to the location requested.

User response: None.

BKI8667W **Table space** *tablespace* **with ID** *id* **was not redirected because its container on the source system** *SID* **is not located in a path starting with** *path* **.**

Explanation: The named table space of type SMS was not redirected because the definition of the table space container in the source system does not match the database characteristics that Backup Object Manager expects and that are cited in the message. Therefore, Backup Object Manager tries to restore the table space to a location identical to the location in the original system.

User response: Make sure that the table space mentioned can be restored to the original location. This requires that the user initiating the redirected restore has the appropriate permissions for placing the table space container in this location and that the table space can be restored without overwriting other data.

In order to avoid this situation in the future, the administrator of the source system may want to recreate the table space according to the database characteristics Backup Object Manager expects.

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.

BKI8690E Free space test for container *path* failed. Only *free bytes* MB free space left but *required bytes* MB required.

Explanation: The system requires a table space container of the size indicated at the path named, but there is not sufficient free space available to create it.

User response: Try to make available the free space required, for example by

1. Removing some files on the volume or file system the container is to reside on.
2. Increasing the size of the file system the container is toi reside on.
3. Shrinking the size of the container requested so that it fits in the free space.

Note: Backup Object Manager assumes that a small part (0.05%) of the free space will be required by the operating system for administrative use. As a consequence, only 99.95% of the free space on the volume or file system is actually available.

BKI8692E The requested data could not be retrieved.

Explanation: The TDI data of a backup image could not be retrieved and displayed.

User response: Look for and respond to preceding error messages.

BKI8693E More than one TDI file matches your query.

Explanation: More than one TDI file matching the search criteria was found on TSM.

User response: Specify additional BackOM command options to restrict the result set.

BKI8700E Internal parser error in TDI parser.

Explanation: An unexpected error occurred in the TDI parser.

User response: Contact IBM Support.

BKI8701E This parser cannot process TDI version *version*.

Explanation: The current version of Backup Object Manager is not compatible with the version the TDI image was created with. As a consequence, the TDI data cannot be processed.

User response: Check the release notes for the appropriate migration procedure.

BKI8702E Too many errors. Bailing out.

Explanation: The TDI parser encountered a number of errors. Restoring is stopped.

User response: Check for and respond to preceding error messages in the Backup Object Manager log.

BKI8703E Out of memory.

Explanation: The TDI parser encountered a token that cannot be read into the main memory. The TDI image cannot be processed, and restoring is stopped.

User response: Contact IBM Support.

BKI8704E Error while reading input file.

Explanation: The TDI parser tried to read more data from disk or from TSM, but did not succeed.

User response: Ensure that the TDI image to be processed exists at the expected location and that the system has sufficient privileges to read it.

BKI8705E *error* in line *line number*.

Explanation: The TDI parser encountered a syntax error in the line indicated. As a consequence, the TDI image cannot be analyzed.

User response: Respond to the error message and correct your TDI image.

BKI8706E The container at *path* is inappropriate for table space *tablespace*.

Explanation: The container at the location indicated cannot be added to the table space named because of incompatible properties.

User response: Check the properties of the container and the table space. Ensure that the IDs of the containers are unique for the table space named.

BKI8707E Missing statement *keyword* in block *block name* near line *line number*.

Explanation: A keyword is missing in the named block ending at the line given.

User response: Insert the required statement in the block.

BKI8708E The [TDI] header block must be the first block.

Explanation: The TDI image does not start with the required header ([TDI] block). Only comments or whitespace are allowed before this block.

User response: Ensure that the [TDI] block is the first block in the TDI image.

BKI8709E The required block *block name* is missing.

Explanation: The named block is missing in your TDI image.

User response: Insert the missing block using valid values.

BKI8710W Duplicate block *block name* ignored at line *line number*.

Explanation: At the line indicated, a block begins whose name was encountered before. The system ignores the duplicate block; it uses the data from the first occurrence of duplicate blocks.

User response: Make sure that block names are unique within a TDI image.

BKI8711W Duplicate statement *keyword* ignored in line *line number*.

Explanation: At the line indicated, a duplicate statement was encountered within a block. The system ignores the duplicate statement.

