IBM Spectrum Protect for Enterprise Resource Planning
Data Protection for SAP for Oracle
Version 8.1.11

Installation and User's Guide

Note:

Before you use this information and the product it supports, read the information in "Notices" on page 99.

This edition applies to version 8, release 1, modification 11 of IBM Spectrum Protect for Enterprise Resource Planning (product number 5725-X03), and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 1995, 2020.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures vii

Tables ix

About this publication xi
- Who should read this guide xi
- Publications xi

What's new xiii

Chapter 1. Getting started 1
- Integration between SAP and Oracle 1
- BACKINT interface 2
- Oracle Recovery Manager (RMAN) 3

Chapter 2. Planning 5
- Database server considerations 5
- Network performance optimization 6
- Backup server optimization 6
- Store data on the IBM Spectrum Protect server 7
  - Parallel backup paths and backup servers 7
- Archive inactive data 8
- Restore versus backup 8
- Create multiple redo log copies 9
- Planning for using IBM HACMP for AIX 9
  - HACMP impact 10
- Digital signing of executable files (Windows) 10

Chapter 3. Installing 13
- Preparing to install 13
- Prerequisites 13
- Installing in silent mode 14
- Installing in a UNIX or Linux environment 15
  - Uninstalling older versions (UNIX and Linux) 17
- Installing in a Windows environment 17
  - Enabling ProLE to access configuration files on a remote share (Windows) 18
  - Uninstalling older versions (Windows) 19

Chapter 4. Upgrading 21
- Upgrading the base product 21

Chapter 5. Configuring 23
- Changing configuration tasks for the Data Protection for SAP base product 23
  - Verifying the installation 23
  - Configuring profile tasks 25
  - Configuring distributed file system tasks 28
  - Configuring as an HACMP application 29
- Configuring IBM Spectrum Protect 31

IBM Spectrum Protect client tasks....31
IBM Spectrum Protect server tasks....34

Chapter 6. Protecting data....43
Backing up SAP data....43
Schedule automated backup tasks....43
Windows scheduling example....45
Schedule batch sample....45
Full offline backup batch file sample....45
Full offline backup shell script sample....46
Restoring SAP data....47
Protecting with the Data Protection for SAP file manager....47
Clone the SAP system....50
Cloning an SAP system when automatic password handling is used....50
Cloning an SAP system when manual password handling is used....51

Chapter 7. Tuning performance....53
Server-related tuning....54
Alternate network paths and servers....54
Options....54
Performance options for Data Protection for SAP....54
Buffer copies....55
Buffer size....55
Compression of data for backup....55
Automation options....56
Data transfer....57
Data throughput rate....57
Performance sensors....57
Performance tuning for data transfer....58
Multiple servers....59
Multiple sessions....59
Multiplexing....60
Multiple network paths....60

Chapter 8. Troubleshooting....61
Troubleshooting common problems....61
Reproducing problems....61
Internet Protocol version 6 (IPv6) support....62
Log files that contain information and messages....62
Setup requirements....63
Information to collect for support....64
Troubleshooting problems....65
Messages....65
File manager....65
BACKINT problem resolution....65
RMAN problem resolution....67
Manually start Data Protection for SAP....68

Chapter 9. Reference information....73
Version numbers....73
BRARCHIVE function....73
Manage IBM Spectrum Protect sessions....73
Crontab example....73
Crontab file sample....74
Data Protection for SAP profile....74
Profile parameter descriptions....75
Sample profile file for UNIX or Linux....81

Sample profile (Windows)....85
Locating sample files....89
Save and delete redo logs, batch file sample....89
Save and delete redo logs, shell script sample....90
Client user options file sample (UNIX, Linux)....90
Client user options file sample (Windows)....91
Client system options file sample (dsm.sys)....91
Include and exclude list sample (UNIX, Linux)....91
Include/exclude list sample (Windows)....92
Client options files sample....93
Planning sheet for the base product....93
Network settings for IBM Spectrum Protect....94
Networks with large bandwidth delay....95
SP switch (RISC 6000)....96

Appendix A. Accessibility....97

Notices....99

Glossary....103

Index....105

Figures

1. Scope of Data Protection for SAP for Oracle 1

2. Data Protection for SAP with BR*Tools by using the BACKINT Interface 2

3. IBM Spectrum Protect for Enterprise Resource Planning with BR*Tools that use the RMAN Interface 3

4. Sample environment for HACMP takeover 9

5. Production Backup Example 44

6. File manager - Result of an inquiry procedure 48

7. File manager - Result of an inquiry procedure showing file names 48

8. File manager - Result of a redirected restore procedure 49

9. A balanced configuration 53

10. Data transfer for a backup and restore 55

11. Null Block Compression 55

12. High-level view of the data flow during backup 57

13. Performance optimizing by using sensors 58

14. Data Protection for SAP data transfer 58

15. Multiple servers 59

16. Parallel (multiple) sessions 59

17. Multiplexing 60

18. Parallel (multiple) paths 60

19. SAP and Data Protection for SAP for Oracle configuration files on UNIX or Linux 64

20. Problem isolation for BACKINT 66

21. Problem isolation for RMAN 67

Tables

1. File Extensions for Shared Libraries..... 15

2. SAP backup profile parameter combinations.....24

3. SERVER statement and appropriate profile and option file settings..... 25

4. Password handling for UNIX or Linux..... 39

5. Password handling for Windows.....40

6. Prefixes when you use BR*Tools..... 65

7. Installation parameters for Data Protection for SAP..... 94

8. Tuning IBM Spectrum Protect configuration file attributes.....95

9. Tuning of network settings.....95

10. Tuning of SP switch buffer pools..... 96

About this publication

This publication documents how to use IBM Spectrum Protect for Enterprise Resource Planning Data Protection for SAP. It describes the procedures that are needed to install and customize IBM Spectrum Protect for Enterprise Resource Planning which is the interface between SAP and IBM Spectrum Protect.

Who should read this guide

This guide is intended for system programmers and administrators who are responsible for implementing a backup solution in an SAP environment using the IBM Spectrum Protect. It describes the procedures needed to install and customize Data Protection for SAP, the interface between SAP and the IBM Spectrum Protect. The reader should be familiar with the documentation for SAP and IBM Spectrum Protect.

Publications

The IBM Spectrum® Protect product family includes IBM Spectrum Protect Plus, IBM Spectrum Protect for Virtual Environments, IBM Spectrum Protect for Databases, and several other storage management products from IBM®.

To view IBM product documentation, see IBM Knowledge Center.

© Copyright IBM Corp. 1995, 2020

What's new for IBM Spectrum Protect for Enterprise Resource Planning

The update for IBM Spectrum Protect for Enterprise Resource Planning Version 8.1.11 is listed in the table. Review the release notes before you install the product.

New and changed information in this product documentation is indicated by a vertical bar (|) to the left of the change.

Release	New features and updates
8.1.11	**Documentation updates** The IBM Spectrum Protect for Enterprise Resource Planning Knowledge Center and User's Guides have been updated with entries from the 8.1 Documentation updates technote since the last full Knowledge Center update for 8.1.4.
8.1.9	**Secure connection with TSL/SSL** In 8.1.9, you can connect to your SAP HANA databases by using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) connections.
8.1.6	**Backup enhancement: backup size** The accuracy of the estimated backup size that is sent to the IBM Spectrum Protect server has been improved. Instead of a fixed value that depended on the allocated memory size, the exact value of the backup is used.
8.1.4	**Take advantage of potential performance improvements enabled by parallel processing** IBM Spectrum Protect for Enterprise Resource Planning Version 8.1.4 can process multiple redo log copies in dedicated threads when used with SAP HANA, IBM DB2®, or Oracle RMAN database technology. If the system offers sufficient CPU power and bandwidth, these redo logs are sent to IBM Spectrum Protect servers in parallel, which can improve system performance.
8.1.1	The V8.1.1 release resolved defects, but did not introduce major new features.
8.1.0	**New product name** IBM Tivoli® Storage Manager for Enterprise Resource Planning is renamed to IBM Spectrum Protect for Enterprise Resource Planning in V8.1.0.

© Copyright IBM Corp. 1995, 2020

Chapter 1. Getting started

Data Protection for SAP and IBM Spectrum Protect provide a reliable, high performance, and production-oriented solution that enables back up and restore of SAP systems.

Data Protection for SAP is integrated with SAP backup and recovery utilities BRBACKUP, BRARCHIVE, BRRESTORE, and BRRECOVER, and applies SAP backup and recovery procedures. Data Protection for SAP is optimized for SAP databases and therefore provides efficient management of large data volumes.

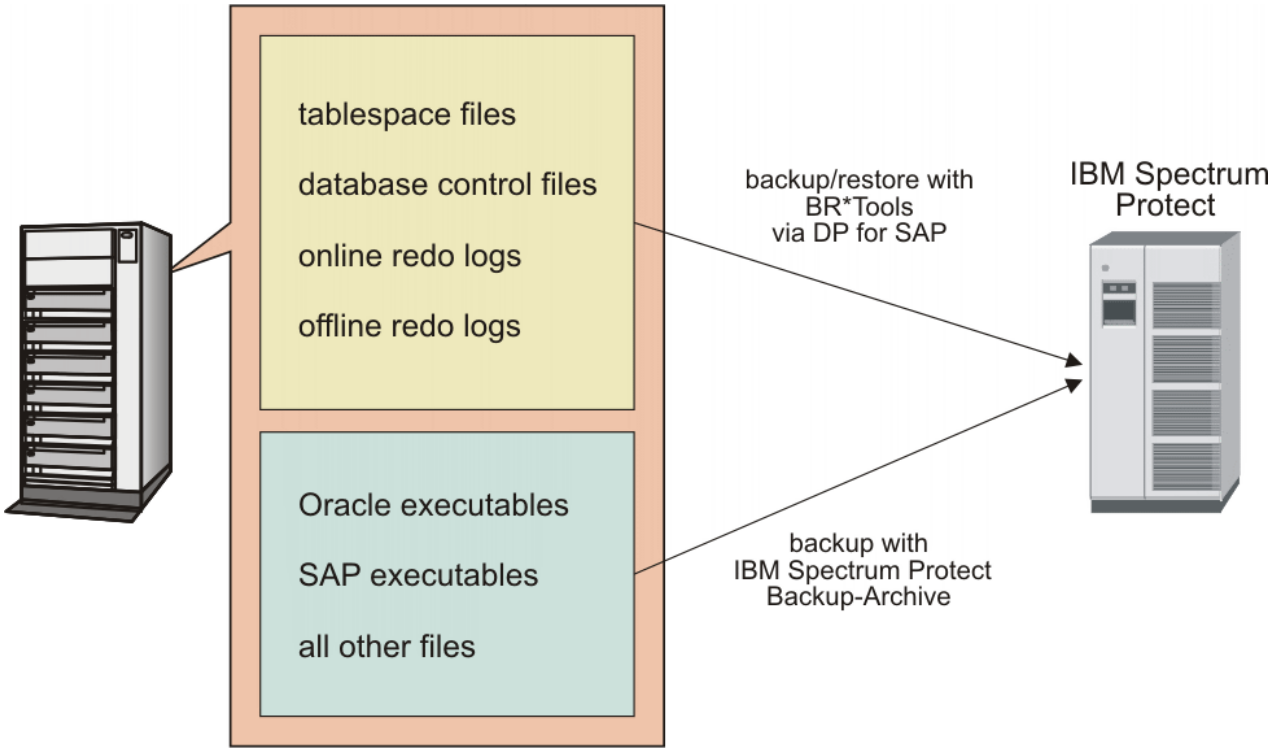

Figure 1. Scope of Data Protection for SAP for Oracle

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

Other files, such as SAP and Oracle executable files, can be backed up using the IBM Spectrum Protect backup-archive client. This action is important for disaster recovery purposes, as all SAP and Oracle executable files must be available before you use Data Protection for SAP to restore and recover the database.

Integration between SAP and Oracle

Data Protection for SAP operates as an unseen link between Oracle and BR*Tools and the IBM Spectrum Protect server.

There are two adapters in the Data Protection for SAP product:

`backint`
: This executable file is called directly by SAP. It is used for full online and offline database backups, and for backing up control and redo log files.

orasbt.dll
: This shared media management library is dynamically linked by Oracle RMAN. When a backup is done and uses this shared library, SAP communicates through Oracle RMAN instead of Data Protection for SAP. Incremental backups are possible when RMAN is used with this shared library.

© Copyright IBM Corp. 1995, 2020

Both adapters share the `initSID.utl` profile file. This file contains information that describes how to do backup and restore operations, and can be customized for the Data Protection for SAP environment. Both adapters communicate with the IBM Spectrum Protect server through an API that is shared with other Data Protection components. These adapters require that the Data Protection for SAP ProLE background process is running.

BACKINT interface

Data Protection for SAP provides the BACKINT interface to run full online and offline backups of Oracle databases, control files, and redo log files. The BACKINT interface communicates directly with SAP.

The following figure shows the interaction between BR*Tools, Data Protection for SAP, and the BACKINT interface when a backup or restore is running.

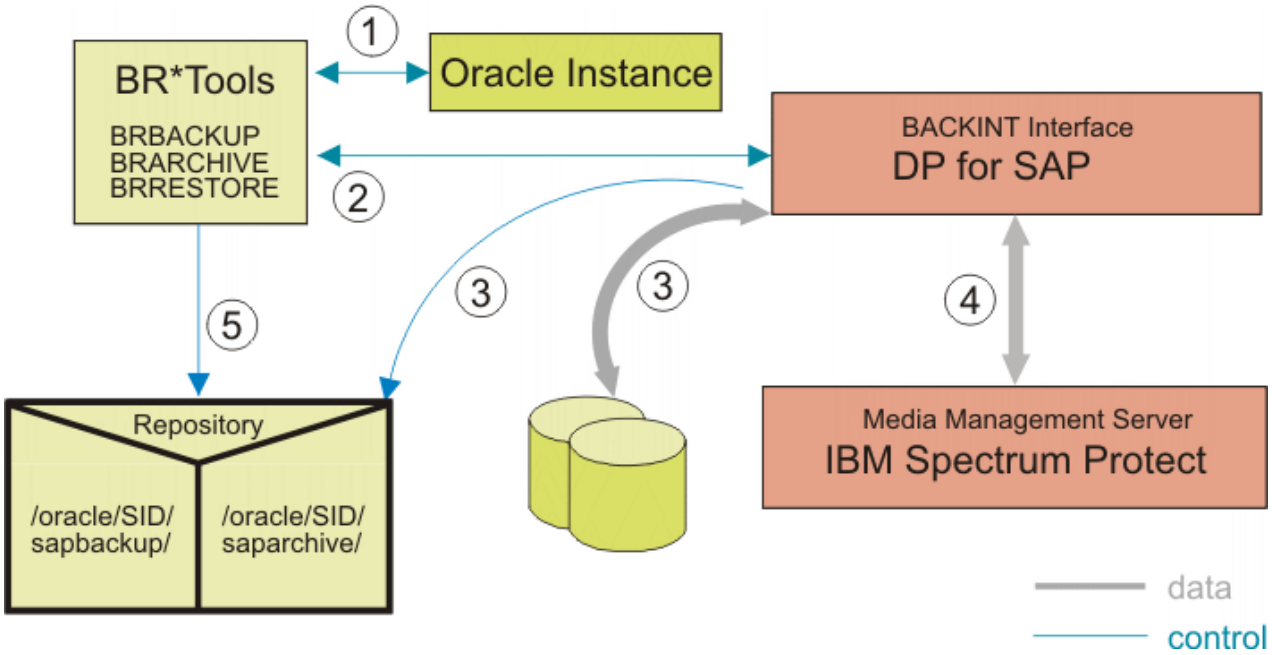

*Figure 2. Data Protection for SAP with BR*Tools by using the BACKINT Interface*

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

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

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

Oracle Backup/Restore and Data Protection for SAP

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

- BRBACKUP: Provides online or offline partial or full backups of table spaces.

- BRARCHIVE: Provides back ups of archived redo log files.
- BRRESTORE: Provides system-guided restore of Oracle backups.
- BRRECOVER: Provides recover capabilities.

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

Oracle Recovery Manager (RMAN)

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

Make sure to review SAP® support information about how to configure SAP on your operating system to do a backup by using RMAN with your database version. SAP information is available at SAP Service Marketplace.

When you use RMAN, IBM Spectrum Protect for Enterprise Resource Planning is loaded by one (or more) Oracle processes as a shared library. These Oracle processes decide on how many parallel sessions are opened, when a session is opened and closed, and which data object (table space) is included in the session. Some of the parameters, that are previously mentioned, must be configured for RMAN. Depending on how RMAN is used, these parameters can be configured either within the RMAN script or within the BR*Tools configuration file (init*SID*.sap).

If you want to use parallel sessions with RMAN, make sure that you configure at least the same number of sessions within the IBM Spectrum Protect for Enterprise Resource Planning configuration file as you configure for RMAN.

The following figure shows the interaction between BR*Tools, IBM Spectrum Protect for Enterprise Resource Planning, Oracle RMAN, and Data Protection for SAP when running a backup or restore.

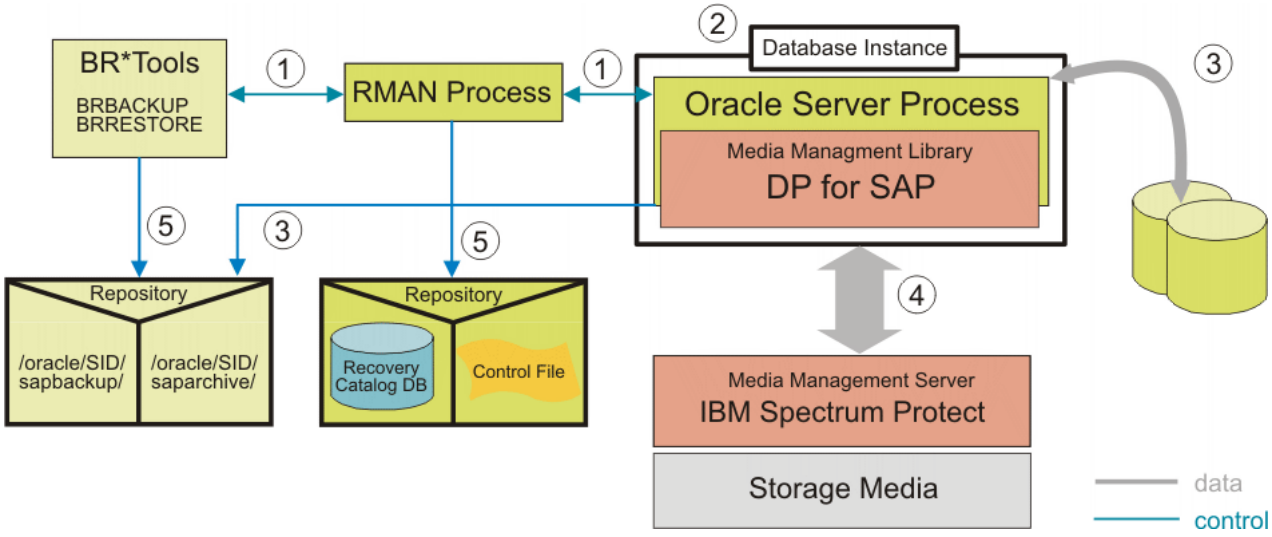

*Figure 3. IBM Spectrum Protect for Enterprise Resource Planning with BR*Tools that use the RMAN Interface*

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

IBM Spectrum Protect for Enterprise Resource Planning runs as a linked library controlled by the Oracle Server Process.

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

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

A special configuration is required when IBM Spectrum Protect for Enterprise Resource Planning is used with Oracle RMAN for offloaded backups to IBM Spectrum Protect from IBM Spectrum Protect Snapshot backups that are created with IBM Spectrum Protect Snapshot. An incremental backup is enabled by using profile parameters in the IBM Spectrum Protect for Enterprise Resource Planning configuration file, the `.utl` file.

Chapter 2. Planning

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

About this task

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

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

Database server considerations

In general, the production (SAP® database) server is the most critical component for data transfer, especially when parallelism is applied. As a result, special attention is given to the following 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 reduced by managing the buffers.