User response: Make sure to not specify duplicate statements within a block.

BKI8728E Could not attach to instance 'instance'.

Explanation: BackOM was not able to attach to the instance 'instance'.

User response: First, check the system environment for possible instance candidates. Try the action again by additionally specifying the BackOM command option '-i <instance name>'.

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.

BKI8730I Scaling table space containers to *number* percent ...

Explanation: All table space containers will be increased by the percentage indicated during the table space container redefinition step.

User response: None.

BKI8731I Normalizing table space containers ...

Explanation: All containers of a table space will be of the same size after redefinition.

User response: None.

BKI8732E The TDI used for redirected restore contains an invalid database alias.

Explanation: There is an invalid database alias specified in the *alias* statement of the TDI image.

User response: Provide a valid alias.

BKI8733E The TDI used for redirected restore contains an invalid instance name.

Explanation: There is an invalid database instance specified in the *instance* statement of the TDI image.

User response: Provide a valid instance name.

BKI8734E The TDI used for redirected restore contains an invalid partition number.

Explanation: There is an invalid partition number specified in the *Node* statement of the TDI image.

User response: Provide a valid partition number.

BKI8736E Table space *tablespace* must have at least one container.

Explanation: The TDI image defines the table space named without containers.

User response: Ensure that there is at least one container associated with every table space.

BKI8737E Table space *tablespace* has containers with the combined storage too small.

Explanation: The number of used pages of the table space named exceeds the combined size of its table space containers defined in the TDI image.

User response: Ensure that every table space has containers of a combined size that is sufficient to hold the used pages of the table space.

BKI8738E The container at *path* has a page size that is incompatible with its table space.

Explanation: The container indicated does not have the same page size as its table space according to the definitions in the TDI image.

User response: Contact IBM Support

BKI8739E The type of the container at *path* is incompatible with its table space.

Explanation: The container indicated cannot be used with its associated table space according to the definitions in the TDI image. SMS table spaces can only have path containers, and DMS table spaces must have file or device containers.

User response: Ensure that the appropriate types of containers are used with each table space

BKI8740E The path *path* of a container must not be relative.

Explanation: In the TDI image, the named path defining a container does not seem to be a fully qualified path.

User response: Ensure that all paths in your TDI are fully qualified

BKI8741E The container at *path* would overwrite existing files or directories.

Explanation: The TDI image contains the definition of the container indicated whose location is already in use. This is only allowed when restoring to the source database. Restoring to a different location is stopped.

User response: Ensure that all path containers defined in the TDI image point to non-existing paths and all file containers point to non-existing files

BKI8742E The container at *path* is a device container which is not supported.

Explanation: In the TDI image, a device container is defined. However, device containers are not supported by Backup Object Manager.

User response: Do not use device containers.

BKI8743I Local TDI check returned *return code*.

Explanation: The TDI with the target database table space definition was checked. If the return code given does not equal 0 errors occurred.

User response: In the case of a non-zero return code, contact IBM Support.

BKI8744I TDI replacement check returned *return code*.

Explanation: The system checked whether the table space definitions of the target TDI can replace the definitions of the source TDI. If the return code given does not equal 0 the table space definitions of the target TDI are not valid.

User response: In the case of a non-zero return code, contact IBM Support.

BKI8745E The TDI is invalid.

Explanation: The TDI with the target table space definitions is not valid. Restoring to a different location is stopped.

User response: Check the Backup Object Manager log for the return code of the validation. Check for and respond to preceding error messages in the Backup Object Manager log.

BKI8746I The TDI is valid.

Explanation: The TDI with the target table space definition is valid. Processing continues.

User response: None.

BKI8747E Not all table spaces of the original database are contained in the TDI.

Explanation: At least one table space of the original database is missing in the TDI definitions of the target database. However, a new location must be given for all table spaces of the original database. Therefore, restoring to a different location is stopped.

User response: Provide the information on the missing table spaces and their containers.

BKI8748E The TDI does not define enough storage to hold all the data of the original database.

Explanation: The target TDI has at least one table space whose containers are too small to hold the data of the source database.

User response: Increase the container size or add more containers to the table spaces.

BKI8749E The page size of a table space in the TDI does not match the one of the original database.

Explanation: The target TDI contains at least one table space with a matching ID in the source TDI, but their page sizes do not match.

User response: Ensure that table spaces have the same page sizes in both the source and the target TDI.

BKI8750E The number of used pages of a table space in the TDI does not match the one of the original database.

Explanation: The target TDI contains at least one table space with a matching ID in the source TDI, but the number of used pages of the target table space does not match the number of used pages in the original database.

User response: Ensure that the number of used pages of a table space is the same in both the source and the target TDI.

BKI8751E The table space type in the TDI does not match the one of the original database.

Explanation: The target TDI holds at least one table space with a matching ID in the source TDI, but the table space types are different.

User response: Ensure that the type of a table space is the same in both the source and the target TDI.

BKI8752E **BackOM does not support redirected restore with device containers.**

Explanation: The target TDI contains at least one definition of a device container. However, device containers are not supported by Backup Object Manager's redirected restore function.

User response: Do not use the Backup Object Manager's redirected restore facility for device containers.

BKI8753E **A container cannot be created at *path*.**

Explanation: Either the location where the table space container is to be created does not exist, or the permissions of the user are not sufficient.

User response: Check the location and the permissions.

BKI8755I **Getting reference TDI from TSM ...**

Explanation: Retrieving the appropriate TDI to be used by internal checking routines from the TSM server.

User response: None.

BKI8756W **Could not get reference TDI from TSM. No input validation is done.**

Explanation: The system could not find a TDI image matching the database backup to be restored on TSM. The restore action will be continued, but the input data cannot be validated before the restore starts.

User response: None.

BKI8757I **Performing redirected restore from *source alias* to *target alias*...**

Explanation: Redirected restore of *source alias* to *target alias* is starting.

User response: None

BKI8758E **The TDI does not contain data for table space *tablespace*.**

Explanation: A definition of the table space named is expected to be provided in the TDI, but could not be found.

User response: Ensure that all table spaces of the source database are also defined in the target TDI.

BKI8759E **Redirecting of at least one container failed.**

Explanation: The system tried to create the containers for a table space, but at least one of them could not be redirected to a different location. Usually, the location of one of the table space containers is not allowed. A list of containers the system tries to create can be found in the Backup Object Manager log. One of them failed.

User response: Check for and respond to further error messages in the Backup Object Manager log.

BKI8760E **Not all directories for the containers could be created.**

Explanation: The system tried to create the directories to place the containers in, but at least one failed.

User response: Ensure that the system has sufficient privileges to create the directories at the desired locations.

BKI8761E **The container at *path* does not have the minimum size of two extends.**

Explanation: A table space container to be created must have at least the size of two extends.

User response: Correct the size of the container to be created.

BKI8762I **Set table space container with ID *id* and name *tablespace_container*.**

Explanation: Backup Object Manager redirects a table space container to the ID and name indicated.

User response: None.

BKI8763E **The extent size of a table space in the TDI does not match the one of the original database.**

Explanation: The extend sizes of corresponding table spaces defined in the source and target TDIs must be equal. However, for at least one table space different extend sizes are defined in the source and target databases.

User response: Define matching extend sizes for corresponding table spaces.

BKI8765I **Testing redirected restore from *source alias* to *target alias* ...**

Explanation: The system is testing whether the original database can be restored to the target location. It checks whether

- the file system where the table space containers are to be created has sufficient free space. (If specified, normalizing and scaling are also considered.)

- there are existing files and directories identical to the containers defined for the target database. This would indicate that a database of same name and of same structure already exists, and data could be overridden.
- the structures of the source and target databases (table space types, page sizes, extend sizes) allow for a redirected restore.

User response: None.

BKI8766I Check successful. Redirected restore possible with these settings.

Explanation: The redirected restore test finished successfully. Thus, the redirected restore operation can be started with the options specified for the test run.

User response: None.

BKI8767W Warnings occurred.

Explanation: The redirected restore test detected one or more minor conflicts. These conflicts may or may not prevent a successful redirected restore operation. Nevertheless, it is recommended to resolve them.