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 parallel is allowed, distribute data across several disks to take advantage of this feature.

Disk layout
The manner in which the database files are laid out can affect data transfer rates.

Data Protection for SAP allows parallel access to database files during backup and restore operations.

Since parallel is allowed, distribute data across several disks to take advantage of this feature.

Database size
The size of a database can be reduced by offloading inactive data to an external archive.

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

Backup types.
Online backups save database files, control files, and redo logs non-disruptively. However, more data is saved to redo log files during an online backup. The amount of data that is saved to redo logs during an online backup might be decreased when you use the file-online mode that is provided by SAP. A backup in this mode takes longer. Incremental backups reduce the backup time and the amount of

© Copyright IBM Corp. 1995, 2020

data to be sent to the backup server while restore time might be increased. For incremental backups, Oracle RMAN must be employed. For details on backup options, refer to your Oracle and SAP documentation.

Network performance optimization

When you are setting up the network, there are some items to consider that can improve network performance.

Consider these items when you set up the network:

LAN-free backup
LAN-free backup can reduce the load on the network and on the IBM Spectrum Protect server, thus improving data transfer rates. When you use LAN-free backup, ensure that Fibre Channel adapter capacity to the SAN can accommodate the data transfer rates of the disk reads and tape writes.

Network bandwidth
In general, 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
Increase the overall throughput rate to the backup server by providing a way to specify multiple network paths.

Backup server optimization

Data Protection for SAP uses the IBM Spectrum Protect archive function for all backup activities. When you are setting up the IBM Spectrum Protect server for use with IBM Spectrum Protect for Enterprise Resource Planning, the following considerations help you to optimize performance when you set up the IBM Spectrum Protect server.

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

CPU power
For a specific data throughput, the CPU load on the backup server is approximately 60% of the load on the database server. Therefore, backup server CPU power is not as critical as the CPU power of the database server. However, demands on the IBM Spectrum Protect server CPU do increase when several clients access a single IBM Spectrum Protect server.

Storage hierarchy

Backup of large data files is to be directed to tape to achieve the highest transfer rates. If disks must be used, use one disk pool per session. Small files such as log files, are to be directed to disk storage first and then moved to tape collectively to avoid excessive tape mounts.

Parallel sessions
The IBM Spectrum Protect server allows the use of several tape drives in parallel to store data. This setup can increase overall data throughput. To fully use this feature, two conditions must exist. The corresponding IBM Spectrum Protect node must be allowed the appropriate number of mount points and the device class must be allowed the appropriate mount limits.

Store data on the IBM Spectrum Protect server

In SAP terminology, *backup* (**BRBACKUP**) refers to the backup of data; *archive* (**BRARCHIVE**) refers to the backing up of log files. Data Protection for SAP uses the IBM Spectrum Protect archive function for backups and archives.

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

Tape storage is the preferred media for storing database contents as it provides the best data throughput for backup and restore operations. For a large scale-out system, the number of required tape drives might become too large. In this case, use a virtual tape library (VTL). A disk-tape storage hierarchy is used for backing up redo log files. This action provides the best protection against data loss, and eliminates the need to mount a tape for each redo log file.

Data Protection for SAP transfers data to and from the backup server through single or multiple (parallel) sessions to the IBM Spectrum Protect server. Each session must have a storage device that is 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 that are required for a complete restore.

Collocation is an IBM Spectrum Protect function that ensures client data is maintained together on one tape. Deactivate collocation in these situations:

- Deactivate collocation for Data Protection for SAP backups when you enable parallel sessions for use with multiple tape drives in parallel.
- Deactivate collocation when you use the multiple log copy function.

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

To improve availability (alternate servers) or performance (multiple servers), configure Data Protection for SAP to use multiple IBM Spectrum Protect servers. Consider the location of all backup data before you remove an IBM Spectrum Protect server from the Data Protection for SAP profile.

Because Data Protection for SAP accesses only those servers that are defined in the profile, be cautious when you remove an IBM Spectrum Protect server if it contains valid backup data.

Database backups are retained for a specified period and then become obsolete. Manage backup storage space efficiently, by deleting obsolete backups in one of the following ways:

- Set an appropriate archive retention period with IBM Spectrum Protect options.
- Use the Data Protection for SAP backup version control function. When the number of backup versions that are specified by this function is exceeded, entire backup generations are deleted. The backups that can be deleted are full backups and all related Oracle redo log backups.

The SAP backup log might still list deleted (expired) backups since this log cannot be updated by Data Protection for SAP.

Parallel backup paths and backup servers

Data Protection for SAP can use several communication links between IBM Spectrum Protect clients 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 IBM Spectrum Protect client-to-server communication and enable disaster recovery backup to a remote IBM Spectrum Protect server.

In Data Protection for SAP terminology, path denotes a connection between an IBM Spectrum Protect client or node, and an IBM Spectrum Protect server. A set of communication parameters is set for each defined communication path. An IBM Spectrum Protect 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 IBM Spectrum Protect servers "fast" and "slow", then two client option files `fast.opt` and `slow.opt` are required. Windows also requires an extra client user option file, `dsm.opt`. All option files must be in the same directory.

Each path in the `init`*`SID`*`.utl` profile is defined by a server statement and the corresponding definitions in the IBM Spectrum Protect client system option file `dsm.sys` (UNIX and Linux) or *`server`*`.opt` (Windows). The SERVER <server 1..n> statement denotes IBM Spectrum Protect servers that are defined in the Data Protection for SAP profile. This definition corresponds to the statement SERVERNAME *`server 1..n`* in the IBM Spectrum Protect client option file or files.

These servers are identified by their TCPSERVERADDRESS and can be on one system (multiple paths) or several systems (multiple servers). SESSIONS denotes the number of parallel sessions that Data Protection for SAP schedules for the 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 IBM Spectrum Protect server by using the first path in the profile.

If this attempt is 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 ends the backup job.

Archive inactive data

Data Protection for SAP creates a database image that is stored at the bit-level and can be used for routine backup operations.

To restore an outdated backup, you must restore it into the same environment it was originally taken from. This process requires you to maintain older versions of SAP, the operating system, database, and IBM Spectrum Protect data to enable a rebuild of the 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.

Restore versus backup

Configuration changes and infrastructure problems affect backup and restore operations.

Changes that support a fast backup while you are using resources can be considered applicable to the restore operation. Tune the backup operation and then run a restore to verify that the restore operation 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 must be decompressed.

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

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

Create multiple redo log copies

Data Protection for SAP can save a number of copies of each redo log by using different IBM Spectrum Protect server management classes. By creating multiple redo-log copies on separate physical media, the administrator can restore and recover a database even if a backup tape becomes corrupted.

The Data Protection for SAP profile file keywords important for creating multiple redo log copies:

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

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

- Data Protection for SAP creates as many backup copies of each redo log as are specified by the **REDOLOG_COPIES** keyword.
- Data Protection for SAP requires as many archive management classes that are defined by **BRARCHIVEMGTCLASS** as there are redo-log copies requested. To best protect against the loss of data, it is important that the different management classes are linked to different storage pools within IBM Spectrum Protect storage. This way, various redo log copies are on different backup media.
- When RMAN is used, Data Protection for SAP requires that the maximum number of sessions that are defined by **MAX_SESSIONS** is greater than or equal to the number of redo log copies that are requested. A setup with a smaller number of sessions is not advised with the backint interface.
- Data Protection for SAP cannot control the order in which IBM Spectrum Protect processes the requests. Therefore, an administrator cannot rely on sessions to be processed in the order they were started by Data Protection for SAP.

Planning for using IBM HACMP for AIX

Information is provided about Data Protection for SAP that is useful when you plan for HACMP failover configurations.

The following 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 must be taken on the database servers only.

This figure illustrates the takeover environment:

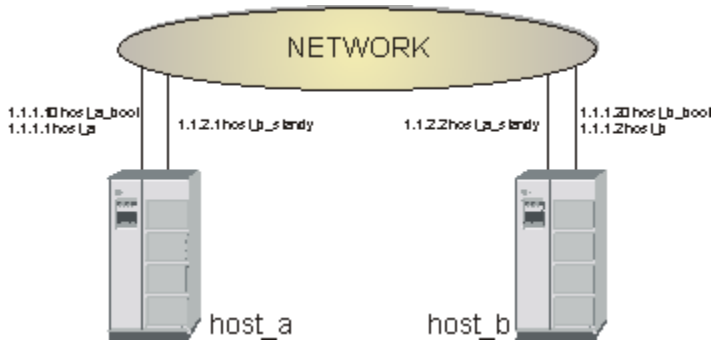

Figure 4. Sample environment for HACMP takeover

HACMP impact

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

Files

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

Dependencies

- Both hosts must have the same level of IBM Spectrum Protect API installed.
- Both hosts must be Data Protection for SAP.
- On both hosts, the `dsm.sys` file (in `/usr/tivoli/tsm/client/api/bin/dsm.sys`) must contain all server names that are required for takeover.

Communication

Backint connects to ProLE by using the following procedure:

- Retrieves the IP address for localhost (can be 127.0.0.1 for IPv4).
- Retrieves the backint service (port 57323).
- Connects to 127.0.0.1:*backint service*.

Digital signing of executable files (Windows)

Data Protection for SAP executable files (except .JAR files) for Windows systems have a digital signature.

The following files are affected:

- Passport Advantage® package for Windows
- Data Protection for SAP installation files:
  - *version*`-TIV-TSMERPORA-WinX64.exe`
- The Data Protection for SAP application files:
  - `backfm.exe`
  - `backint.exe`
  - `prole.exe`
  - `orasbt.dll`

Code signing employs digital IDs, also known as certificates.

Having a valid digital signature ensures the authenticity and integrity of an executable file. It identifies the software publisher as IBM Corporation to the person who downloads or starts it. However, it does not mean that the user or a system administrator implicitly trusts the publisher. A user or administrator must decide to install or run an application on a case-by-case basis. The factors of their decision are 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 by 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, more information is displayed about the IBM Certificate and the entire chain of trusted certificate authority signatures.

2. For the installation wizard, there is also the possibility to see the IBM digital signature from the software publisher link that is displayed in the **Security Warning** window.

A warning is shown if the certificate is expired and if a time stamp is not present. A warning is also shown 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.

The executable file must be stored on an NTFS disk. The Internet Explorer Enhanced Security Configuration component (also known as Microsoft Internet Explorer hardening) reduces the server vulnerability to attacks from web content by applying more restrictive Internet Explorer security settings. As a consequence, Internet Explorer Enhanced Security Configuration might prevent some websites from displaying properly. It might also prevent users and administrators from accessing resources with Universal Naming Convention (UNC) paths on a corporate intranet. For more information about managing Internet Explorer Enhanced Security Configuration, see http://www.microsoft.com/en-us/download/details.aspx?id=15013 A security warning might be displayed whenever you run an executable file that is 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 updates the metadata for the file with the zone (Internet or restricted) it was downloaded from. The metadata is saved as an Alternate Data Stream (ADS), which is a feature of NTFS with which the same file name can be used to cover multiple data streams. When you open a file that 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 shown:

```
      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. This is different from configuring the web server with a digital certificate.

Chapter 3. Installing

This section provides installation instructions for a typical install. There are different procedures to install through the console, or to install the product in silent mode.

Procedure

- Review the prerequisite information for the version before you start to install the software: http://www.ibm.com/support/docview.wss?uid=swg21987210
- Install the Data Protection for SAP product using the **InstallAnywhere** installation wizard.

Preparing to install

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

Before you begin

When you are installing Data Protection for SAP, consider that the product can be installed and operated for SAP systems with Oracle databases that employ a standard file system or raw logical volumes.

Be aware of differences between UNIX or Linux, and Windows versions of Data Protection for SAP. For example, UNIX or Linux uses the path separator "/" and Windows uses the path separator "\" with a drive letter.

Procedure

1. Verify that the Data Protection for SAP package is complete. See the README.1ST file on each installation disk (or disk image) for a description of the contents.
2. Verify that the prerequisites are met as described in http://www.ibm.com/support/docview.wss?uid=swg21987210.
3. Review planning sheet information as described in the *Planning sheet for the base product* topic.
4. Install or upgrade Data Protection for SAP.

Prerequisites

Before you install Data Protection for SAP , review the hardware, software, and application requirements.

Requirements for Data Protection for SAP are published in the hardware and software requirements technote for each release. Review the technote for your version in the *IBM Spectrum Protect for Enterprise Resource Planning - all requirement documents* site, http://www.ibm.com/support/docview.wss?uid=swg21987210. From the page, follow the link to the technote for your release or update level.

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

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

- Oracle database
- SAP R/3 or SAP e-business Solution
- IBM Spectrum Protect backup-archive client

© Copyright IBM Corp. 1995, 2020

For information about configuring the IBM Spectrum Protect API client, see the *Configure the IBM Spectrum Protect client options* topic. TCP/IP must be ready for communication between the IBM Spectrum Protect server and the IBM Spectrum Protect client.

- An operating system level that is supported by SAP and the IBM Spectrum Protect client

The release notes contain current information about Data Protection for SAP hardware, software, operating system, and maintenance levels.

When Data Protection for SAP is installed on a distributed file system, the root user requires read/write access to the file system during the installation.

An installation planning form for Data Protection for SAP is available in the `planning_sheet` (UNIX and Linux) or `planning_sheet.txt` (Windows) files in the installation directory. They are also available for printing in the *Planning sheet for the base product* topic. When prerequisites are met and installation planning information is completed, Data Protection for SAP is ready to be installed.

Installing in silent mode

You can install Data Protection for SAP for Oracle in silent mode using a response file. An installation that runs in silent mode suppresses the installation wizard. Instead, user data entry and status messages are displayed in the command line window.

Procedure

To run a silent or unattended installation complete the following steps.

1. Create a response file during an installation in either graphic or console mode by using option `-DRECORDFILE` denoting the response file name:

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

   Note: This command is for a UNIX system. For a Windows system, use the corresponding `.exe` file with the same options.

2. Start the executable file with the `-i silent` option (silent mode) and the `-f` option that denotes the file name of the response file:

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

   Note: This command is for a UNIX system. For a Windows system, use the corresponding `.exe` file with the same options.

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

Example

Sample properties file:

```
USER_INSTALL_DIR=/usr/tivoli/tsm/tdp_r3/ora64
SID=SID
SAP_CFG_FILE=/oracle/SID/dbs
SAP_BR_TOOL=/usr/sap/SID/SYS/exe/run
TSM_CFG_FILE=
TSMUTL_YES=1
TSMUTL_NO=0
TSMUTL_SERVERADRESSE=TSMServer
TSMUTL_NODE=R3NODE
TSMUTL_BACKUPMGM=MDB
TSMUTL_ARCHIVEMGM=MLOG1 MLOG2
TSMAPI_YES=
TSMAPI_NO=
TSMAPI_DSMI_DIR=
TSMAPI_DSMI_CONFIG=
TSMAPI_DSMI_LOG=
RMANYES=1
RMANNO=0
NAMEPORTAA_ADRESSE=
NAMEPORTAA_PORT=5126
```

Lines starting with "'#" are treated as comments.

Note: This example is a UNIX properties file. When you install IBM Spectrum Protect for ERP in silent mode for Windows, use the corresponding Windows properties file.

Installing in a UNIX or Linux environment

Data Protection for SAP is delivered as a single executable file for each operating system. Use the executable file to start the installation wizard and to install the product.

About this task

Packages on the FTP server contain "FTP" before the operating system designation.

- For a disk or disk image, the name has the following format:

```
version-TIV-TSMERPORA-platform
```

When the file is started, the IBM Spectrum Protect for ERP installation wizard guides you through the procedure. Read the descriptions carefully and follow the guidelines that are displayed on the windows.

Shared libraries have different file extensions on different UNIX or Linux operating systems. Within the following the section, the file extensions of shared libraries are represented as *ext*. Replace this text with the extension that applies to your operating system:

Table 1. File Extensions for Shared Libraries

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

In the following description, you must replace the directory name `ora`*`bit`* in the installation path. Depending on the version of IBM Spectrum Protect for ERP you install, you must replace it with:

Directory name	Bit-width version of IBM Spectrum Protect for ERP
ora64	64

Procedure

1. Log in as the root user on the SAP database server system.
2. If the Oracle RMAN interface is used, configure the Data Protection for SAP backup-archive client on your SAP database server as described in the *Configuring IBM Spectrum Protect* topic.
3. Verify that the *DISPLAY* variable is set to view the installation prompts through a graphical X-Window.
4. Start the appropriate IBM Spectrum Protect for ERP installation file for your operating system and your Oracle database.
5. Perform these tasks if the Oracle RMAN interface was selected during the installation process:
   a) Set the IBM Spectrum Protect for ERP password for Data Protection for SAP as described in the *Determining the IBM Spectrum Protect password method* topic.
   b) Make sure `/usr/lib` is specified in the library path environment of your system.
   c) Customize the SAP backup profile `init`*`SID`*`.sap` to use RMAN by adding this text:

```
backup_dev_type=rman_util
rman_parms="ENV=(XINT_PROFILE=path/initSID.utl,
PROLE_PORT=portnumber,&BR_INFO)"
```

   Locate the appropriate *ProLE* port number in the `/etc/services` file. Look for port name `tdpr3ora64`.

   If IBM Spectrum Protect for ERP is not installed in the default path and backups are done by using Oracle RMAN, then the environment variable **XINT_NLS_CATALOG_PATH** must be added to the parameter **rman_pars** in the `initSID.sap` file. The value of **XINT_NLS_CATALOG_PATH** must be set to the new customized installation path. Otherwise, the message catalog is not found.
6. If the Oracle RMAN interface was not selected during the installation process, create these links:

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

7. View the summary in the last page of the installation wizard. The IBM Spectrum Protect for ERP installation path is displayed in the summary where the installation log file (`log.txt`) is located.

Results

These modifications are automatically done to your system during installation:

These files are installed in the IBM Spectrum Protect for ERP installation directory:

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

An entry is created in `/etc/inittab` that automatically starts the "ProLE" daemon on UNIX systems.

The EN_US folder is created, which contains the message catalog file `tsmerp.cat`. The `_uninst` folder is also created, which contains more files.

These IBM Spectrum Protect for ERP configuration files are installed in the SAP directory (typically, `/oracle/SID/dbs`):

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

Uninstalling older versions (UNIX and Linux)

Follow the procedure to uninstall a previous version of IBM Spectrum Protect for Enterprise Resource Planning

Procedure

1. Log in to the SAP database server system 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 IBM Spectrum Protect for Enterprise Resource Planning is not running.
4. Start the uninstall executable file and follow the instructions of the uninstall procedure. The uninstall executable file is in one of the following directories:
   - AIX 64-bit:

     ```
     /usr/tivoli/tsm/tdp_r3/ora64/Uninstall_TIV-TSMERPORA/
     Uninstall_TIV-TSMERPORA  [-i silent | -i console]
     ```

   - Other UNIX 64-bit or Linux 64-bit:

     ```
     /opt/tivoli/tsm/tdp_r3/ora64/Uninstall_TIV-TSMERPORA/
     Uninstall_TIV-TSMERPORA [-i silent | -i console]
     ```

Installing in a Windows environment

IBM Spectrum Protect for ERP is delivered as a single executable file (`.exe`) for each operating system. Packages on the FTP server contain FTP before the operating system designation.

About this task

IBM Spectrum Protect for ERP for these operating systems is delivered as a single executable file for each operating system. The packages are named as follows:

- The package name on the disk or the disk image, which is shown in this example:

  ```
  version-TIV-TSMERPORA-platform
  ```

Procedure

1. Log in as a user with administrator authority on the SAP database server system.
2. If the RMAN interface is to be installed:
   a) Stop the `OracleService`*SID* service.
   b) Configure the IBM Spectrum Protect backup-archive client on your SAP database server as described in the *Configure the IBM Spectrum Protect client options* topic.
3. In Windows Explorer, go to the directory where the installation package is located.
4. Start the IBM Spectrum Protect for ERP executable file, and follow the instructions of the installation dialog.
5. Follow these steps if the Oracle RMAN interface was selected during the installation process:
   a) Set the IBM Spectrum Protect for ERP password for IBM Spectrum Protect as described in the *Determining the IBM Spectrum Protect password method* topic.

b) Customize the SAP backup profile `init`*`SID`*`.sap` to use RMAN by adding this text:

```
backup_dev_type=rman_util
rman_parms="ENV=(XINT_PROFILE=path/initSID.utl,
PROLE_PORT=portnumber,&BR_INFO)"
```

Locate the appropriate *ProLE* port number in the *`drive`*`:\WINNT\system32\drivers\etc\services` file. Look for port name tdpr3ora64.

If IBM Spectrum Protect for ERP is not installed in the default path and backups are done by using Oracle RMAN, then the environment variable **XINT_NLS_CATALOG_PATH** must be added to the parameter `rman_pars` in the `initSID.sap` file. The value of **XINT_NLS_CATALOG_PATH** must be set to the new customized installation path, otherwise the message catalog is not found.

c) Restart the Oracle service: `OracleService`*`SID`*.

6. View the summary on the last page of installation wizard. The IBM Spectrum Protect for ERP installation path is displayed in the summary where the installation log file (`log.txt`) is located.

Results

During installation your system is modified in the following way:

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

These files are installed in the IBM Spectrum Protect for ERP installation directory:

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

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

These IBM Spectrum Protect for ERP configuration files are installed in the SAP directory:

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

Enabling ProLE to access configuration files on a remote share (Windows)

When ProLE is started as a regular service, it operates under the ID of the local system account with Administrator privileges. However, a session opened on a remote system does not have credentials or permissions. You must grant access to ProLE to access the files on a remote share.

About this task

ProLE sessions on a remote system cannot access files that are on that remote share. This condition 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\`). Data Protection for SAP accepts UNC notation for the profile but not for all the files that are specified within the profile. These files are opened by ProLE, which by default has no permission to access remote shares.

Follow the procedure to enable ProLE to access all files on a remote share:

Procedure

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

Uninstalling older versions (Windows)

Follow these steps to uninstall a previous version of Data Protection for SAP in a Windows environment.

Procedure

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

Chapter 4. Upgrading

Follow the tasks to upgrade to Data Protection for SAP.

Upgrading the base product

Upgrade Data Protection for SAP from an earlier version.

Before you begin

If you are upgrading IBM Spectrum Protect for Enterprise Resource Planning on a busy SAP system where the software continuously starts log archives, it might be difficult to find a maintenance gap without any active log archiving processes. To alleviate this situation, you can stop the prole daemon. Each operating system has a different method to stop the prole daemon as follows.

- **AIX** As a root user, run the following command: `rmitab po64`.
- **RHEL 7 and later, SLES 12 and later** As root user, run the following command: `systemctl stop prole_ora`.
- **Older Linux versions and other Unix operating systems** As root user, comment out the line with prole in `/etc/inittab` and run command `init q`.
- **Windows** As a user with Administrator privileges, either run command `net stop prole`, or use the Services control panel to stop the prole service.

Tip: When you stop the prole daemon, redo log archive operations will not work. Typically, this is not an issue because the next archive run would pick up all the redo logs that previously failed to archive. But, if the system is generating a large amount of redo logs, the file system might run out of space.

About this task

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. The previous version provides the empty file. The file must then be initialized by setting the IBM Spectrum Protect password. However, the information about the current backup number is lost. As a result, more backup versions must be retained for a longer time than is specified by the **MAX_VERSIONS** parameter.

Procedure

1. Verify that the Data Protection for SAP package is complete. The installation packages are provided on a disc or disc image (downloadable from Passport Advantage), or the IBM FTP server. See the release notes file in the IBM Spectrum Protect Knowledge Center for the most current release information.
2. Make sure that the requirements for the new version of Data Protection for SAP are met as described in http://www.ibm.com/support/docview.wss?uid=swg21987210.
3. Make sure that planning information is available as described in the *Prerequisites* topic.
4. A full backup of the SAP database must be performed before you upgrade to the new version.
5. Uninstall the old version as described in the *Uninstalling older versions* topics.
6. Install the new version of Data Protection for SAP as described in the *Prerequisites* topic.
7. Verify the installation as described in the *Verifying the installation* topic.
8. A full backup must be performed after you upgrade to the new version.
9. Following an upgrade and subsequent RMAN setup on Windows, start (or restart) service `OracleService`*SID* to activate the new Data Protection for SAP environment.

© Copyright IBM Corp. 1995, 2020

Chapter 5. Configuring

In addition to configuring Data Protection for SAP, you need to configure other applications, for example, the IBM Spectrum Protect backup-archive client.

About this task

Data Protection for SAP requires certain configuration tasks to be run for the following applications.

- Data Protection for SAP base product
- Oracle RMAN and related files
- HACMP
- Distributed File System
- IBM Spectrum Protect backup-archive client
- IBM Spectrum Protect server

Changing configuration tasks for the Data Protection for SAP base product

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

About this task

Data Protection for SAP requires that you complete certain configuration tasks before it runs a backup operation.

Verifying the installation

The following tasks are part of the product configuration. The verification tasks for initial and upgrade installations need to be met.

About this task

Make sure that the following considerations are met before verifying the installation.

- The SAP backup profile is configured properly. This profile can be found on UNIX or Linux systems in the path `$ORACLE_HOME/dbs` and on Windows systems in the path `%ORACLE_HOME%\database`.

  This configuration refers to the following keywords within that profile:

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

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

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

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

  Available values for the **`backup_dev_type`** and **`backup_type`** keywords.

© Copyright IBM Corp. 1995, 2020

Table 2. SAP backup profile parameter combinations		
Operation	**backup_dev_type**	**backup_type**
Offline backup	`util_file`	`offline`
Online backup	`util_file`	`online`
Online backup with individual table space locking	`util_file_online`	`online`
Online backup through RMAN	`rman_util`	`online`

The SAP backup profile parameter must be set or changed as follows to run online backups with individual table space that lock with the data protection software:

```
backup_type      = online
backup_dev_type  = util_file_online
util_par_file = ORACLE_HOME/dbs/initSID.utl
```

Start the verification for initial and upgrade installations with a table space backup with BR*Tools. Then, start a full online or offline backup with BRBACKUP:

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

A complete restore or recovery of the entire SAP database must be run with BR*Tools. However, a complete offline backup with BRBACKUP must be done first. For backup tests, the BR*Tools utilities BRBACKUP and BRARCHIVE must be used. For restore or recovery test, only BRRECOVER must be used.

Verifying the RMAN setup (UNIX, Linux)
In the following description, you must replace the directory name `ora*bit*` in the installation path. Depending on the version that you install, you must replace it with `ora64` for the 64–bit version of IBM Spectrum Protect for Enterprise Resource Planning.

Procedure

1. Make sure that Oracle is linked to the correct library: `/usr/lib/libobk.*ext* /usr/tivoli/tsm/tdp_r3/ora*bit*/libtdp_r3.*ext*`.
   This link is not required in a distributed file system.
2. Remove the library that is specified in `/$ORACLE_HOME/rdbms/lib/libobk.*ext*`.
3. Make sure that the installed Oracle Server is a 64-bit version.
4. Examine the `sbtio.log` in the directory that is specified in the `user_dump_dest` keyword within the Oracle profile `init*SID*.ora`. This file is at `oracle/SID/saptrace/usertrace/sbtio.log`.
5. Check the log file `sbtio.log` for lines that start with `BKI`. The first message for each RMAN session is: `BKI7060I: Data Protection for SAP session: process ID`
   If you cannot find any such message in the file, the library is not correctly linked with Oracle.
6. Examine the `dsierror.log` in the directory that is specified with the environment variable **DSMI_LOG** or in the file that is denoted by keyword `ERROR`*logname* in the first stanza of file `dsm.sys`.
7. To get a IBM Spectrum Protect API trace file, set the following entries in the client system options file `dsm.sys`: `tracefile */path/trace file* traceflags api api_detail config policy`
   The additional soft link might help: `ln -s /usr/tivoli/tsm/tdp_r3/ora*bit*/libtdp_r3.*ext* /usr/lib/libtdp_r3.*ext*.1`

Verifying the RMAN setup on Windows

Verify that the RMAN interface is set up correctly in a Windows environment by looking at the `sbtio.log` log file.

Procedure

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

Configuring profile tasks

To configure the Data Protection for SAP profile file, you must set the server statement and in the IBM Spectrum Protect client options file.

Set the SERVER statement in the Data Protection for SAP profile

The SERVER statement is specified in the Data Protection for SAP profile, and in the IBM Spectrum Protect client option file.

There are corresponding keywords in the IBM Spectrum Protect 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 IBM Spectrum Protect client option file are established by using the logical server name. This logical server name is defined by the keywords SERVER or SERVERNAME.

Table 3. SERVER statement and appropriate profile and option file settings.

Configuration possibilities	**Data Protection for SAP profile `init`*`SID`*`.utl`**	**IBM Spectrum Protect 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` do not specify
single path; automatic password by IBM Spectrum Protect	`SERVER` *server* `ADSMNODE` do not specify	`SERVERNAME` *server* `NODENAME` *node* `TCPSERVERADDRESS` *address*
several paths/servers; no password or manual password	`SERVER` *server 1* `ADSMNODE` *node 1* `SERVER` *server 1* `ADSMNODE` *node n*	`SERVERNAME` *server 1* `NODENAME` do not specify `TCPSERVERADDRESS` *address 1* `SERVERNAME` *server n* `NODENAME` do not specify `TCPSERVERADDRESS` *address n*

Table 3. SERVER statement and appropriate profile and option file settings. (continued)		
Configuration possibilities	**Data Protection for SAP profile `initSID.utl`**	**IBM Spectrum Protect client option file `dsm.sys` or `server.opt` [2]**

several paths/servers; automatic password by IBM Spectrum Protect[3]	`SERVER server 1`
	`ADSMNODE do not specify`
	
	`SERVER server n`
	`ADSMNODE do not specify`
		`SERVERNAME server 1`
		`NODENAME do not specify`
		`TCPSERVERADDRESS address 1`
		
		`SERVERNAME server n`
		`NODENAME do not specify`
		`TCPSERVERADDRESS address n`

several paths/servers; automatic password by IBM Spectrum Protect [4]	`SERVER server`
	`ADSMNODE do not specify`
	`TCP_ADDRESS address 1`
	
	`SERVER server n`
	`ADSMNODE do not specify`
	`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 or Linux, `dsm.sys` is the single client option file for all IBM Spectrum Protect servers.

On Windows, there is a separate client option file *`server`*`.opt` for each IBM Spectrum Protect server.

[3]
If two different physical systems have the same IBM Spectrum Protect node name or if multiple paths are defined on one node by using several server stanzas, `passwordaccess generate` might work only 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. 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. The updated copy is generated by the first stanza that is used after password expiration. To avoid this situation, update the passwords before they expire. When the passwords are expired, run 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 valid entry.
3. Run `dsmc -servername=stanza2` and use the new password to generate a valid entry.

[4]
If you are using IBM Spectrum Protect API 5.5 (or later), you can use the **TCP_ADDRESS** parameter in the Data Protection for SAP profile. This parameter eliminates the requirement to set multiple stanzas in the IBM Spectrum Protect client option file for multiple paths. The parameter also eliminates the problem when it updates the password (see [3]).

Example of SERVER statement with alternate paths

This example assumes that the IBM Spectrum Protect server is configured with two tape drives and two LAN connections.

A backup is typically processed through network path 1 (**SERVER** statement 1). If network path 1 is unavailable, the backup is processed by using network path 2 (**SERVER** statement 2). If path 1 is active, Data Protection for SAP 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 two sessions on path 2. Since **MAX_SESSIONS** specifies 2, the backup is processed by using path 2.

The Data Protection for SAP profile that is used in this alternate path configuration is shown in the following example:

```
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
```

Example of SERVER statement with parallel servers

This example assumes the following configuration:

- Two IBM Spectrum Protect 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 that is connected to two networks.
- Daily backups are run on both systems.

The following is an example of the Data Protection for SAP profile that is 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

Data Protection for SAP profile is used in certain disaster recovery configurations.

This example assumes the following configuration for two servers a and b:

- Two IBM Spectrum Protect 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 that is connected to this FDDI network.
- Normal backups are processed with server a, which is local to the SAP database server.
- A disaster recovery backup is stored on remote server b every Friday.

The following is an example of the Data Protection for SAP profile that is 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
```

Configuring distributed file system tasks

Configure Data Protection for SAP in a distributed file system. If the SAP systems are statically assigned to specific hosts, you do not need to configure in a distributed file system. If the root user ID has write access to the distributed file system, you do not need to configure in a distributed file system.

Configuring for a distributed file system

Configure IBM Spectrum Protect for ERP in a distributed file system with the following procedure.

Before you begin

For a single SID on a host, IBM Spectrum Protect for ERP sets the ProLE service to run with the `ora`*`SID`* user ID instead of root. Follow the procedure to set up the ProLE service to run with the `ora`*`SID`* user ID.

About this task

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

- All SAP systems 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 the *Preparing to install* topic.

Procedure

1. Enable root access to the distributed file system.
2. Install IBM Spectrum Protect for ERP by using the procedure that is described in the *Preparing to install* topic.
3. On a UNIX system, replace the following entry in the `/etc/inittab` file:

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

   with this entry:

```
po64:345:respawn:su - oraSID -c /usr/tivoli/tsm/tdp_r3/ora64/prole -p profile
```

If upstart is configured, the `init` script `/etc/init/prole_db2.conf` must be used. *SID* must be the actual SID.

4. Refresh the `/etc/inittab` processes.
5. Disable root access to the distributed file system.

Results

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

Configuring as an HACMP application

Configure Data Protection for SAP for HACMP. Data Protection for SAP must be defined as an application to HACMP, and must be in a resource group that has a cascading or rotating takeover relationship. It does not support a concurrent access resource group.

Before you begin

A prerequisite for installation is a correct setup of the IBM Spectrum Protect client.

About this task

Although the *HACMP for AIX Installation Guide* can be reviewed for detailed instructions, a high-level summary is provided here.

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

```
smit hacmp
```

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

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

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

   Stop Script
   Enter the full path name 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.

Adding Data Protection for SAP to a HACMP resource group

A final step in enabling Data Protection for SAP for HACMP failover is to define it to a cluster resource group.

Before you begin

Although the *HACMP for AIX Installation Guide* can be reviewed for detailed instructions, a high-level summary is provided here. Perform these tasks to define the resources that are part of a resource group:

Procedure

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 wanted resource group. Press Enter and SMIT displays the **Configure a Resource Group** screen.
3. Enter values that define all the resources you want to add to this resource group.
4. After you enter field values, synchronize cluster resources.
5. Press F10 to exit SMIT or F3 to return to previous SMIT screens to run other configuration tasks or synchronize the changes that you just made. To synchronize the cluster definition, go to the Cluster Resources SMIT screen and select the **Synchronize Cluster Resources** option.

What to do next

The IBM Spectrum Protect client application must be added to the same resource group that contains the file systems it will back up. The file systems that are defined in the resource group are to also be the ones that are specified in the domain for this client instance in the client user options file. Both JFS and NFS file systems can be defined as cluster resources, although NFS supports only two node clusters in a cascading takeover relationship.

HACMP stop script example

A stop script that operates in an HACMP environment is illustrated.

Depending on the installation environment, the sample stop script might have 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 because of 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 by entering the cluster again.

The stop script is called by HACMP with the root user ID.

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

```
#!/bin/ksh
# # # #
```

Setting IBM Spectrum Protect client options on UNIX or Linux

IBM Spectrum Protect clients on UNIX or Linux are configured by setting options in the `dsm.opt` and `dsm.sys` files. The `include/exclude` file is used to define which files are included or excluded during backup, archive, or hierarchical storage processing.

About this task

Configure the IBM Spectrum Protect backup-archive client to operate in an SAP environment with the following procedure.

Procedure

1. Install the IBM Spectrum Protect client software on the SAP database server system.
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`. If the server and client are on the same system, select loopback. This selection improves TCP/IP communication speed.
4. Specify `InclExcl` if you want IBM Spectrum Protect to include or exclude the files that are listed in `inclexcl.list`.

   You might want to exclude all database files that are processed by the BR*Tools.
5. Throughput improves when tape drives attached to the IBM Spectrum Protect server provide hardware compression. However, combining hardware compression and IBM Spectrum Protect client software compression (`Compression ON`) is not advised. It might be necessary to experiment with IBM Spectrum Protect client software compression settings to determine its impact in your environment. IBM Spectrum Protect client software compression generally improves performance only when network throughput is low.
6. Edit the client user options file `dsm.opt` and set these values as appropriate for your installation:

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

Results

When the IBM Spectrum Protect API client is installed on a UNIX or Linux system, ensure that a link exists that points to the IBM Spectrum Protect API installation directory, `/usr/tivoli/tsm/client/api/bin64`.

```
/usr/lib/libApiDS.ext
```

The IBM Spectrum Protect provides two features for specifying the location of the IBM Spectrum Protect API Client error log: the environment variable **DSMI_LOG** and the IBM Spectrum Protect system client option ERRORLOGName in `dsm.sys`. For **DSMI_LOG**, a directory is specified to which a file named `dsierror.log` is written. For ERRORLOGName a path and user-defined file name are defined.

To achieve conclusive logical linking of the environment, configuration and log files in your SAP backup-archive system, you must use the IBM Spectrum Protect system client option ERRORLOGName rather than the environment variable **DSMI_LOG**.

When you use ERRORLOGName, you can include the SID in the file name. This information can speed up problem determination by simplifying identification of the correct error log file. You can match log file names to the active user client options file name, which must also contain the SID and be stored in

environment variable **DSMI_CONFIG**. This information is especially useful on systems with several SIDs.

The suggested configuration prepares the system for IBM Spectrum Protect API Client tracing for both **backint** and RMAN operation.

With this 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** exists in your environment from an earlier setup, it is overridden by `dsm.sys` option **ERRORLOGName**. However, 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.

Setting IBM Spectrum Protect client options

IBM Spectrum Protect 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.

About this task

To configure the IBM Spectrum Protect backup/archive clients to operate in an SAP environment, complete the following steps:

Procedure

1. Install the IBM Spectrum Protect client software on the SAP database server system.
2. For each logical IBM Spectrum Protect server, a corresponding client option file is needed. 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 system. This selection improves TCP/IP communication speed.
4. Specify `InclExcl` if you want IBM Spectrum Protect to include or exclude the files that are listed in `inclexcl.list`. You might want to exclude all database files that are processed by the BR*Tools.
5. Throughput improves when tape drives attached to the IBM Spectrum Protect server provide hardware compression. However, combining hardware compression and IBM Spectrum Protect client software compression (`Compression ON`) is not advised. It might be necessary to experiment with IBM Spectrum Protect client software compression settings to determine its impact in your environment. IBM Spectrum Protect client software compression generally improves performance only when network throughput is low.

Results

An IBM Spectrum Protect error log (required for each client) can be specified for each process regardless of the number of IBM Spectrum Protect client option files *server*`.opt` involved. The IBM Spectrum Protect error log is determined by these rules:

1. The IBM Spectrum Protect 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 IBM Spectrum Protect 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 IBM Spectrum Protect client log is written to file `dsierror.log` in the local path.

Set up the IBM Spectrum Protect client so that different processes write to separate error logs. The error log path must be defined in the **DSMI_LOG** environment variable if the client options files are shared among processes.

IBM Spectrum Protect server tasks

Data Protection for SAP requires configuration tasks to be done for the IBM Spectrum Protect server as part of the overall product configuration.

Configure the IBM Spectrum Protect server

When you are configuring Data Protection for SAP you must set up the IBM Spectrum Protect server, and run general and specific server configurations such as setting up storage devices.

Although the task examples use IBM Spectrum Protect commands, these tasks can also be run using the IBM Spectrum Protect web client GUI.

Consider the following performance-related guidelines before you install the IBM Spectrum Protect server.

IBM Spectrum Protect server host system
The IBM Spectrum Protect server must be installed on an exclusive system. The tasks that are presented here avoid concurrent processes and disk I/O access with other applications. A single IBM Spectrum Protect server is sufficient for a single SAP system landscape. If the IBM Spectrum Protect server is used to back up and restore other clients, consider installing the server on a large system or by using several IBM Spectrum Protect servers.

Network topology
Network topologies such as Fast Ethernet and Gigabit Ethernet work well with the IBM Spectrum Protect server. Use fast network topologies to prevent bottlenecks during backup and restore operations. The IBM Spectrum Protect 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 an IBM Spectrum Protect server. The use of a High Performance Switch network can improve backup and performance.

These steps are considered complete when the IBM Spectrum Protect server is successfully installed:

- Recovery log volume is allocated and initialized.
- Recovery log mirror volume is allocated and initialized.
- Database volume is allocated and initialized.
- Database mirror volume is allocated and initialized.
- Extra labeled volumes for the backup and archive storage pools are allocated and initialized (disks, tapes, or combinations).
- Licenses are registered.
- The IBM Spectrum Protect server is started.

The latest code fixes for IBM Spectrum Protect can be found at: `ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance`

Specifying an IBM Spectrum Protect server

To configure Data Protection for SAP, you need to specify an IBM Spectrum Protect server in the profile file.

About this task

Follow these steps to add an IBM Spectrum Protect server:

Procedure

1. Add a server statement to the Data Protection for SAP profile.
2. Adapt the IBM Spectrum Protect options files as described in the *Verifying the IBM Spectrum Protect server name* topic.
3. Set and save the IBM Spectrum Protect password for the new server as described in the *Setting the IBM Spectrum Protect password* topic.

Specifying a storage device

A storage device needs to be added when you are configuring. A storage device defines a device class, which handles the type of media. The default device class that is defined for disks is `DISK` and is considered sufficient.

About this task

Verify that the following items are established within the IBM Spectrum Protect server after installation.

- Query the defined library:

```
q library
```

- Query the defined drives:

```
q drive
```

- Query the defined device class:

```
q devclass
```

Defining a storage pool

A storage pool needs to be added when during the configuration. 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.

Procedure

1. Define a storage pool for the SAP system data: `define stgpool sap_incr` *`device_class_name`* `maxscr=5`
2. Define a storage pool for the data files : `define stgpool sap_db` *`device_class_name`* `maxscr=20`
3. Define a storage pool for the first copy of offline redo log files : `define stgpool sap_log1` *`device_class_name`* `maxscr=3`
4. It is advised that you back up the offline redo log files twice on two different IBM Spectrum Protect volumes. Define an extra storage pool for the second copy of offline redo log files: `define stgpool sap_log2` *`device_class_name`* `maxscr=3`

Results

When a library tape device is associated, the maximum *scratch volumes* (labeled volumes that are empty or contain no valid data) that this storage pool is 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.

Defining a policy

A server policy needs to be specified when you are configuring IBM Spectrum Protect policies. Specify how files are backed up, archived, moved from client node storage, and 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*.

About this task

After you set definitions, a default policy set must be assigned, validated, and activated. For the policy definition, log on as an IBM Spectrum Protect Administrator by using the *Admin Command Line* or the *Web Admin* and run the following commands.

Procedure

1. Define a policy domain and policy set:

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

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

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

   If you are planning to use this IBM Spectrum Protect 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 uses *version control* for managing SAP database backups by backing up all data to only those management classes for which an archive copy group is defined (**type**`archive`). To prevent backed up files within IBM Spectrum Protect server storage from being deleted due to expiration dates (IBM Spectrum Protect deletes expired files), the copy group parameter **retver**, which specifies the number of days a file is to be kept, must 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
```

Registering a node

The node must be registered when you are completing the configuration. The IBM Spectrum Protect server views its registered clients, application clients, host servers, and source servers as nodes.

About this task

To register a node, log on as the IBM Spectrum Protect administrator by using the *Admin Command Line* or the *Web Admin*, run the following command:**register node C21 passwd domain=sap_c21 maxnummp=8**

When you use 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 must use more than one mount point, the parameter must be set to the wanted number of mount points. This parameter is not to be set higher than the total number of drives available on the IBM Spectrum Protect server.

Setting the `IdleTimeOut` parameter

For simulations of network transfer and media rates, the IBM Spectrum Protect server must be configured so that sessions do not time out during simulation.

About this task

To avoid sessions timing out, set the parameter **IdleTimeOut** to a value higher than the time required for sending the largest table space file to the IBM Spectrum Protect. For example:

```
setopt IdleTimeOut 60
```

Determining the IBM Spectrum Protect password method

Specify how Data Protection for SAP manages the IBM Spectrum Protect password. There are three options.

About this task

There are three methods of password handling:

No password is required

No authentication is completed on the IBM Spectrum Protect server. Each user that is connected to the backup server can access IBM Spectrum Protect data without a password. This method is advised only if adequate security measures are established.

For example, no password might be acceptable when the IBM Spectrum Protect is only used for SAP, and authentication and authorization is done at the operating system level. This scenario is valid when no other clients are registered to the IBM Spectrum Protect.

Manual handling of password

A password is required for each connection to the IBM Spectrum Protect server. In this method, Data Protection for SAP stores the encrypted password in its configuration files.

While the password does not expire and is not changed on the IBM Spectrum Protect server, Data Protection for SAP automatically uses the stored password when it connects to IBM Spectrum Protect. This method provides password security and can be set up easily. Whenever the password expires or is changed, the new password must be set with this command:

(UNIX or Linux):

```
backint -p full path to UTL file/initSID.utl -f password
```

(Windows):

```
backint -p full path to UTL file\initSID.utl -f password
```

On Windows, the path can also be specified in UNC notation (for example: `-p \\SERVER_A\dpsap \initSID.utl`. However, the password updates must be synchronized on the IBM Spectrum Protect server with the **update node** command. These steps must also be repeated whenever the IBM Spectrum Protect password expires. Therefore, this method must be used only during installation or testing, and a long password expiration period must be specified. Manual password handling is not advised for production operations.

If you are setting the password to be automated (such as in a script), enter this command:

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

where *passwordA* is the password for IBM Spectrum Protect node *nodeA* on IBM Spectrum Protect 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 when you record IBM Spectrum Protect passwords in a script.

Automatic handling of password

A password is required for each connection to the IBM Spectrum Protect server. After the first connection, the password is managed by IBM Spectrum Protect. The IBM Spectrum Protect client stores the current password locally. When the password expires, the password is changed and stored automatically. If you are planning to use Oracle RMAN and schedule your backups or restores from a system user different from the database owner, you must grant access permissions to your data files on disk for this user.

You must specify the IBM Spectrum Protect password currently being used by using Data Protection for SAP to connect to the server. Whenever the password is changed manually on the IBM Spectrum Protect server, use the **update node** command to update the password. Use the following command for automatic password handling:

(UNIX or Linux):

```
backint -p full path to UTL file/initSID.utl -f password
```

This method is advised for an automated production environment.

Windows:

```
backint -p full path to UTL file\initSID.utl -f password
```

On Windows, the path can also be specified in UNC notation (for example: `-p \\SERVER_A\dpsap \initSID.utl`

Setting the IBM Spectrum Protect password
Data Protection for SAP is to be installed after the IBM Spectrum Protect installation is completed. IBM Spectrum Protect provides different password methods to protect data.

About this task

Data Protection for SAP must use the same method as specified in IBM Spectrum Protect. The default password method during Data Protection for SAP installation is PASSWORDACCESS prompt.

Provide Data Protection for SAP with the password for the IBM Spectrum Protect node by entering this command:

```
backom -c password
```

The default parameters for Data Protection for SAP are set according to this default value. If a different password method is set in IBM Spectrum Protect, adjust the Data Protection for SAP parameters.

Provide Data Protection for SAP with the password for the IBM Spectrum Protect node by following these steps in the shell:

Procedure

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

```
backint -p full path to UTL file\initSID.utl -f password
```

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

```
backint -p full path to UTL file/initSID.utl -f password
```

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

Password configuration matrix
After you select the suitable password-handling method, follow this configuration matrix to set the password keywords and parameters.

Proceed as indicated by the step number.

Table 4. Password handling for UNIX or Linux

Step	Profile/Action	Parameter	Password		
			No	Manual	Set by IBM Spectrum Protect
1	IBM Spectrum Protect 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	IBM Spectrum Protect admin	UPDATE NODE (see notes 1, 6)	Unavailable	*password*	*password*
4	Data Protection for SAP profile (`initSID.utl`)	For each SERVER statement, specify: PASSWORDREQUIRED ADSMNODE	NO *nodename*	YES *nodename*	NO (see note 4)
5	Data Protection for SAP command line	Specify in each SERVER statement: `backint -p initSID.utl -f password`	Unavailable	*password* (See notes 3,7,8)	*password* (See notes 3,7,8)

Note:

1. See appropriate IBM Spectrum Protect documentation.

2. If you are using manual password generation during testing, make sure that the expiration period is set to an appropriate time.
3. This password must be the one that is effective on the IBM Spectrum Protect server for the node.
4. **ADSMNODE** must not be set when **PASSWORDACCESS** generate is set.
5. The users *SID*adm and ora*SID* must have read and write permission for the `path` specified in the PASSWORDDIR option in the IBM Spectrum Protect client options file.
6. This step is only necessary if the password is expired (manual-handling only) or must be changed on the IBM Spectrum Protect server.
7. A password must be entered for each server statement in the Data Protection for SAP profile.
8. When you use Oracle RMAN with PASSWORDACCESS GENERATE, backups must always be started with the same user ID provided in step 5 (setting of passwords).

Password configuration matrix (Windows)
When the preferred method of password-handling is determined, review the following steps to set the keywords and parameters in the various profiles.

Detailed information about password-handling methods is available in the *Determining the IBM Spectrum Protect password method* topic.

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

Table 5. Password handling for Windows

Step	Profile/Action	Parameter	Password		
			No	**Manual**	**Set by IBM Spectrum Protect**
1	IBM Spectrum Protect 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	IBM Spectrum Protect admin	UPDATE NODE (see notes 1,6)	Unavailable.	*password*	*password*
4	Data Protection for SAP profile init*SID*.utl	For each SERVER statement, specify: PASSWORDREQUIRED ADSMNODE	NO *nodename*	YES *nodename*	NO (see note 4)
5	Data Protection for SAP command line	Specify in each SERVER statement: `backint -p initSID.utl -f password`	Unavailable	*password* (see note 1)	*password*

Note:

1. See IBM Spectrum Protect documentation.
2. If you are using manual password generation during testing, make sure that the expiration period is set to an appropriate time.
3. For an initial setup, this password must be the same password that is specified when the node was registered to IBM Spectrum Protect. The password must be changed first on the IBM Spectrum Protect server and then on Data Protection for SAP.
4. **ADSMNODE** must not be set when **PASSWORDACCESS** generate is set.

5. The users *SID*adm and sapservice*SID* must have read and write permission for the path specified in the PASSWORDDIR option in the IBM Spectrum Protect client options file.
6. This step is only necessary if the password is expired (manual-handling only) or must be changed on the IBM Spectrum Protect server.
7. A password must be entered for each server statement in the Data Protection for SAP profile.

Verifying the server name

You must verify that the server name and the parameters are correct in the init*SID*.utl file.

Procedure

- Review the IBM Spectrum Protect client options files to make sure that the server name matches the name that is specified in the server statement of the init*SID*.utl file.
- Review that other parameters are set correctly. These settings depend on the password method selected.
- (UNIX or Linux) Define the IBM Spectrum Protect server in the IBM Spectrum Protect client system options file (dsm.sys). The server stanza that is specified in dsm.sys must match the entry in init*SID*.utl.
- (Windows) 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 that is specified in init*SID*.utl.

Chapter 6. Protecting data

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

Backing up SAP data

Plan a daily backup strategy with scheduled and automated backups for the system.

About this task

Follow the tasks to put the backup strategy in place. Use the samples to help you for your operating system.

Schedule automated backup tasks

Scheduling and automating backup and archive operations helps to ensure that data is backed up regularly at a specified time. Products that are used to schedule backup operations can be used to automate these 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 by using either the Schedule Services feature (on Windows) or the **crontab** command (for UNIX or Linux).

IBM Spectrum Protect scheduler
IBM Spectrum Protect also provides a scheduler function for all of its clients. As a result, automation can be set for multiple database servers. The IBM Spectrum Protect administrative client GUI provides an easy-to-use wizard for defining schedules. Information about how to define IBM Spectrum Protect schedules can be found in the *IBM Spectrum Protect Administrator's Reference*.

Sample IBM Spectrum Protect schedule

This sample procedure is flexible because you can define a command file with any set of commands you choose. This allows you to use the same command file to define schedules on other IBM Spectrum Protect servers.

1. Enter the following command on the server console or from an administrative client to define the schedule. The administrative client does not have to be running on the same system as the IBM Spectrum Protect server.

   ```
   def sched PolicyDB daily_db_bkup desc="Daily Online DB Backup"
     action=command objects="/home/admin/sched/schedbkdb.scr"
     starttime=21:00 duration=15 duru=minutes period=1 perunits=day
     dayofweek=any
   ```

   IBM Spectrum Protect displays this message:

   ```
   ANR2500I Schedule daily_db_bkup defined in policy domain PolicyDB.
   ```

2. To associate Data Protection for SAP to this backup schedule, issue the following command:

   ```
   define association PolicyDB daily_db_bkup NodeA1
   ```

   IBM Spectrum Protect displays this message:

   ```
   ANR2510I Node NodeA1 associated with schedule
    daily_db_bkup in policy domain PolicyDB.
   ```

© Copyright IBM Corp. 1995, 2020

A backup event (schedule) is now defined on the IBM Spectrum Protect server. The schedule runs a command file called schedbkdb.scr located in the /home/admin/sched directory. The backup starts around 9:00 PM., runs once a day, and can start on any day of the week. Use the IBM Spectrum Protect administrative commands query schedule or query association to confirm that you set the schedule and association correctly.

IBM Workload Scheduler

The IBM Workload Scheduler provides event-driven automation, monitoring, and job control for both local and remote systems.

Sample backup strategy for daily backup processing

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

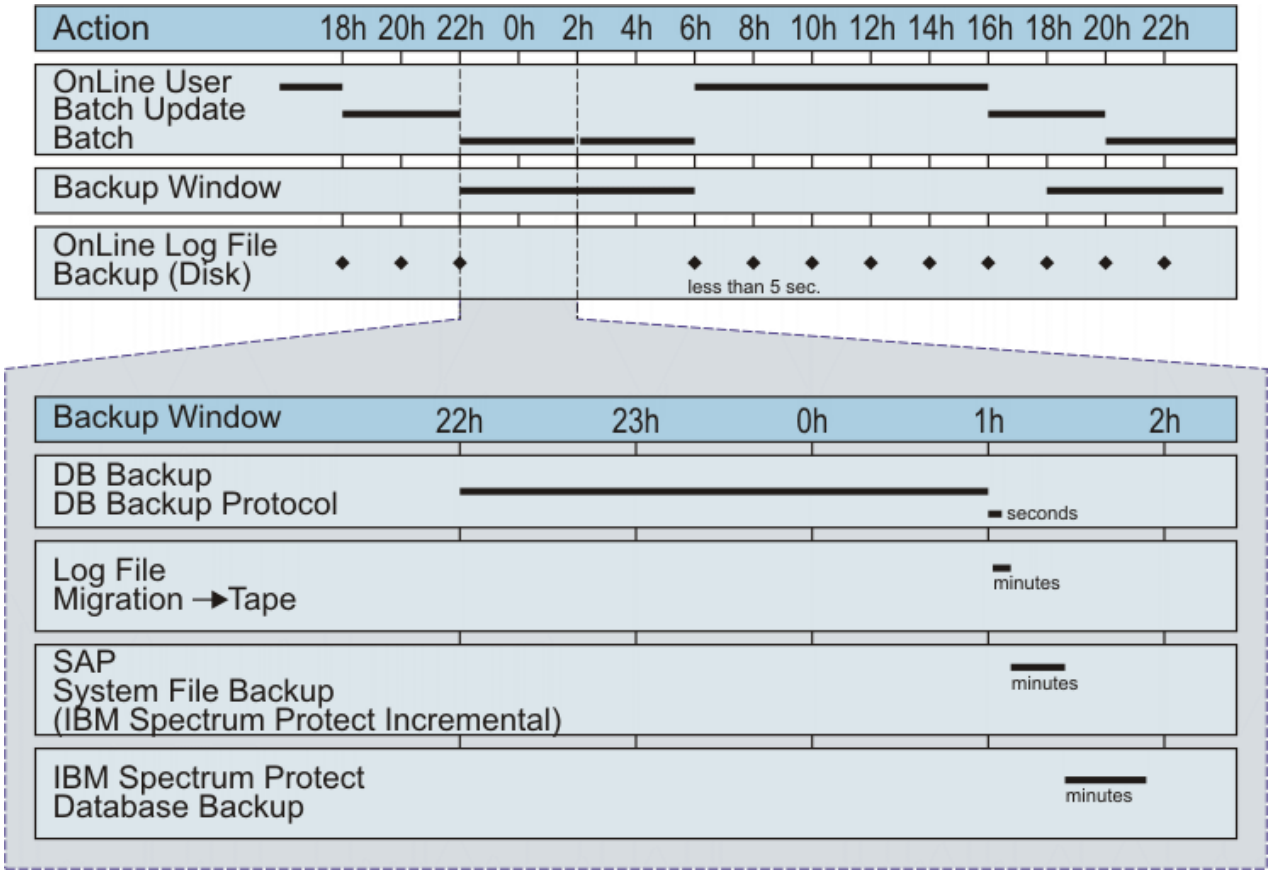

Figure 5. Production Backup Example

The automated backup example shown in the graphic displays these common tasks:

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

Backups can be moved to disk storage and to tape media. The IBM Spectrum Protect 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

An example of a batch file schedule is shown.

About this task

On Windows systems, the schedule service must be running 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 starts the batch file `backup.cmd`. In this example, the command runs the schedule every Friday at 8:00 p.m.:

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

Schedule batch sample

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

Full offline backup batch file sample

```
@echo off
rem Full Offline Backup batch file:
rem -----------------------------------------------------------------------
rem file name: backup.cmd
rem -----------------------------------------------------------------------
rem Sample BRBACKUP batch file
rem -----------------------------------------------------------------------
rem Task:
rem Invokes the SAP utility BRBACKUP in order to perform a full offline
rem backup of all tablespaces using Data Protection for SAP (R)
rem -----------------------------------------------------------------------
rem ***** NOTE ***** NOTE ***** NOTE *****
rem
rem This script is intended only as a model and should be
rem carefully tailored to the needs of the specific site.
rem
rem ***** NOTE ***** NOTE ***** NOTE *****
```