User response: Check for and respond to preceding warning messages in the Backup Object Manager log.

BKI8768E Check failed. Redirected restore not possible with these settings.

Explanation: The redirected restore test detected one or more major errors which will prevent a successful redirected restore with these settings.

User response: Check for and respond to preceding error messages in the Backup Object Manager log.

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.

BKI8770I Getting TDI for redirected restore from TSM ...

Explanation: The system is retrieving the TDI image from the TSM server.

User response: None.

BKI8771E The TDI for the redirected restore could not be retrieved.

Explanation: The TDI image specified could not be found.

User response: Provide the correct location of the TDI image.

BKI8772E The selected database has a structure that prevents automatic cloning.

Explanation: You tried to clone an SAP database using redirected restore, but the database does not have the default directory structure of an SAP database. The cloning facility of Backup Object Manager redirected restore cannot be used for this system.

User response: You may use either the interactive or the batch mode of Backup Object Manager redirected restore.

BKI8773E The interactive modification of the containers failed.

Explanation: You tried to interactively change the location of containers, but this operation failed.

User response: Contact IBM Support.

BKI8776E You are not allowed to delete this container.

Explanation: You tried to delete the last container of a table space. However, at least one container must be available to every table space.

User response: Make sure that there is at least one container defined for every table space.

BKI8798E You cannot continue as there are errors.

Explanation: You tried to start a restore operation after redefining the containers interactively, but errors were detected in the input data. The operation cannot continue.

User response: Check all table spaces with '!!' error marks in the list and correct the definitions of their containers. Then continue.

BKI8799E A container must have a size of at least twice the extent size (minimum size for this table space).

Explanation: The container size specified is too small. The minimum size of a container is twice the extent size.

User response: Correct the container size.

BKI8800I **The command is:** ***command*****.**

Explanation: Displays the command that was issued. The following commands are possible: `Backup`, `Restore`, `Archive/Retrieve`.

User response: None.

BKI8801I **PID of calling process:** ***PID_number*****.**

Explanation: Displays the process id of the DB2 process which called the shared library.

User response: None.

BKI8802I **Found** ***number*** **backup image(s) on TSM server.**

Explanation: For restore and delete operations Data Protection for SAP queries TSM for backup images by means of a timestamp and shows the number of found images.

User response: None.

BKI8803I **The DB2 backup image size for this session is about** ***size*****.**

Explanation: The estimated size of the data to be backed up is displayed.

User response: None.

BKI8804W **The recovery log could not be written.**

Explanation: After every backup or restore, Data Protection for SAP writes a record into the recovery log file `tdprlf.<SID>.<node_name>.log`. It is located in the path pointed to by environment variable TDP_DIR.

User response: Check, if the permissions are set correctly and if there is sufficient free space in your file system.

BKI8805I **The restore was cancelled by the user. Existing data was not overwritten.**

Explanation: The existing database is still operational.

User response: None.

BKI8806I *product version.release.modification (Beta) build_number build_data*

Explanation: Writes version information into the product log file.

User response: None.

BKI8807I **Archive log file** ***log number*** **of chain** ***log chain number*****.**

Explanation: Writes information about the log file to be archived into the product log file.

User response: None.

BKI8808I **Retrieve log file** ***log number*** **of chain** ***log chain number*****.**

Explanation: Writes information about the log file to be retrieved into the product log file.

User response: None

BKI8810I **Cleaning up resources of process** ***PID_number*****.**

Explanation: All resources used by the product will be released.

User response: None.

BKI8812I **Committed TSM sessions will be deleted.**

Explanation: During a backup with multiple sessions, an error occurred. The backup operation is stopped. TSM sessions already committed during this operation are being deleted from the TSM server in order to prevent them from being considered restorable.

User response: None.

BKI8813E **Error deleting committed TSM sessions.**

Explanation: One or more committed TSM sessions could not be deleted during the postprocessing of the failed backup run.

User response: Use the Backup Object Manager to delete the file(s) manually..

BKI8814I **Inquire TSM with mask** ***search mask*****.**

Explanation: The string denoted is used to inquire TSM for backup images.

User response: None.

BKI8815I **Information for Log Manager:** *DB2_instance DB2_database_name DB2_database_alias log_and_log_chain_number partition*

Explanation: The information listed is provided to the DB2 Log Manager.

User response: None.

BKI8816I DB2 version 'version' detected

Explanation: TSM for ERP is running on a system where DB2 version 'version' is set up.

User response: None.

BKI8817I No corresponding committed TSM session(s) found. Nothing will be deleted.

Explanation: The cleanup of a failed TSM for ERP database backup could not find any partial TSM backup image of that run already stored on the TSM server for deletion.

User response: None.

BKI8818W Invalid value specified for BACKOM_LOCATION.

Explanation: The BackOM executable was not started for collecting database metadata due to an invalid specification.

User response: Check the value of the TSM for ERP configuration parameter BACKOM_LOCATION. The parameter can be found in the vendor environment file and must contain the fully qualified name of the BackOM executable.

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.

BKI8820E No valid TSM session found.

Explanation: A running TSM for ERP workflow could not continue due to a missing TSM session.

User response: Contact your IBM support personnel.

BKI8821I Using option(s) 'options'.

Explanation: The 'options' string specifies vendor options that DB2 provides to the TSM for ERP library as part of the calling function. These could be options directly provided as part of the database backup or restore command or options made persistent in the database configuration, here the parameters VENDOROPT, LOGARCHOPT1 or LOGARCHOPT2.

User response: None.

BKI8822I Configuration parameter(s): parameters

Explanation: The list specifies a set of runtime parameters that the TSM for ERP library is using for the calling workflow.

User response: None.

BKI8823W Configuration parameter SRC_DB_ALIAS requires parameter SRC_DB_INSTANCE and vice versa.

Explanation: To be able to recover a database after a redirected restore using the built-in DB2 rollforward command, TSM for ERP needs both SRC_DB_ALIAS and SRC_DB_INSTANCE.

User response: Include both parameters SRC_DB_ALIAS and SRC_DB_INSTANCE in the TSM for ERP vendor environment file and retry the database recovery.

BKI8824I Partitioning backup image into segments of maximum *size*.

Explanation: The backup image is partitioned into segments equal to the maximum *size* value. This partitioning is implemented per backup session.

User response: No user response is required.

BKI8825I Creating the commit object for session *session_id* comprising a total of *number* segments.

Explanation: A commit object is generated at the end of backup processing. This commit object guarantees the integrity of the backup object segments that compose a backup session. This action occurs on a per session basis where all backed up segments of a session are stored within that commit object. The commit object is used internally by Tivoli Storage Manager for Enterprise Resource Planning.

User response: No user response is required.

BKI8826I Found database image *image_name*. This image is partitioned into *number* segments.

Explanation: The database backup image *image_name* was found on Tivoli Storage Manager. This image is partitioned into *number* segments.

User response: No user response is required.

BKI8827E The commit object is missing.

Explanation: The commit object cannot be located on Tivoli Storage Manager. The commit object is a prerequisite when restoring segmented backup images. It ensures that a valid database is not destroyed or overwritten by an incomplete database restore.

User response: Check IBM Electronic Support for additional information: http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

---

BKI8828E **A backup object segment associated with backup image *image_name* is missing.**

Explanation: The integrity of the backup image *image_name* is compromised because a backup object segment is missing.

User response: The backup image *image_name* cannot be used for restore. Specify an older backup image for restore. In addition, start a new database backup as soon as possible.

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.

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

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).

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.

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.

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

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

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

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

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

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

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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs. Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

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

Trademarks

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

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 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.

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 6.2 information center: http://publib.boulder.ibm.com/infocenter/tsminfo/v6r2.

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.

Administration Assistant
A Web-browser based graphical interface to support and assist customizing of Data Protection for SAP 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.

BackOM
See Backup Object Manager.

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 Object Manager (BackOM)
A utility provided with Data Protection for SAP for backing up databases and for querying, restoring, and deleting backup objects residing on the TSM server.

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 DB2 log files, incremental backups, etc.).

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. Database cloning can be achieved with the redirected restore function of the Backup Object Manager.

Command Line Processor (CLP)
A character based interface of DB2 for entering SQL statements and database manager commands (e.g. backup or restore).