```
rem ------------------------------------------------------------------------
rem
rem For the following examples, the system ID of the ORACLE database
rem is assumed to be "C21".
rem
rem ------------------------------------------------------------------------
rem
rem First, let's do a full offline backup of the ORACLE database. This
rem includes at least files located in the following file systems:
rem c:\oracle\C21\sapdata0
rem c:\oracle\C21\sapdata1
rem c:\oracle\C21\sapdata2
rem c:\oracle\C21\sapdata3
rem c:\oracle\C21\sapdata4
rem
rem Remarks on the parameters of BRBACKUP:
rem
rem -u system/manager ORACLE username/password
rem -c run BRBACKUP in quiet mode
rem -m all backup all tablespaces
rem -t offline perform backup offline
rem
rem The following should be configured within the SAP profile
rem initC21.sap:
rem
rem backup_dev_type = util_file
rem causes BRBACKUP to use the external program
rem Data Protection for SAP (R)
rem util_par_file = %ORACLE_HOME%\database\initC21.utl
rem Data Protection for SAP (R) profile
rem ------------------------------COMMAND---------------------------------
brbackup -u system/manager -c -m all -t offline
```

Full offline backup shell script sample

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

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

Restoring SAP data

Use the Data Protection for SAP file manager for managing restore operations.

Protecting with the Data Protection for SAP file manager

The Data Protection for SAP file manager is a tool that simplifies the Data Protection for SAP inquire, restore, and delete operations.

Before you begin

Before using the file manager review the following details:

- The file manager completes all operations by using the standard functions that are provided by Data Protection for SAP.
- The interface consists of a split window that is character-based. In the left-hand window, all backup IDs found on all IBM Spectrum Protect servers that match the backup ID prefix that is configured in the Data Protection for SAP profile are displayed. In the right-hand window, all the files that belong to the selected backup ID are displayed. Individual backup IDs or multiple files can be selected.

About this task

Users with Oracle database restore and recovery experience should use BR*Tools for restore operations.

Procedure

1. Start the file manager with the path and name of the Data Protection for SAP profile. The user must be a member of the dba group:

   (UNIX or Linux):

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

   (Windows):

   ```
   backfm -p drive:\orant\database\initSID.utl [-o log file directory]
   ```

   If the `-o` parameter is specified at startup, the default directory for log files is changed.
2. The file manager calls the **backint** executable file to connect to the IBM Spectrum Protect server configured in the Data Protection for SAP profile. If this call fails, the file manager shows an error message but does not analyze the cause of the error. Use the **backint** inquire function to analyze the error.
3. An automatic inquire operation for all backup IDs is done by the file manager. The following figure displays a set of backup IDs located by an inquiry procedure. If you mark the backup ID you are interested in and then press the **Tab** key to move the cursor to the right panel, all file names belonging to the marked backup ID is displayed.

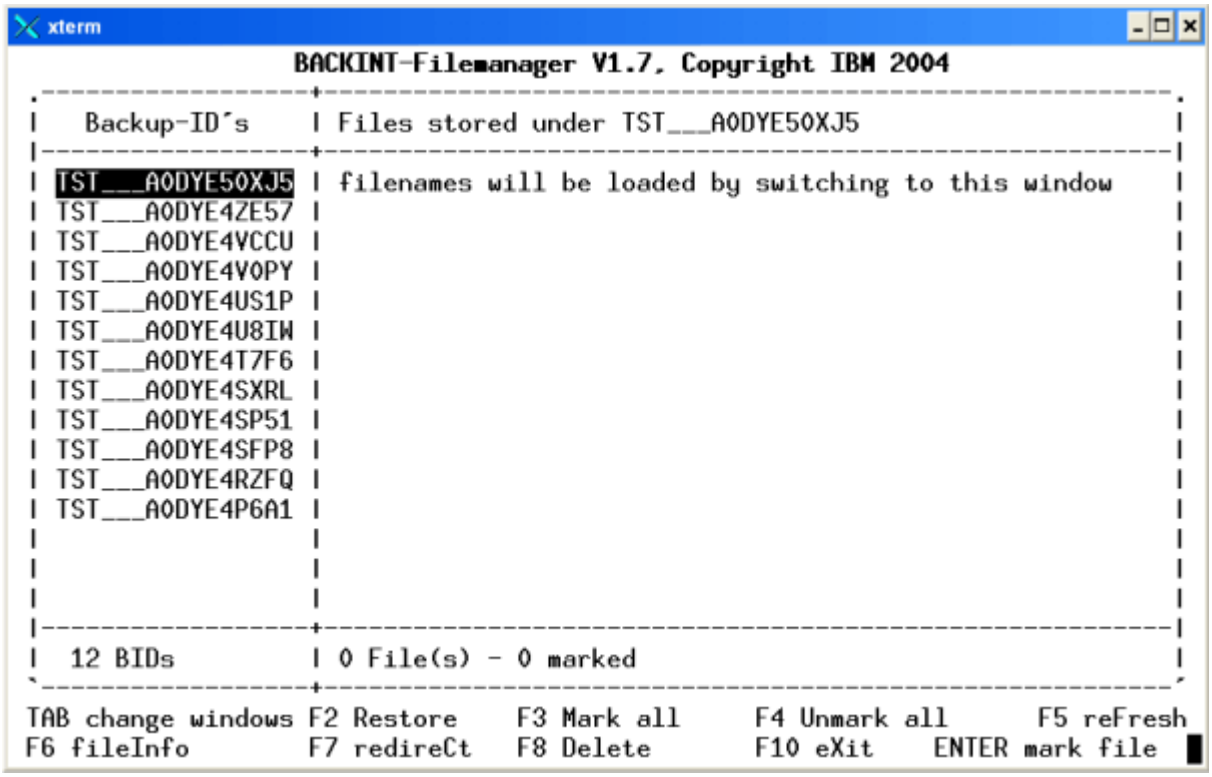

Figure 6. File manager - Result of an inquiry procedure

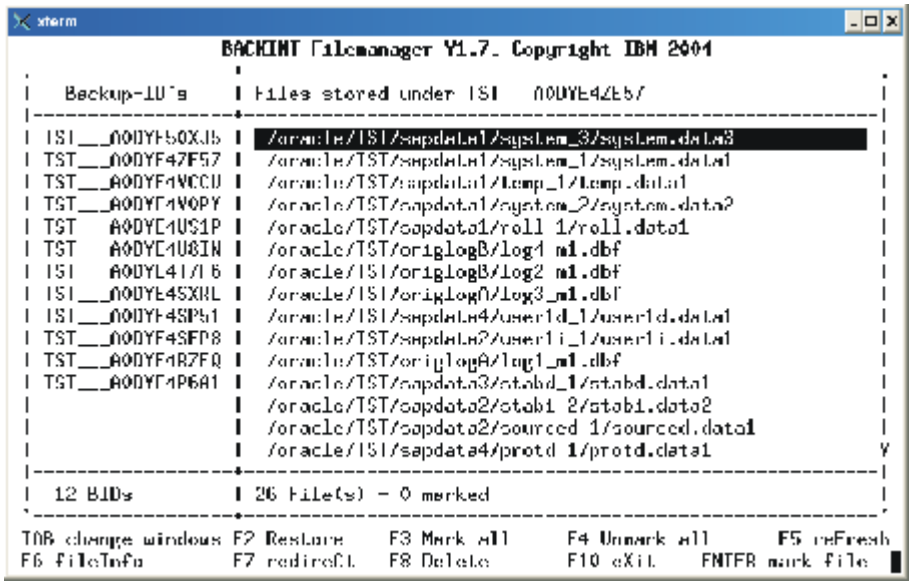

Figure 7. File manager - Result of an inquiry procedure showing file names

Results

The following function keys are defined for restore and delete operations:

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

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

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

For restore operations, the wanted files first must be marked. This action can be done either with the **F3** function key to mark all the files that were found or with the **ENTER** key to mark only one wanted file. Marked files can be identified by the symbol "*"in front of the file name. Only the marked files are restored. For every restore operation, a log file is created in the following location,

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

F3 - Mark all
All files that belong to the current backup ID is marked.

F4 - Unmark all
Unmark all files that belong to the current backup ID.

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

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

For backup IDs, the sequence number is displayed (backup version count). For files, the IBM Spectrum Protect expiration date and time are displayed.

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

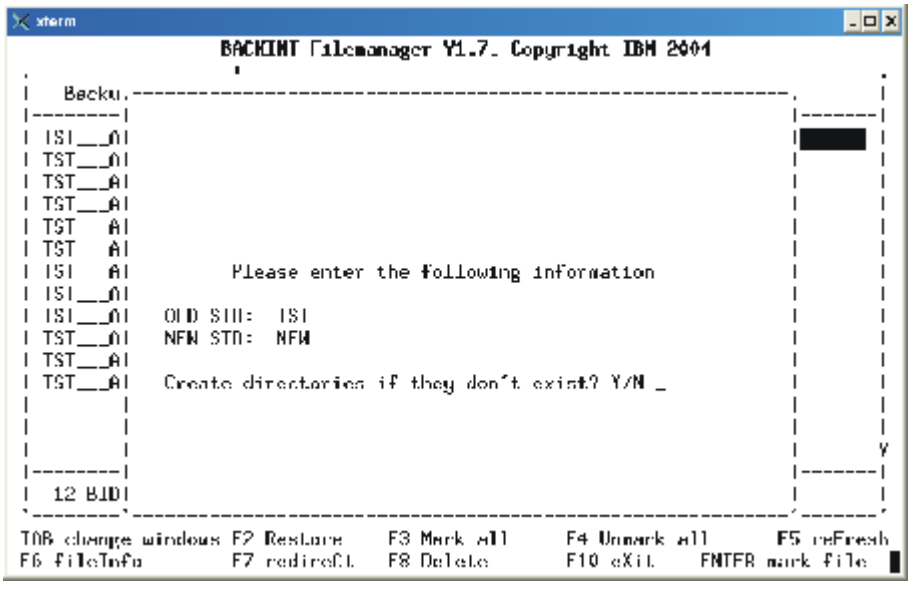

Figure 8. File manager - Result of a redirected restore procedure

F8 - Delete
Delete the selected backup ID and all corresponding files. The file manager can delete backup IDs with all included files. It is not possible to delete single files within a backup ID. To delete a backup ID, it must be highlighted. After you press **F8**, you must confirm the deletion operation. The backup ID and all included files are deleted from the IBM Spectrum Protect server.

F10 - Exit
Exit from Data Protection for SAP file manager

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

Clone the SAP system

SAP system cloning is used to obtain an exact copy of one SAP system, and copy it to a target SAP system.

This information about how to clone a SAP system is to be used to complement the primary SAP documentation

SAP cloning

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

SAP system cloning considered appropriate in these situations:

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

Cloning an SAP system when automatic password handling is used

Clone an original SAP system for copying it to a target SAP system.

About this task

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

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

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

Follow the procedure when automatic password handling `passwordaccess=`*`generate`* is in use:

Procedure

1. Make sure that the same node name and password that are specified in the IBM Spectrum Protect client options file on the source system are specified on the target system.

   Note: Make sure the client uses the password that is stored on the IBM Spectrum Protect server. Although passwords are stored in different locations, the only original password is the one that is on the IBM Spectrum Protect server.
2. Make a backup copy of the client option file on the target system.

3. Copy the client option file from the source system to the target system.
4. Edit the client option file and add `NODENAME source system` to the server stanza.
5. Reset the IBM Spectrum Protect password for the target system node on the server.
6. As root (UNIX or Linux) or administrator (Windows), set the new password on the client.
7. Make a backup copy of the `init`*`SID`*`.utl` file on the target system.
8. Copy the `init`*`SID`*`.utl` file from the source system to the target system. Rename the file from `init`*`SID`*`.utl` to `init`*`target_SID`*`.utl`.
9. Edit the `init`*`SID`*`.utl` file on the target system to reflect all the correct file and path names, especially for **CONFIGFILE** and **TRACEFILE**.
10. Restore the database under the SAP considerations.
11. After the restore, reset the client option file and `init`*`SID`*`.utl` file to their original and set the passwords on the target system.
12. Reset the passwords on the source system.

Cloning an SAP system when manual password handling is used

This procedure describes the tasks for restoring an Oracle SID to a different system with a different SID. Use the procedure that reflects the password-handling method for the environment.

About this task

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

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

Results

Perform these tasks when manual password handling (`passwordaccess=prompt`) is used: If you are using `passwordaccess=prompt`, you must set only the node name and password in the `init`*`SID`*`.utl` file:

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

   ```
   backint -p /oracle/SID/dbs/initSID.utl -f password
   ```

   (Windows):

   ```
   backint -p drive:\orant\database\initSID.utl -f password
   ```

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

Chapter 7. Tuning performance

Information needed to tune Data Protection for SAP performance is provided. A system is considered balanced when the threads on the disk and the network sides are similarly busy throughout the backup, and when resource usage is good. To improve overall throughput, consider adding more resources to create a balanced system.

About this task

In an optimum setup, a slight network bottleneck is preferred. Under certain conditions, the degree of imbalance cannot be determined from the graphical presentation. Depending on your system characteristics that include system buffering and buffer sizes, usage might reduce to almost zero in the graphical presentation although the system is 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. A balanced system, however, does not necessarily mean that the data throughput cannot be improved further. Adding new resources can improve the throughput rate.

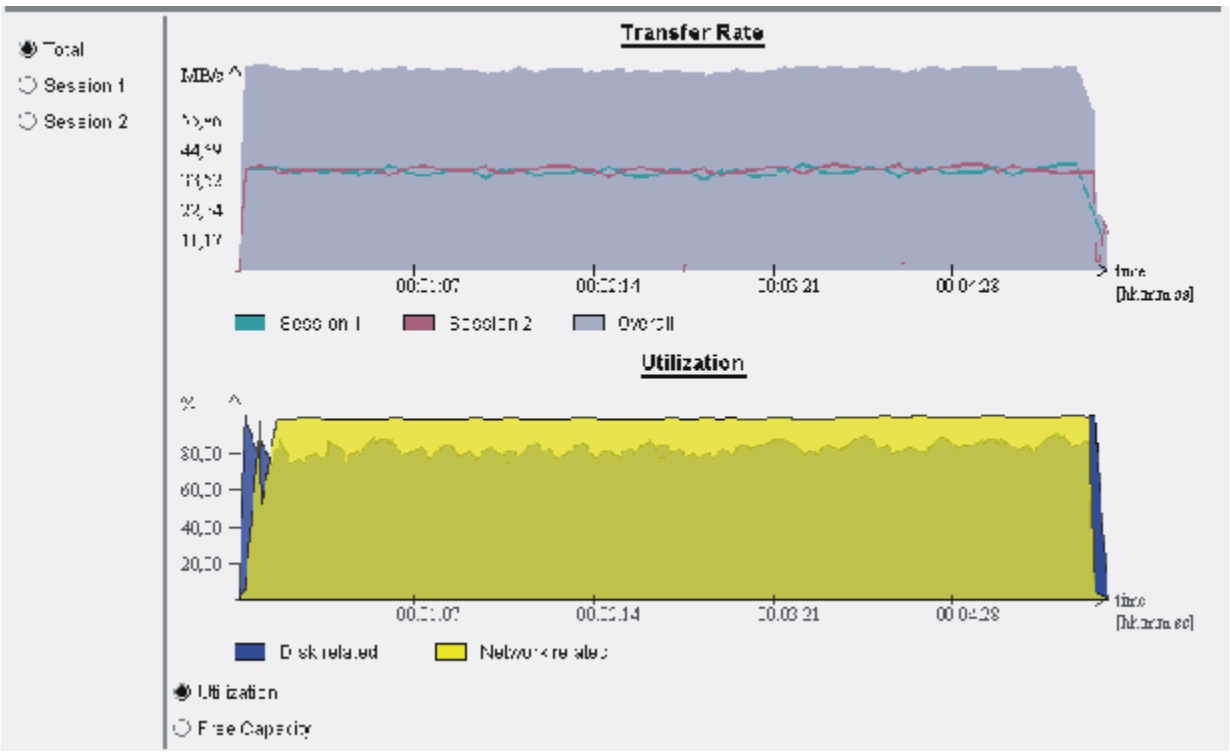

Figure 9. A balanced configuration

Procedure

- Maintain an optimum setup by ensuring tapes are maintained in streaming mode.
- Ensure that there is no network idle time, and that the network is at least as fast as the tape.
- Consider adding new resources to improve the throughput rate.

© Copyright IBM Corp. 1995, 2020

Server-related tuning

You can manage the data that is stored on the IBM Spectrum Protect server for IBM Spectrum Protect for ERP. You can manage which servers are used to store data.

Alternate network paths and servers

Multiple network paths and multiple backup servers can be specified. When the number of available sessions to multiple servers exceeds the number of sessions that are allowed, Data Protection for SAP uses the first sessions that it can establish.

Data Protection for SAP continues to use the number of sessions that are allowed as defined by the MAX_SESSIONS keyword. This setup allows data to be backed up even when a resource (such as an IBM Spectrum Protect server or its network interface) is unavailable. The servers that are used for the backup must be available to restore the data. The days of the week that a server is used can also be specified using the USE_AT keyword. For more information, see the *Profile parameter descriptions* topic.

Options

Use Data Protection for SAP options to tune performance.

Tune performance for Data Protection for SAP by using multiple sessions, network paths, servers, or through multiplexing and other options.

Performance options for Data Protection for SAP

Data transfer rates are impacted by the types of disks that are used for the databases, the network capabilities that are accessed by the database host and the IBM Spectrum Protect server, and the type of storage device that contains the backup.

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

Parallel and 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.

Multiplexing
Multiplexing simultaneously transfers data from different files through one session (MULTIPLEXING) to maximize tape performance. Multiplexing is useful for tape storage since tape drives often have higher data transfer rates than the disks. Combining multiplexing and parallel sessions can optimize overall backup and restore performance.

Disk sorting
Data Protection for SAP uses adaptive file sequencing during backup processing. This sorts database files in sequential order to avoid simultaneously reading files on the same disk. As a result, processing time is reduced.

Multiple and parallel network paths and servers
Improve performance by configuring Data Protection for SAP to distribute a database backup across two or more IBM Spectrum Protect servers. In addition, you can balance network traffic by providing two (or more) separate network connections between the SAP database host and the IBM Spectrum Protect server.

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

Individual tablespace locking
Data Protection for SAP provides a backup profile parameter (`util_file_online`) that minimizes the number of archived redo logs that are backed up during online backup operations. This parameter informs the SAP database utilities of the files (and related table spaces) to be backed up. The SAP utilities then switch those table spaces into backup mode. After the files are backed up, the table spaces are released and a new cycle starts.

RL_COMPRESSION

The RL_COMPRESSION profile keyword is compresses a partially filled database. This process can result in reduced network traffic and fewer tapes that are required for backup.

Adjustments for improving performance of data transfer

Data Protection for SAP is configured to send uncompressed data to the IBM Spectrum Protect server that uses a single session.

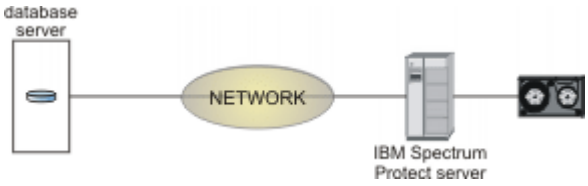

Figure 10. Data transfer for a backup and restore

A single configuration that is best for all environments is not possible or realistic. However, the information that is provided here can help in determining which configuration is best for your environment.

Buffer copies

You can change the Data Protection for SAP options to prevent copying data buffers, the original data buffers are sent between IBM Spectrum Protect components. This change can improve performance.

Data Protection for SAP uses internal buffers to store and exchange data with the IBM Spectrum Protect server. When data is sent from one component to another, data buffers are copied by default. Data Protection for SAP can prevent copying data buffers by sending the original data buffers. This process reduces the CPU load of the database server.

Buffer size

Adjust buffer size disk I/O to improve transfer rates.

The internal data buffer size can be adjusted for Data Protection for SAP. These buffers are used for reading the disk and sending data to the IBM Spectrum Protect client API. The default values typically produce acceptable performance.

Optimize the buffer size for disk I/O to improve transfer rates. For disk subsystems, the best transfer rates are achieved when the buffer size is set equal to the stripe size. Before you increase the size of internal buffers, however, ensure that sufficient storage is available for the number of buffers that are specified by Data Protection for SAP. This number correlates to the number of sessions requested. The number of buffers doubles when compression is specified.

Compression of data for backup

You can adjust the amount of data that is being sent to the IBM Spectrum Protect server by compressing zero-byte blocks (RL_COMPRESSION profile keyword).

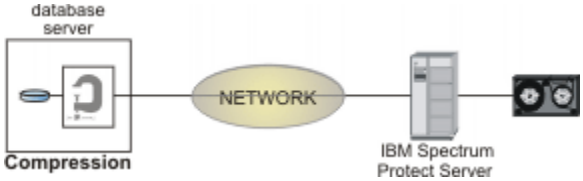

Figure 11. Null Block Compression

Data Protection for SAP can decrease the amount of data that is sent to the IBM Spectrum Protect server by compressing zero-byte blocks. Compression can increase the CPU load on the database server and can improve performance in situations when the network is at 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, in the *Profile parameter descriptions* topic, for details on how to activate Data Protection for SAP compression.

Automation options

You can improve administrative productivity by using the Data Protection for SAP automation options.

Selectable management classes

Specify different IBM Spectrum Protect management classes for backup data and archive data. Configure Data Protection for SAP to back up directly to a tape storage pool and to archive log files to a disk storage pool.

Multiple management classes can be specified to use with multiple Oracle redo log copies. The profile keywords BRARCHIVEMGTCLASS and BRBACKUPMGTCLASS in the *Profile parameter descriptions* topic provides information about specifying management classes.

Retain backups by version

Retaining backups by version, limits the number of full backups that are retained on the IBM Spectrum Protect server. When the number of full backups on the server exceeds the value of the **MAX_VERSIONS** parameter, the oldest versions are deleted. Retaining backups provides a trace of all redo log files, database control files, and partial and incremental backups that are associated with a full backup. All these objects are removed together with the full backup.

Important: If a backup is created when the profile parameter **MAX_VERSIONS** is set to zero, this backup is excluded from the backup versions processing. It is not considered when counting the number of backup generations, and it is not deleted when it becomes older than the backups that are retained.

Multiple redo log copies

Backing up multiple copies of a log file in a single archive operation helps protect data in the event of tape defects or disaster recovery situation. These copies can be on different physical IBM Spectrum Protect volumes or different IBM Spectrum Protect servers. When a log file copy is unavailable at restore time, Data Protection for SAP automatically switches to another copy. It continues restoring the log file from that copy. The description of the profile keyword REDOLOG_COPIES, in the *Profile parameter descriptions* topic, provides detailed information about creating and by 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 IBM Spectrum Protect servers. Also using multiple network connections to the IBM Spectrum Protect server can help. In this configuration, Data Protection for SAP checks all servers and network connections for availability, and then does the backup even if some resources are unavailable.

Policies can also be set that use different IBM Spectrum Protect 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 IBM Spectrum Protect server.

Frontend and 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 the *Profile parameter descriptions* topic.

Data transfer

When you use Data Protection for SAP, data is passed from disk through to the network and finally to tape. A balanced configuration can help to prevent bottlenecks and to ensure optimized performance.

Data throughput rate

Throughput rates differ for different environments because of different disk, network bandwidth, server systems, number of tapes, and configuration settings. When you are moving data, certain elements that are used in the movement of data can be tuned to improve data throughput.

Throughput rates differ widely among various environments because of different disk, network bandwidth, server systems, number of tapes, and configuration settings. The information that is provided here concentrates on selected elements that are involved in the movement of data. This information determines how to use existing resources to their maximum efficiency and provide insight as to how throughput can be improved.

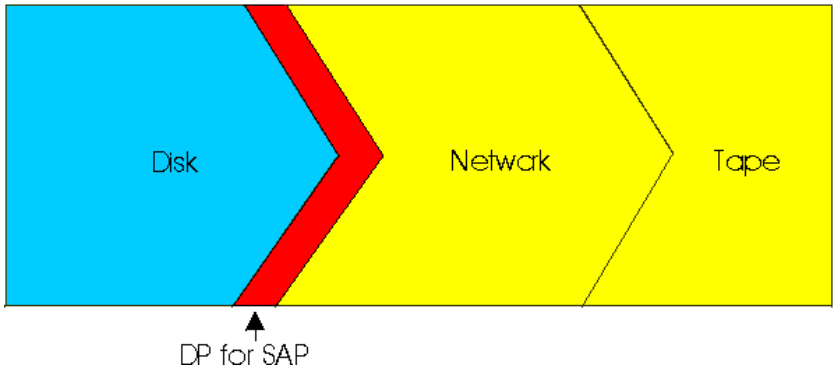

Figure 12. High-level view of the data flow during backup

From a high-level view, the data packages must send these elements when it does a backup with Data Protection for SAP: Data is read from disk that is 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. This situation 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 the logfile as the average transmission rate. However, identifying bottlenecks that are derived from log file messages is difficult. For this analysis effort, Data Protection for SAP provides performance sensors that indicate a bottleneck. These bottlenecks are located either in the elements that are represented in blue (for disk) or in yellow (for network and tape respectively) in the graphic.

Performance sensors

Data Protection for SAP 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 function provides a way to determine whether the streams of incoming and outgoing Data Protection for SAP data are balanced.

The method of transferring data packages depends on how IBM Spectrum Protect is configured. In a standard configuration, the data packages are sent from the IBM Spectrum Protect API client through the network to the backup server. In an environment that is configured for LAN-free operations, the data packages are processed by the IBM Spectrum Protect API client and the IBM Spectrum Protect Storage Agent.

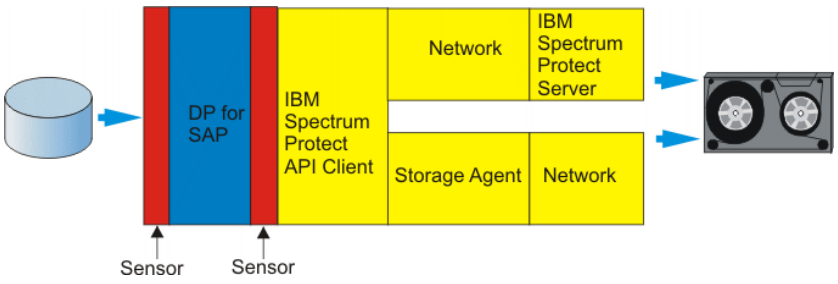

Figure 13. Performance optimizing by using sensors

When a backup operation begins, filling the buffers is necessary before the effects of a bottleneck are viewable.

Performance tuning for data transfer

During data transfer, a continuous stream of data is generated between the SAP database server, the network, and the IBM Spectrum Protect server. The weakest component in this stream decreases the overall data transfer rate.

There are three main components that are involved during a Data Protection for SAP data transfer:

- The SAP database server.
- The network.
- The IBM Spectrum Protect server, which is also referred to as a backup server.

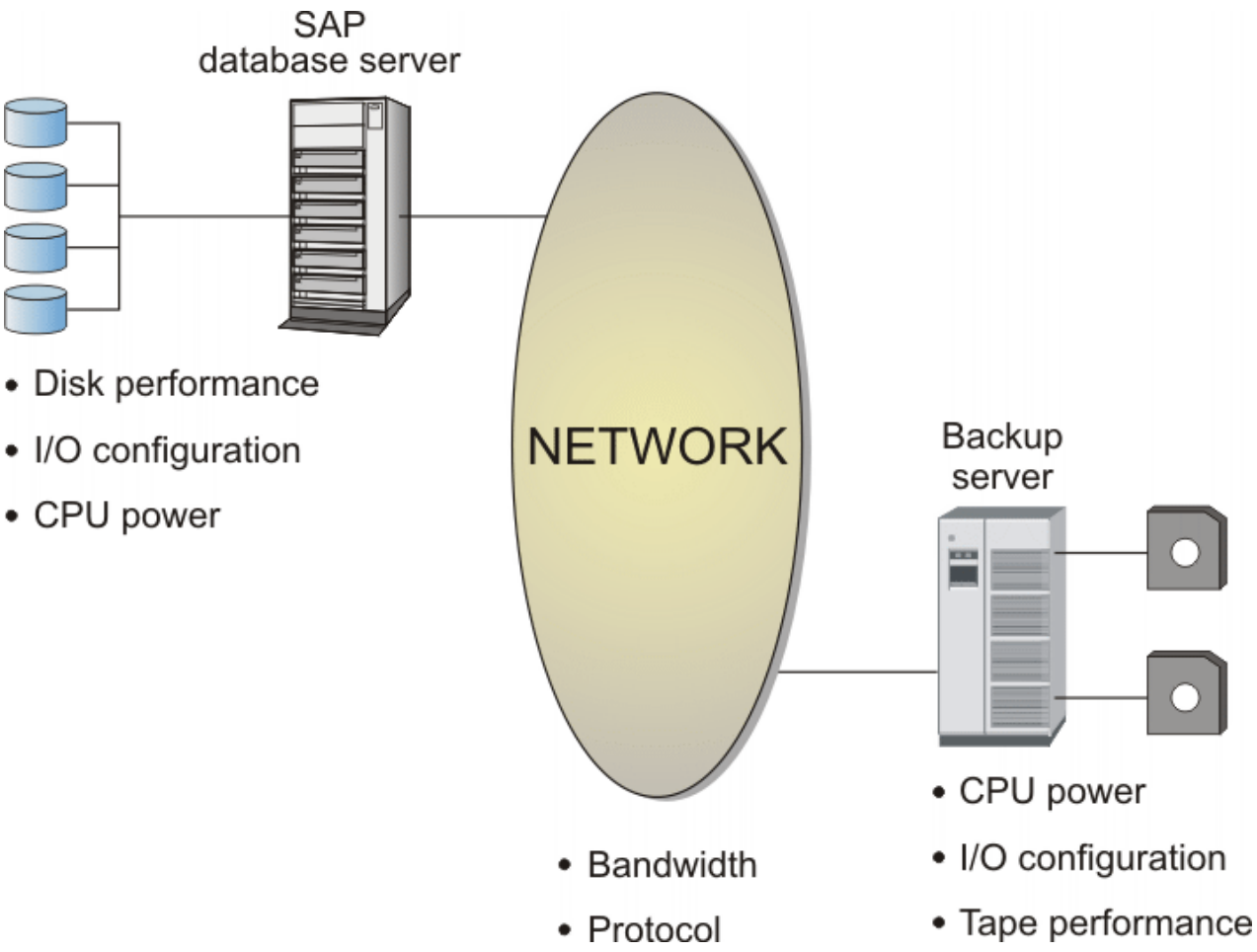

Figure 14. Data Protection for SAP data transfer

Multiple servers

Data Protection for SAP 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.

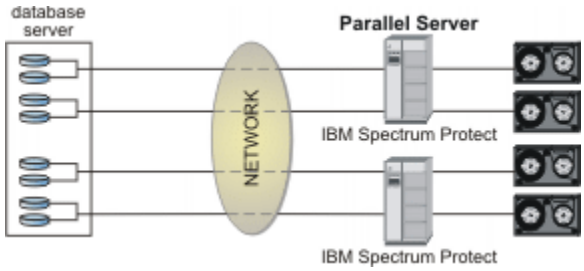

Figure 15. Multiple servers

A server statement must be entered in the Data Protection for SAP profile for each adapter of the backup server. A description for the SERVER keyword is given in the *Profile parameter descriptions* topic. The value of the MAX_SESSIONS keyword is not greater than the sum of all SESSION values specified for the SERVER statements that are used concurrently.

When RMAN is used, the number of SESSION configured for each SERVER must be greater than or equal to the number of sessions that are configured for the MAX_SESSIONS keyword that are specified during restore operations. This configuration prevents RMAN from requesting a number of objects (in parallel from the same server) that exceeds the number of sessions that are available for that server.

Multiple sessions

You can use multiple tape drives simultaneously to increase the transfer rate to or from the IBM Spectrum Protect server. Several backup sessions access the database in parallel on the database server, and the data is written simultaneously to several tape drives.

Figure 16. Parallel (multiple) sessions

The Data Protection for SAP Oracle keywords MAX_SESSIONS, MAX_BACK_SESSIONS, MAX_ARCH_SESSIONS, MAX_RESTORE_SESSIONS, and are keywords used for defining the number of parallel sessions to be established with the IBM Spectrum Protect server for database backup, archive (backup of log files) and restore. When you run a database backup, the data is typically written directly to tape drives on the IBM Spectrum Protect server. The parameter that is specified in the MAX_SESSIONS keyword must match the number of tape drives that are used simultaneously.

These must be available to the management class defined as BRBACKUPMGTCLASS in the Data Protection for SAP profile. When you set up the IBM Spectrum Protect server, make sure not to activate collocation in the (tape) storage pool that is defined for the management class that is chosen as BRBACKUPMGTCLASS. In addition, ensure that as many tape drives for this management class are available as the number of sessions that are defined in MAX_SESSIONS. Multiple access to the same tape might slow down data transfer.

These must be available to the management class defined as BRARCHIVEMGTCLASS in the Data Protection for SAP profile. If you are using tape pools as primary pools for this management class, these considerations for database backups also apply to disk storage pools:

- Several sessions of one BRARCHIVE operation can use one or two independent disk storage pools.
- Several sessions of BRARCHIVE operations of different databases can simultaneously use one or two independent disk storage pools.

The number of storage pools that are required depends on the number of backup copies that are requested for a log file.

Multiplexing

Multiplexing uses parallel access points to data on the database server. This configuration is useful when tape drives are used during database backup operations on the backup server.

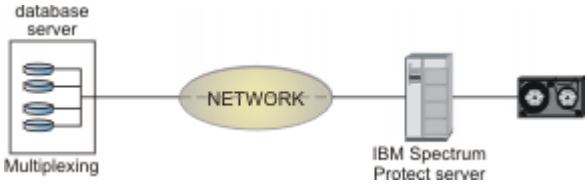

Figure 17. Multiplexing

The value of keyword MULTIPLEXING defines the number of files that are read in parallel within a single session. Appropriate MULTIPLEXING values are expected in the range of 1 to 4. The best value for your environment depends on the I/O rate of your disks, the location of your data on the disks, the network capacity, the throughput rate of the storage media, and the compression setting. If the MULTIPLEXING value is too high, the processing that occurs might offset any performance gain.

Multiple network paths

Data Protection for SAP allows multiple network connections (paths) for data transfer between the database server and the backup server. Parallel paths can be used to eliminate network points of constraint.

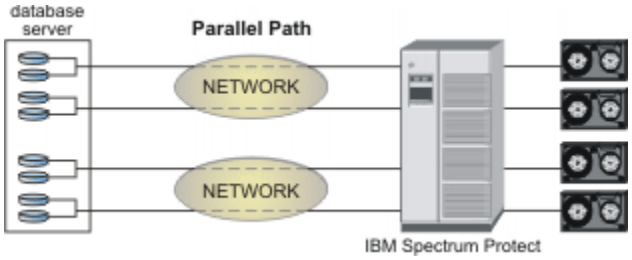

Figure 18. Parallel (multiple) paths

For each additional path, more 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. This scenario is described for the SERVER keyword in the *Profile parameter descriptions* topic. The value of the MAX_SESSIONS keyword is not greater than the sum of all SESSION values specified for the SERVER statements that are used concurrently. Detailed information about setting up multiple parallel network paths is described in the *Parallel backup paths and backup servers* topic.

Chapter 8. Troubleshooting

To assist with troubleshooting and problem determination, diagnostic files and system information are displayed in a centralized location. Investigating the details in log files helps to troubleshoot problems.

About this task

Investigate and compare the log files of the application and the IBM Spectrum Protect server activity log to find out the differences between successful and unsuccessful operations. The log file names are provided for reference:

- `brbackup` / `brrestore log`
- `sbtio.log`

Look for one of these patterns when a problem occurs:

- The problem always occurs at the same time. If this condition is true, view the appropriate log files to determine if scheduled processes are occurring simultaneously. Examples of such processes are virus checker, automatic updates, or batch jobs.
- The problem always occurs after another operation is done or the same operation is done.
- The problem occurs when another application or process is processed in parallel.

Troubleshooting common problems

Compare the log files of the application in question (`brbackup` / `brrestore log`, `sbtio.log`, and the IBM Spectrum Protect server activity log) to find out the differences between successful and unsuccessful operations.

About this task

When problems occur, look for one of the following patterns:

- The problem always occurs at the same time. If this condition is true, view the appropriate log files to determine whether there are any scheduled processes that occur simultaneously. Examples of such processes are virus checker, automatic updates, or batch jobs.
- The problem always occurs after another operation is done or the same operation is done.
- The problem occurs when another application or process is processed in parallel.

Reproducing problems

Use the checklist to che\ck what caused the problem, and then attempt to reproduce the problem.

About this task

When you encounter a problem that occurs during an operation that previously ran successfully, review this list to determine the root cause of the problem.

- The setup changed.
- One or more of the operating system, network, database, or hardware components changed.
- Patches or updates to one or more of the components were applied.
- Changes occur that originate by the system:
  - Check whether the disks are running full with the UNIX or Linux `df` command.
  - If network performance decreases, check whether additional hosts, additional applications, or defects in software or hardware occurred. Compare the log files. The log file names are provided for reference:

© Copyright IBM Corp. 1995, 2020

- brbackup / brrestore log
- sbtio.log

– If IBM Spectrum Protect server processing decreases, check whether more clients or more operations were added. Information is also available in the IBM Spectrum Protect server activity log.

If none of these changes caused the problem, view the last modified time stamp of the configuration files (init*SID*.utl, init*SID*.sap, dsm.sys, dsm.opt, /etc/services, /etc/inittab. This UNIX or Linux command lists all files in the /etc directory, which are modified during the previous five days:

```
find /etc -type f -ctime 5 -print
```

If you can identify changes that are 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 supports both IPv4 and IPv6 for internal communication.

Data Protection for SAP supports both IPv4 and IPv6 for internal communication in that it runs in IPv4, IPv6, and mixed environments on AIX and Linux. However, these products do not use IPv6. 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 listens for both IPv4 and IPv6 connection requests if the system is configured accordingly. Connection requests to ProLE are made for the addresses that are returned by the system for the respective port on the local host. Connection requests to other systems are made for the addresses that are 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 must be changed to *service or port*@*IP address* if the IP address is specified in the IPv6 notation. If 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.

Log files that contain information and messages

Data Protection for SAP processes are recorded in log files. Information about backup operations can be used to determine which backup should be used to restore your data.

The backint.log log file contains the IBM Spectrum Protect for ERP data for all database and redo log file backup and restore operations that complete successfully or fail.

The Backup Object Manager writes to the backom.log log file.

These files are in the following paths:

- UNIX or Linux: $SAPDATA_HOME/sapbackup for backup and restore runs
- UNIX or Linux: $SAPDATA_HOME/saparch for redo log archive runs

Windows:

- %SAPDATA_HOME%\sapbackup for backup and restore runs
- %SAPDATA_HOME%\saparch for redo log archive runs

All log files that are written during a backup, restore, or archive operation are listed in summary log files with start and end time stamps. The summary log files are in the same directory as the log files themselves and have the following names:

- back*SID*.log
- rest*SID*.log
- arch*SID*.log

If you are running Oracle RMAN, the log file `sbtio.log` (which is specified by `user_dump_dest` in the Oracle control files) might also must be viewed. For most installations, this file is defined as `$SAPDATA_HOME/saptrace/usertrace/sbtio.log`. This file contains all messages that are issued by the Data Protection for SAP RMAN connector during operation of Oracle RMAN.

Setup requirements

When you are troubleshooting issues while using Data Protection for SAP software there are items that you can check to ensure that the setup completed correctly.

Review these considerations to better understand the installation setup on UNIX or Linux systems:

- Make sure an entry similar to this example is defined in the `/etc/inittab` file:

```
po64:2:respawn:/usr/tivoli/tsm/tdp_r3/ora64/prole -p tdpr3ora64
Server component hostname 5126
```


```
po64:2:respawn:/usr/tivoli/tsm/tdp_r3/ora64/prole -p tdpr3ora64
Server component hostname 5126
```


  This entry starts a daemon process for ProLE. This process listens on the following ports:

  – Data Protection for SAP port `tdpr3ora64` for **backint**.
  – RMAN connections for Oracle 64-bit port `tdpr3ora64` for **backint**, RMAN connections, and Data Protection for SAP.

  The port can have a different name; however, the name must match the name in the `/etc/services` file as shown in this example:

```
tdpr3ora64      57323/tcp
```

  The lines are added to the `/etc/services` file during the installation process.
- Make sure the Data Protection for SAP configuration file `init*SID*.utl` is in the `$ORACLE_HOME/dbs` directory.
- When you use the BR*Tools with Data Protection for SAP, modify the `init*SID*.sap` file by setting `backup_dev_type = util_file` and variable `util_par_file` to the fully qualified path and file name of `init*SID*.utl`.

Review these considerations to better understand the installation setup on Windows systems:

- Make sure that all files are installed.
- 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 the example:

  (Data Protection for SAP for Oracle)

```
tdpr3ora64      57323/tcp
```

  The example shows the Data Protection for SAP 64-bit port. For Data Protection for SAP for Oracle, this port name is needed for the `init*SID*.sap` file when RMAN is configured.
- Make sure the Data Protection for SAP configuration file `init*SID*.utl` is in the `%ORACLE_HOME%\database` directory.
- Make sure the Data Protection for SAP configuration file `init*SID*.utl` is in the `%ORACLE_HOME%\database` directory (on Oracle).
- When you use the BR*Tools, modify the `init*SID*.sap` file by setting `backup_dev_type = util_file` and variable `util_par_file` to the fully qualified path and file name of `init*SID*.utl`.

- The names of the IBM Spectrum Protect servers that are specified in `init`*`SID`*`.utl` must match the names in the `dsm.sys` file. If the IBM Spectrum Protect API or IBM Spectrum Protect backup archive client are installed into their default locations, then it is not necessary to set the DSMI_* variables. If the variables are set, however, make sure that 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 that are specified by these variables.

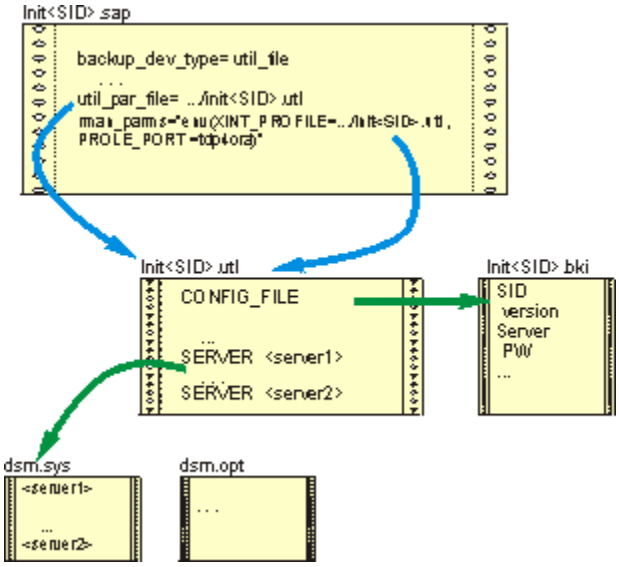

Figure 19. SAP and Data Protection for SAP for Oracle configuration files on UNIX or Linux

On UNIX or Linux systems, the names of the IBM Spectrum Protect servers that are specified in `init`*`SID`*`.utl` must match the names in the `dsm.sys` file. If the IBM Spectrum Protect API or IBM Spectrum Protect backup archive client are installed into their default locations, then it is not necessary to set the DSMI_* variables. If the variables are set, however, make sure that 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 that are specified by these variables. Also, verify that write permissions exist for the `init`*`SID`*`.bki` file as this file is the only one 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 that is specified in the `init`*`SID`*`.utl` file. The environment variable *DSMI_CONFIG* must specify an option file within this directory. *DSMI_CONFIG* is to specify the `dsm.opt` file in this directory. The *DSMI_DIR* environment variable must also specify the directory where the IBM Spectrum Protect API message text file is in. This example shows a typical the `c:\Program Files\Tivoli\tsm\api64` directory.

Information to collect for support

When you contact support, you must be able to provide the following information.

- The Data Protection for SAP version level.
- The operating system level and patches that were applied.
- The version level.
- The IBM Spectrum Protect server version.
- The IBM Spectrum Protect server operating system level.
- Data Protection for SAP configuration file (`initSID.utl`) including IBM Spectrum Protect client configuration files (`dsm.sys`, `dsm.opt`).
- Data Protection for SAP profile (`initSID.utl`).
- BR*Tools output for the operation in question (BRARCHIVE, BRRESTORE).

- The change history of the system components (if the process worked previously).

More information might also be requested from the service representative.

Troubleshooting problems

Information about how to resolve errors that might occur is provided.

Text that is displayed on the screen during `brbackup`, `brrestore`, and SAP tools operations are typically written to a log file. Oracle also writes internal operations in the alert log and core files in the directory that is specified in the Oracle control files, for example `$SAPDATA_HOME/saptrace/background/alert_SID.log`.

Messages

During BR*Tools processing, logs that contain all issued messages are written to paths `/oracle/SID/sapbackup` (for BRBACKUP) or `/oracle/SID/saparch` (for BRARCHIVE).

The message prefix indicates the issuing components. Refer to the documentation for the component that issued the message for detailed information. However, the following prefixes are used when you use BR*Tools with Data Protection for SAP:

*Table 6. Prefixes when you use BR*Tools*

Prefix	Issuing component
ANS / ANR	IBM Spectrum Protect
BKI	Data Protection for SAP
BR	BR*Tools
ORA	Oracle database kernel
RMAN	RMAN

File manager

The most important requirement for file manager is that Data Protection for SAP is set up correctly.

This requirement is especially true in regard to the **backint** executable file. This file must be able to connect to the IBM Spectrum Protect server without errors. If this call fails, the file manager displays an error message but does not analyze the reason for the failure. To analyze the error, start **backint** manually with the inquire function and check the output for error messages.

BACKINT problem resolution

Make sure that the BACKINT interface is working correctly before you examine the RMAN interface.

About this task

The following figure displays how to isolate the problem when the settings performed by the installer are verified.

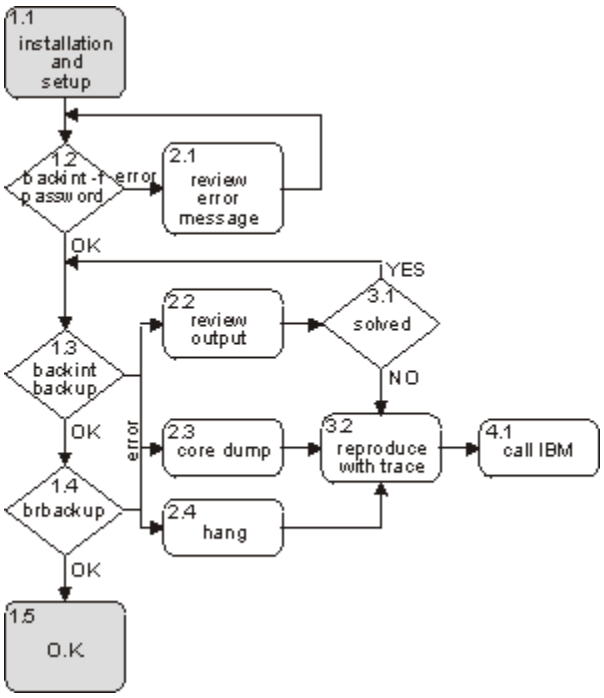

Figure 20. Problem isolation for BACKINT

After installation is completed (Step 1.1) and manual password handling is specified, set the password (Step 1.2). 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 that is configured within the `init`*`SID`*`.utl` file. An error message displays when a problem occurred.

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 by using the option `-p`*`PORT`*, check this port as well. If all of this effort does not help, start the ProLE from another shell on UNIX or Linux with this command:

```
prole -p PORT
```

Issue this command on Windows:

```
prole -console -p PORT
```

Attempt to start **backint** again.

BKI5001E: IBM Spectrum Protect Error: Server not found in configuration file
On UNIX or Linux, the IBM Spectrum Protect server that is defined in the `init`*`SID`*`.utl` file does not match the server that is specified in the `dsm.sys` file. On Windows, the *`server`*`.opt` file might be missing.

BKI5001E: IBM Spectrum Protect Error: ANS1353E (RC53) Session rejected: Unknown or incorrect ID entered
This message can display when the node in the server stanza of the UTL file is not valid on the server.

HANG
If **backint** hangs after the password is entered, the server IP address that is 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 do a backup by using **backint** to verify the settings are correct. When the backup completes successfully, the message #SAVED*BIDFILENAME* displays for each saved file and `BKI0024I: Return code is: 0` also displays. If an error message displays, view the error description in *IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP Messages* for information about how to resolve it. The primary Data Protection for SAP setup is almost complete. The BR*Tools and Oracle (when you use RMAN) must also be configured correctly. Proceed to Step 1.3 and start `brbackup`.

RMAN problem resolution

To isolate problems that occur when you use RMAN, there are a series of checks to complete.

About this task

The following graphic provides information to isolate problems that occur when you use RMAN.

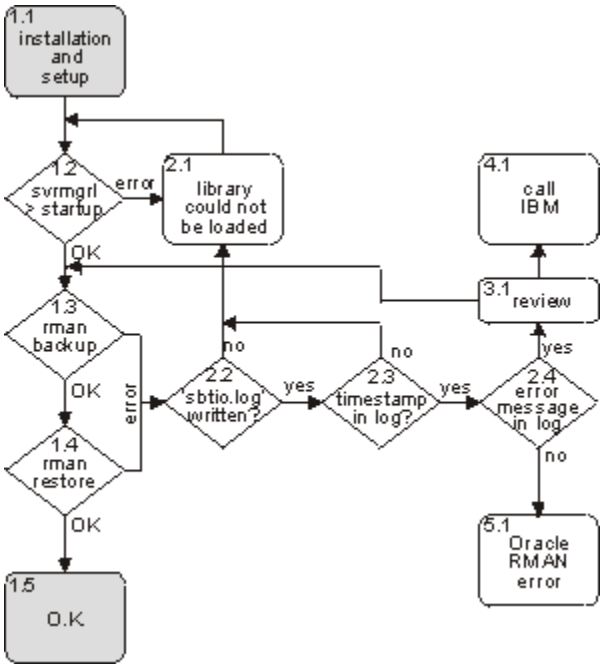

Figure 21. Problem isolation for RMAN

After Data Protection for SAP and Oracle are configured to work together (Step 1.1), attempt to start Oracle by using the server manager `svrmgrl` (on UNIX or Linux) or `svrmgr30` (on Windows) with Oracle 8.x. Use SQL Plus (`sqlplus`) with Oracle 9.x. When an error occurs while you use RMAN, always view the `sbtio.log` file first. This file is in the directory that is specified by the `user_dump_dest` keyword in the Oracle `init`*`SID`*`.ora` profile (at `$ORACLE_HOME/saptrace/usertrace/sbtio.log` by default). If the `sbtio.log` file does not exist (Step 2.2), then either Oracle was unable to load the shared library that contains the RMAN connector for Data Protection for SAP or an error was encountered before the Data Protection for SAP library was called. In both cases, an Oracle error message exists in the `brbackup` log file that begins with ORA-, PLS-, or RMAN-. Try to resolve this problem by using the Oracle and SAP®

documentation. If the `sbtio.log` file exists, search for a message beginning with BKI*XXXXY* where *XXXX* is a four-digit number and *Y* is the letter I, W, or E. When such a message occurs, the RMAN connector for Data Protection for SAP loaded correctly and was called by RMAN. This is the first message for every new session in Step 2.3:

```
BKI7060I: Data Protection for SAP version and build number session: 764
```

If this message is not available, Oracle loaded an incorrect library.

Perform these tasks on Windows when an incorrect library is loaded by Oracle:

Procedure

1. Remove or rename all occurrences of the file `orasbt.dll` except the one in the Data Protection for SAP installation directory. Then, copy this one to `%ORACLE_HOME%\bin`.
2. Stop the `OracleService`*SID* and restart it.

Results

Several factors must be considered when an incorrect library is loaded by Oracle on UNIX or Linux. For example, the RMAN library `libtdp_r3.`*ext* is not located by the Oracle executable file. Oracle suggests using the *SBT_LIBRARY* variable to specify the library. However, do not use this variable for a version of Oracle before Oracle 9.2. Oracle recommends not to issue the **make** command. However, this recommendation is not applicable for all combinations of operating system and Oracle combinations. As a result, issuing the **make** command on any UNIX or Linux system with Data Protection for SAP is acceptable. When issued correctly, this command can confirm that the library and the Oracle executable files are compatible. Also, make sure the library and soft link that is entered during the command exists and that the soft link is valid:

```
make -f ins_rdbms.mk ioracle LLIBMM=lib or link
```

It might be helpful to add the location of the link or library to the **LIBPATH** environment variable (on AIX) or to the **LD_LIBRARY_PATH** environment variable (on other UNIX or Linux systems).

On Windows based systems, the location of `orasbt.dll` must be in the **PATH**. Also, ensure that you have only one `orasbt.dll` in your system's **PATH**. Check if a core file is written or if Oracle wrote a trace within the `saptrace/usertrace` directory.

In (Step 2.4) the file `sbtio.log` is written and you find an error message that starts with BKI. Using the **backint** executable file to determine any problems might make it easier because you can see all messages on the screen. Also, if something goes wrong, you do not disturb Oracle. If **backint** is working as expected, return to problem determination with RMAN.

There must be a connection that is established to ProLE and the IBM Spectrum Protect server, and a password must be set (by using **backint**) as well. If some of these steps fail, you get the same error messages with RMAN as you get with **backint**.

Manually start Data Protection for SAP

Information about how to start Data Protection for SAP from the command line to assist with troubleshooting efforts is provided.

Data Protection for SAP is typically started by the BR*Tools utilities with a set of appropriate parameters. For troubleshooting purposes, call Data Protection for SAP directly from the command line:

```
backint -?
```

This command displays a list of all possible Data Protection for SAP command-line options. You can manually run data protection operations that can assist with correcting errors. For the C shell, enclose the option string in quotation marks (`backint '-?'`).

Backup function
Data Protection for SAP is typically started by the BR*Tools utilities with a set of appropriate parameters.

About this task

For troubleshooting purposes, call Data Protection for SAP directly from the command line:

```
backint -?
```

This command displays a list of all possible Data Protection for SAP command-line options. You can manually run data protection operations, which can assist with correcting errors. For the C shell, enclose the option string in quotation marks (`backint '-?'`).

The backup function is typically started by the SAP database utilities BRBACKUP and BRARCHIVE. For **backup** and **inquire**, these programs provide an input file to Data Protection for SAP. The file contains the names and paths of the database files to be processed. For troubleshooting, it might be necessary to directly call this Data Protection for SAP function directly to back up individual files as shown in these examples. Issue this command on UNIX or Linux systems:

```
backint -p /oracle/SID/dbs/initSID.utl -f backup
```

Issue this command on Windows systems:

```
backint -p drive: or UNC name\orant\database\initSID.utl -f backup
```

The Data Protection for SAP profile `initSID.utl` must be specified with the path and file name statement as shown in the examples. The program prompts you to enter one (or more) file names. Every successful backup operation (collection of one or more files) is allocated its own backup ID within IBM Spectrum Protect. Remember to press `CTRL + D` (on a UNIX or Linux system) or `CTRL + Z` (on a Windows system) after the file name to back up is entered.

Delete function
Data Protection for SAP is typically started by the BR*Tools utilities with a set of appropriate parameters.

About this task

For troubleshooting purposes, call Data Protection for SAP directly from the command line:

```
backint -?
```

This command displays a list of all possible Data Protection for SAP command-line options. You can manually run data protection operations, which can assist with correcting errors. For the C shell, enclose the option string in quotation marks (`backint '-?'`).

The delete function is used as part of the Data Protection for SAP version control mechanism. It can be called only by Data Protection for SAP or by a user. This function can be started from the command line as shown in these examples. Issue this command on UNIX or Linux systems:

```
backint -p /oracle/SID/dbs/initSID.utl -f delete
```

Issue this command on Windows systems:

```
backint -p drive: or UNC name\orant\database\initSID.utl -f delete
```

You are prompted to enter the backup ID to be deleted. It is not possible to delete single files within a backup ID. You can delete only complete backup IDs.

Inquire function
Data Protection for SAP is typically started by the BR*Tools utilities with a set of appropriate parameters.

About this task

For troubleshooting purposes, call Data Protection for SAP directly from the command line:

```
backint -?
```

This command displays a list of all possible Data Protection for SAP command-line options. You can manually run data protection operations, which can assist with correcting errors. For the C shell, enclose the option string in quotation marks (`backint '-?'`).

The inquire function is typically started by BR*Tools and BRRESTORE. The function is used to query the IBM Spectrum Protect server for backup IDs or files, which belong to a particular backup ID. For troubleshooting purposes, however, it might be necessary to start this function manually as shown in these examples. Issue this command on UNIX or Linux systems:

```
backint -p /oracle/SID/dbs/initSID.utl -f inquire
```

Issue this command on Windows systems:

```
backint -p drive: or UNC name\orant\database\initSID.utl -f inquire
```

Data Protection for SAP prompts you to enter the inquiry in one of these four formats:

#NULL:
Display all backup IDs that are saved to this point. A typical line of the response might be #BACKUP `JE0___A0DNE9Z74C`. The backup ID in this case is `JE0___A0DNE9Z74C` (#BACKUP does not belong to the backup ID). The first six characters are the user-defined prefix. The next 10 characters represent a unique ID of the backup.

BackupID:
Display all of the files, which belong to that backup ID. A typical result might be ##BACKUP `JE0___A0DNE9Z74C /oracle/C21/dbs/initC21.utl`.

NULL `filename`:
Display all of the backup IDs corresponding to the specified file. *Filename* requires an input that consists of path and name of the file.

BackupID `filename`:
Verify whether a particular file is saved under a certain backup ID. *Filename* requires an input that consists of path and name of the file.

Restore function
IBM Spectrum Protect for Enterprise Resource Planning is typically started by the BR*Tools utilities with a set of appropriate parameters.

About this task

For troubleshooting purposes, call Data Protection for SAP directly from the command line:

```
backint -?
```

This command displays a list of all possible Data Protection for SAP command-line options. You can manually run data protection operations, which can assist with correcting errors. For the C shell, enclose the option string in quotations (`backint '-?'`).

The restore function is typically started by the SAP® database utility BRRESTORE. For troubleshooting, it might be necessary to directly call this Data Protection for SAP function directly to restore individual files as shown in these examples. Issue this command on UNIX or Linux systems:

```
backint -p /oracle/SID/dbs/initSID.utl -f restore
```

Issue this command on Windows systems:

```
backint -p drive: or UNC name\orant\database\initSID.utl -f restore
```

You are prompted to enter the backup ID and the full file names of the files to be restored. If the files are to be restored to another directory, it is necessary to specify the path to the input files. If a file is restored directly, any existing file with the same name is overwritten without warning. When it is necessary to remove an error, restore database files directly only in a controlled manner. In normal operation, a database is never to be restored directly because the SAP database might become corrupted.

Loading the message catalog

When IBM Spectrum Protect for Enterprise Resource Planning fails to load the message catalog, check that the following completed successfully:

1. Verify that the installation was successful and the language files are contained in *DP for SAP install path*/lang.
2. If the installation path is not the default and you are using a backup interface library like RMAN, then you must set the environment variable **XINT_NLS_CATALOG_PATH** to the new installation path before you run any functions. For IBM Spectrum Protect for Enterprise Resource Planning, this variable is set in the parameter rman_parms in the profile initSID.sap.

Chapter 9. Reference information

Reference information, such as versioning and profile information, is provided.

Version numbers

When IBM Spectrum Protect for ERP backup version control is active, version information is stored on the IBM Spectrum Protect server.

The number of IBM Spectrum Protect for ERP backup versions is defined by the MAX_VERSIONS keyword. The version number is increased only after successful backups.

BRARCHIVE function

BRARCHIVE is an SAP tool for managing data in the Oracle database. It is used to back up offline redo log files. To save each redo log file to IBM Spectrum Protect, BRARCHIVE calls Data Protection for SAP either through the BACKINT interface or through RMAN.

BRARCHIVE maintains a list of redo logs to be saved. Redo logs that were successfully saved by Data Protection for SAP might be deleted from the file system immediately by BRARCHIVE. However,

BRARCHIVE deletes redo log files only in the order of the list. If the requested number of backup copies cannot be saved for a redo log, this redo log and all subsequent redo logs are maintained. When BRARCHIVE starts again, these redo logs are saved again even if some are successfully saved earlier.

Data Protection for SAP informs BRARCHIVE about the redo logs that were saved successfully to IBM Spectrum Protect. If a problem occurs, Data Protection for SAP makes several attempts to save the redo log.

When a redo log cannot be saved to the number of copies that are requested, Data Protection for SAP ends with an error. Data Protection for SAP does not try to save redo logs with a higher sequence number because they are saved in a later BRARCHIVE run.

Manage IBM Spectrum Protect sessions

When redo logs are saved directly to a tape pool, the number of IBM Spectrum Protect sessions must not exceed the number of available tape drives.

BRARCHIVE might process redo logs while a database backup is still processing or several BRARCHIVE processes might run simultaneously. These combined sessions might exceed the number of available tape drives. To avoid this situation, save redo logs to disk storage pools and then move them to tape storage.

Crontab example

UNIX or Linux cron jobs can be scheduled with the **crontab** command. This command starts an editing session that creates a crontab file. The cron jobs and the appropriate times are defined within the crontab file.

The file can be customized with this command:

```
crontab -e
```

In this example, a cron job starts the shell script `backup.ksh` at 11:30 p.m. Monday through Friday and uses the SAP database utility BRBACKUP to back up the SAP database. This example shows the entry in the crontab file that starts the script for this scenario:

```
30 23 * * 1,2,3,4,5 /usr/bin/su - ora<SID> -c "/oracle/SID/sapscripts/backup.ksh"
```

© Copyright IBM Corp. 1995, 2020

Crontab file sample

The following sample output, shows the root crontab jobs.