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.

DB2 Log Manager
Integrated log management facility of DB2 introduced with DB2 version 8.2. It provides the ability of log archiving, log retrieving, and managing of multiple log chains. Log files can be archived to disk, tape, TSM, or to vendor devices.

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 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.

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 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.

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.

Log Manager
See DB2 Log Manager

Logretain
DB2 database configuration parameter enabling roll-forward recovery of the database. If logretain is enabled, offline DB2 log files are retained. If the user exit is activated offline log files are archived by calling the configured user exit.

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.

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.
3. See partition

Normalizing of tablespaces
Resizing of tablespace containers during a redirected restore performed by the Backup Object Manager. As a result, all tablespace containers are allocated with the same size. Additionally, the data contained in the tablespace is evenly distributed among the containers. Consequently, parallel access to the data

is optimized. Tablespace normalizing can be combined with scaling.

Offline log file
A log file that is no longer needed by the DB database for roll-back or crash recovery. However, it may be required for a roll-forward recovery. DB2 may call the userexit to copy an offline log file to the log_archive path.

Online active log file
Log file which is currently being used by DB2 to log transactions. It is needed for rollback operations and crash recovery.

Online retained log file
DB2 log file no longer being used for logging transactions, but containing transactions with data pages that have not yet been written from the buffer pool to disk. The DB2 logging user exit is called by DB2 (if configured) to copy a filled or closed online retained log file to the 'log_archive' directory. Online retained log files may be deleted or reused by DB2 when they are no longer needed because all referenced transactions are committed and all changed pages have been written to disk and after the userexit has successfully copied them to the log_archive directory.

Partition
DB2: A part of a database that consists of its own data, indexes, configuration files, and transaction logs. A database partition is sometimes called a node or a database node.

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 History File
A recovery history file is created with each DB2 database and is automatically updated, for example, whenever one of the following operations is performed:
- Backup of a database or tablespace
- Restore of a database or tablespace
- Rollforward of a database or tablespace
- Alter of a tablespace
- Load of a table
- Drop of a table
- Reorganization of a table
- Update of table statistics

Every DB2 backup operation includes a copy of the recovery history file.

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 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

Scaling of tablespaces
Resizing of tablespace containers during a redirected restore performed by the Backup Object Manager. As a result, all tablespace containers are allocated with their original size increased or decreased

by a scaling factor. Tablespace scaling can be combined with normalizing.

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.

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.

SID The system identifier, a unique name of the SAP system, in respect to the database involved.

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.

SID The system identifier, a unique name of the SAP system, in respect to the database involved.

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
An abstraction of a collection of containers into which database objects are stored. A tablespace provides a level of indirection between a database and the tables stored within the database.

Tablespace container
A generic term describing an allocation of space to a tablespace. Depending on the tablespace type, the container can be a directory, device, or file.

Tablespace Definition Information
Data describing the physical layout of a database required by the Backup Object Manager redirected restore function. These data include information on all tablespaces and their associated tablespace containers. The TDI can be created at the end of a full database backup.

TDI Tablespace Definition Information (TDI): a set of metadata stored on Tivoli Storage Manager, reflecting among other things the current physical layout of the database to be backed up. These data are logically attached to the DB2 database backup images created with Data Protection for SAP(R). The TDI will be used by BackOM during redirected restore operations.

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.

User exit
The DB2 database manager can call a user exit program to store and retrieve log files and manage the location of archived log files, if the database configuration parameter 'userexit' is activated. Using a user exit program to archive and retrieve log files enables the database for rollforward recovery.

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.

Vendor API
An interface provided by DB2 to which vendors are able to write compatible software libraries, which should be shared libraries. Thus, the DB2 process is able to issue commands to the Vendor API to write backup data to sequential storage (e.g., Tivoli Storage Manager) and read files from sequential storage.

Vendor Environment File
File used to communicate environment settings to DB2 to be passed on to the shared library. The name of the vendor environment file is passed to DB2 as a parameter of the DB2 'backup database' and 'restore database' commands.

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.

Index

Program Number: 5608-E05

Printed in USA

SC33-6341-11