```
# ------------------------------------------------------------------------
# crontab.sample:
# Sample crontab file to be included in the root crontab jobs.
# ------------------------------------------------------------------------
# Task:
# Submits backup/archive commands at regularly scheduled intervals
# using two simple shell scripts containing SAP backup/archive commands.
# ------------------------------------------------------------------------
#      *****     NOTE     *****     NOTE     *****     NOTE     *****
#
#          This file is intended only as a model and should be
#          carefully tailored to the needs of the specific site.
#
#      *****     NOTE     *****     NOTE     *****     NOTE     *****
# ------------------------------------------------------------------------
#
# Remarks on the crontab file format:
#
# Each crontab file entry consists of a line with six fields, separated
# by spaces and tabs, that contain, respectively:
#   o The minute (0 through 59)
#   o The hour (0 through 23)
#   o The day of the month (1 through 31)
#   o The month of the year (1 through 12)
#   o The day of the week (0 through 6 for Sunday through Saturday)
#   o The shell command
# Each of these fields can contain the following:
#   o A number in the specified range
#   o Two numbers separated by a dash to indicate an inclusive range
#   o A list of numbers separated by commas
#   o An * (asterisk); meaning all allowed values
#
# ------------------------------------------------------------------------
#
# For the following examples, the system id of the ORACLE database
# is assumed to be 'C11' and the username 'oraC11'.
#
# ------------------------------------------------------------------------
# Full database backup, scheduled every Friday at 8:00 p.m.
#
0  20    * * 5
# /usr/bin/su - oraC11 -c "/oracle/C11/sapscripts/backup/backup.ksh"
#
# ------------------------------------------------------------------------
# Save redo logs, scheduled twice a day at 11:30 a.m. and at 5:30 p.m.
# Monday through Friday
#
30 11,17 * * 1,2,3,4,5
/usr/bin/su - oraC11 -c "/oracle/C11/sapscripts/backup/archive.ksh"
```

Data Protection for SAP profile

The Data Protection for SAP profile provides keyword parameters that customize how Data Protection for SAP operates. A sample profile `initSID.utl` is provided on the product media.

During installation on Windows systems, the sample profile (along with all other files) is placed in the `C:\Program Files\Tivoli\TDP4SAP` directory.

During installation on UNIX or Linux systems, this file is copied and renamed to `$ORACLE_HOME/dbs/init$ORACLE_SID.utl`, where *$ORACLE_HOME* is the Oracle home directory and *$ORACLE_SID* is the Oracle System ID (for example, `/oracle/`*SID*`/dbs/init`*SID*`.utl`).

These rules apply to the keyword syntax:

- Each line is analyzed separately.
- Keywords can start in any column of the line.
- Keywords must not be preceded by any string, except blanks.
- If a keyword is encountered several times, the last one is used.

- File processing ends when the END keyword is encountered or the end of file is reached.
- The comment symbol is the number sign (#). Scanning of the current line stops when the comment symbol is encountered. No comment is allowed between the keyword and the value or values. For example:

```
#BRARCHIVEMGTCLASS   MLOG1                    <--  correct
BRARCHIVEMGTCLASS    MLOG1  #                 <--  correct
BRARCHIVEMGTCLASS  # MLOG1                    <--  incorrect
```

- Although some keywords are required, most are optional. Each of the optional keywords has a preset default value.
- The `backint` program on Windows systems accepts the value of the profile name (**-p** option) in Universal Naming Convention (UNC) format as shown here: `\\SERVER_A\profiles\init`*`SID`*`.utl`. However, any file specifications within the profile must use the `drive:path` syntax.

Profile parameter descriptions

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

ADSMNODE ***ORACLE_sid***

Specifies an *ORACLE_sid* that is registered to the IBM Spectrum Protect server as an IBM Spectrum Protect node. This parameter must be defined 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 is used if you have several SAP database systems in your network with the same name, for example, *SID*, and they all use the same IBM Spectrum Protect server. This keyword must not be set when automated password handling is selected. It is to be set for manual password-handling.

ASNODE

Specifies a node name that is registered to the IBM Spectrum Protect server as an IBM Spectrum Protect node. This parameter must be defined with the respective SERVER statement, as shown in the sample profile. When automated password handling is selected and the node is accessed from multiple different SAP systems, for example, HANA scale-out or IBM Spectrum Protect Snapshot offload operations, this parameter avoids storing the encrypted password on multiple hosts (which would cause the password update to fail on all but the first host). This parameter must not be set when manual password handling is selected.

BACKEND ***pgmname [parameterlist]***

Specifies a program *pgmname* that is called by IBM Spectrum Protect for ERP after the backup function completes and before program control is returned to the SAP backup utility. If *pgmname* is not fully qualified, the default search path is used to find the program. If not specified, no backend processing is done.

Example for UNIX or Linux:

```
BACKEND write operator@remotesite Backup of SAP database object completed.
```

This process sends a message to a remote user when the backup finishes.

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___.

BATCH YES|NO

Specify NO if IBM Spectrum Protect for ERP is running with an operator standing by. Specify YES if IBM Spectrum Protect for ERP is running in unattended mode. In unattended mode, IBM Spectrum Protect for ERP stops the run if operator intervention is required. The default for the **BATCH** parameter is YES for the backup-run and NO for the restore-run if the **BATCH** parameter is not present or is commented out in the IBM Spectrum Protect for ERP profile. This parameter has no effect if an RMAN backup or restore is started.

BRARCHIVEMGTCLASS ***management_class [management_class...]***

Specifies the IBM Spectrum Protect management classes that IBM Spectrum Protect for ERP uses when called from BRARCHIVE. Each parameter string can consist of up to 30 characters. Specify a

separate **BRARCHIVEMGTCLASS** for each log file copy requested. As a result, make sure the number of different BRARCHIVE management classes that are specified must be greater than or equal to the number of redo log copies . This parameter must be defined with the respective SERVER statement, as shown in the sample profile.

To use different IBM Spectrum Protect 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 IBM Spectrum Protect management classes that IBM Spectrum Protect for ERP uses when called through BRBACKUP The parameter string can consist of up to 30 characters. This parameter must be defined with the respective SERVER statement, as shown in the sample profile.

BUFFCOPY **SIMPLE|PREVENT|AUTO**
This optional parameter controls how IBM Spectrum Protect for ERP uses the internal buffers for transferring data during a backup. If set to SIMPLE, data buffers are copied when they are sent between IBM Spectrum Protect components. This option is the default. If set to PREVENT, the original data buffers are sent between IBM Spectrum Protect components.

For this mode, **BUFFSIZE** is restricted to a maximum of 896 KB. Furthermore, it cannot be selected when the IBM Spectrum Protect client encryption or client compression features are activated. If set to AUTO, IBM Spectrum Protect for ERP runs 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 that are used for disk I/O. The size of the buffers that are sent to the IBM Spectrum Protect API is the value of **BUFFSIZE** increased by approximately 20 bytes. The valid range is 4096 (4 KB) - 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 that are acquired by IBM Spectrum Protect for ERP correlates to the number of files that are multiplexed in a DataStream (keyword **MULTIPLEXING**) multiplied by the number of sessions (keyword **SESSIONS**). By activating **RL_COMPRESSION**, the number of buffers is doubled.

COMPR_INFO ***path***
Specifies the file where IBM Spectrum Protect for ERP stores information about the compressed size of files. The *path* value specifies the full path and name of the file. When multiplexing is used, IBM Spectrum Protect for ERP attempts to optimize performance by putting files of the same size in one multiplexing stream. If **RL_COMPRESSION** is used in addition to multiplexing, the file sizes of the compressed files can differ very much from the original file sizes. IBM Spectrum Protect for ERP can collect information about the compressed file sizes and use it for further sorting of files. This file size information is stored in the file that is specified by the **COMPR_INFO** parameter. If backups serve as a basis for simulations, **COMPR_INFO** must denote a valid file and **RL_COMPRESSION** must be set to YES to get meaningful simulation results for compression. When the parameter **RL_COMPRESSION** is set to NO, this parameter has no effect. If specified, the information file is written after each backup and the information is used by the following backups and simulations. If there is no compression information about a file because of a database extension, the decompressed file size is used for sorting files.

CONFIG_FILE ***path/initSID.bki***
Specifies the configuration file `init`*`SID`*`.bki` for IBM Spectrum Protect for ERP to store all variable parameters such as passwords and the date of the last password change. This parameter is required.

END
Specifies the end of the parameter definitions. IBM Spectrum Protect for ERP stops searching the file for keywords when **END** is encountered.

EXITONERROR YES|NO|*n*
This keyword specifies whether IBM Spectrum Protect for ERP exits on a backup or restore error during a BRBACKUP/BRRESTORE run. NO means do not exit if an error occurs. YES means exit if one file cannot be backed up. If a number is specified as an argument, IBM Spectrum Protect for ERP counts the number of errors (not warnings or attempts) and exits after the specified number of errors.

This keyword works only for the BRBACKUP/BRRESTORE runs. BRARCHIVE and RMAN activity always exit after the first error. This parameter is ignored if the **BATCH** parameter is set to NO.

FILE_RETRIES *n*|3
This parameter specifies the number of retries when a file cannot be saved or restored. This parameter has no effect if an RMAN backup/restore is started.

FRONTEND *pgmname [parameterlist]*
Specifies a program *pgmname* that is called by IBM Spectrum Protect for ERP in a backup run before the connection to the IBM Spectrum Protect server is established. If *pgmname* is not a fully qualified path, the default search path is used to find the program. If not specified, front-end processing is not done.

Example for UNIX or Linux:

```
FRONTEND write operator@remotesite Backup of SAP database
object is starting.
```

This process sends a message to a remote user before backup begins.

INCREMENTAL NO/CUMULATIVE/DIFFERENTIAL
This parameter specifies whether a backup is run by Oracle RMAN. If it is set to CUMULATIVE or DIFFERENTIAL, incremental backups are done by using Oracle RMAN. The default value is NO. All the other INCREMENTAL* parameters have no effect if **INCREMENTAL** is set to NO.

Note: This parameter can be used only when IBM Spectrum Protect Snapshot is used to offload backups of an SAP Oracle database from the production system and the backups on the backup server are run by Oracle RMAN.

INCREMENTAL_CATALOG_CONNECT_STRING *string*
This parameter specifies the name of the catalog that is passed to RMAN to connect to the catalog database. This catalog is the name of the listener for the catalog database. There is no default value. If **INCREMENTAL** is enabled and this value is missing, an error message is displayed.

INCREMENTAL_CATALOG_USER *string*
This parameter specifies the name of the user that is passed to RMAN to connect to the catalog database. There is no default value. If **INCREMENTAL** is enabled and this value is missing, an error message is displayed.

INCREMENTAL_CHANNELS *integer in the range 1 or higher*
Specifies the number of parallel RMAN channels that can transfer the data. The default is 1.

INCREMENTAL_LEVEL *integer 0 or 1 [USE_AT days of week][From time TO time*
The RMAN incremental level. The default for the incremental level is 0. You can optionally limit the specified incremental level to a specific time or day. If you specify a time or day, multiple occurrences of this parameter are valid while the time specification does not overlap. Time must be specified in 24 hour format. Days can be specified by weekday abbreviations like "Mon, Tue, ..." or by numerical values 0, 1, ..., 6 where 0 stands for Sunday and 6 for Saturday.

LOG_SERVER *servername [verbosity]*
The *servername* value specifies the name of the IBM Spectrum Protect server to which log messages are sent. The *servername* must match one of the servers that are listed in a SERVER statement in order for IBM Spectrum Protect for ERP messages to be logged in the IBM Spectrum Protect 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 IBM Spectrum Protect servers.

MAX_SESSIONS *n* **|** **1**

Specifies the maximum number of parallel IBM Spectrum Protect client sessions that IBM Spectrum Protect for ERP establishes for backup, archive (redo logs) and restore. Each session transfers one database object or, in the case of an RMAN backup or restore, a set of data blocks to or from the IBM Spectrum Protect server by using the IBM Spectrum Protect API client functions. This keyword is required. IBM Spectrum Protect for ERP optimizes the data transfer with attention to the physical location of the Oracle objects. Files that are stored on different volumes are backed up in parallel if multiple sessions are configured. A maximum of 32 parallel sessions can be configured. For a direct backup or restore on tape drives, the number of sessions must be less than or equal to the number of tape drives available for the backup. Make sure that the **MOUNTLIMIT (mountl)** parameter in the device class is set to the number of available tape drives. Make sure that the **MAXNUMMP** parameter of the node is set to the number of available tape drives. The value of keyword **MAX_SESSIONS** must be less than or equal to the sum of the SESSIONS values specified in the **SERVER** statements of the currently available servers.

MAX_ARCH_SESSIONS, MAX_BACK_SESSIONS, MAX_RESTORE_SESSIONS, MAX_CONTROL_SESSIONS

These parameters provide the same function as the **MAX_SESSIONS** parameter but they also provide a more specific use:

- **MAX_ARCH_SESSIONS** defines the number of parallel sessions that are used for archive (backup of log files). Usually archive does not need as many sessions as (data file) backups since the volume is much smaller with log files. This value overrides the value of **MAX_SESSIONS** for the backup of database files.
- **MAX_BACK_SESSION** defines the number of parallel sessions that are used for (data file) backup. This value overwrites the value of **MAX_SESSIONS** for the backup of database files.
- **MAX_CONTROL_SESSION** defines the number of parallel sessions that are used for backing up the control files after a database or redo log backup. If **MAX_CONTROL_SESSION** is not specified, the number of sessions that are used for the control file backup is the same as for the corresponding database or redo log backup. Typically, for a control file backup, the number of sessions can be reduced to avoid unnecessary tape mounts. This value overwrites the value of **MAX_ARCH_SESSIONS** or **MAX_BACK_SESSION** for the backup of control files.
- **MAX_RESTORE_SESSION** defines the number of parallel sessions that are used for restore. For restore, more tape drives might be available than for backup. Using more tape drives might speed up the data transfer for restore if the backup was written to a sufficiently large number of tapes. This value overwrites the value of **MAX_SESSIONS** for restore.

If **MAX_SESSIONS** is specified with one or more of these parameters, these specific parameters override the **MAX_SESSIONS** parameter. You must specify them all if you do not specify the **MAX_SESSIONS** parameter. For the valid range and the rules, see keyword **MAX_SESSIONS**.

MAX_VERSIONS *n* **|** **0**

The *n* value defines the maximum number of full database backup versions to be kept in backup storage. The default setting for this value is 0, meaning that backup version control is disabled. If the number of versions that are found in backup storage is larger than the specified maximum number of backup versions (as specified by the parameter **MAX_VERSIONS**), the oldest versions are deleted (together with the corresponding table space and redo log files) until only the specified maximum number of most recent versions remain. Also, consider these characteristics:

- When IBM Spectrum Protect for ERP deletes an old full backup, all partial backups older than this full backup are also deleted.
- If the backups are distributed over multiple IBM Spectrum Protect servers and one of the servers is temporarily unavailable at the time of a new full backup, it is not possible to find all the backup versions. This situation might result in retaining a backup that would otherwise be deleted.

IBM Spectrum Protect uses the value of the **RETVER** parameter (specified when a copy group is defined) to give files an expiration date. Use only one of these methods to control how long you keep backups:

- If you use IBM Spectrum Protect for ERP backup version control, you must bypass this expiration function. Set the IBM Spectrum Protect parameter RETVER=9999 so that the files are not considered expired and are not deleted by IBM Spectrum Protect.
- If you use the IBM Spectrum Protect expiration function, turn off IBM Spectrum Protect for ERP backup version control. Deactivate IBM Spectrum Protect for ERP backup version control by setting MAX_VERSIONS=0.

MULTIPLEXING ***n*** **|** **1**
Specifies the number of files, which are multiplexed into one DataStream. The allowed range is 1 - 8. The optimal value depends on the actual hardware environment. Multiplexing is most effective when fast tape access exists, fast networks are available, database files are compressed, and the CPU load is moderate. Optimal values are in the range 1 - 4. If not specified, the default value of 1 means multiplexing is not used. This parameter has no effect if an RMAN backup or restore operation is started.

PASSWORDREQUIRED NO|YES
Specifies whether IBM Spectrum Protect requires a password to be supplied by the IBM Spectrum Protect client. This situation depends on the IBM Spectrum Protect installation. If not specified, the default is PASSWORDREQUIRED YES, which implements manual password handling. This parameter must be defined with the respective **SERVER** statement, as shown in the sample profile.

REDOLOG_COPIES ***n*** **|** **1**
Specifies the number of copies IBM Spectrum Protect for ERP stores for each processed Oracle redo log. The valid range is 1 - 9. If not specified, IBM Spectrum Protect for ERP stores one copy of the redo logs. 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 that are specified must be greater than or equal to the number of log file copies specified.

REPORT **NO|YES|2**
If set to YES, IBM Spectrum Protect for ERP produces more information such as information about transferred files. If set to 2, IBM Spectrum Protect for ERP generates an extra summary report that contains detailed backup and restore performance statistics. This summary is displayed at the end of the complete operation. The output is sent to stdout, which is typically the console. If not specified, the default is REPORT NO. This keyword has no effect if an RMAN backup or restore operation is started.

RL_COMPRESSION **NO|YES**
If set to YES, IBM Spectrum Protect for ERP runs a null block compression of the data before they are sent over the network. Although RL compression introduces more CPU load, throughput can be improved when the network is the bottleneck. It is not advised to use RL compression together with the IBM Spectrum Protect API compression. If not specified, the default value is NO meaning null block compression is not done. **RL_COMPRESSION** is only run if a full database backup (BRBACKUP) was started. The offline log files (BRARCHIVE) are not compressed.

SERVER ***servername***
This keyword specifies the name of the IBM Spectrum Protect server to which IBM Spectrum Protect for ERP backups are to be stored. This statement begins a server section in the IBM Spectrum Protect for ERP profile. At least one server section is required. Server sections are 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 IBM Spectrum Protect profiles `dsm.sys` (UNIX, Linux) or `servername.opt` (for Windows). 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 profiles specify the same TCP/IP address for these server names. 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 profiles specify different TCP/IP addresses for the different servers. Do NOT use any profile keywords, ADSM, or TSM as the server name.

SESSIONS ***n*|1**
The *n* value specifies the number of parallel sessions IBM Spectrum Protect for ERP uses for the server. This keyword is required in every server section. This parameter must be defined with the respective **SERVER** statement, as shown in the sample profile.

SORT_FILE
To do a manual sort, a file must be created (*sortfile*). This example of `sortfile` contents is given:

```
/path/filename1 disknumber
/path/filename2 disknumber
     .
      .
       .
/path/filenameN disknumber
```

The disk numbers are counted 1 - n. They do not have any relation to the physical disks. You must specify only the same number for the files on the same physical disk.

TCP_ADDRESS
Specifies the IP address of the IBM Spectrum Protect server in dotted decimal notation. This parameter overrides the value for the parameter **TCPSERVERADDRESS** in the IBM Spectrum Protect client system options file (`dsm.sys`) on UNIX or Linux or in the client options file (*servername*`.opt`) on Windows. The parameter **TCP_ADDRESS** must be defined 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 that are separated by spaces. A trace is written only if both **TRACE** and **TRACEFILE** are specified. Do not use this parameter unless instructed to use it by IBM Spectrum Protect for ERP support. Using it can significantly deteriorate the performance of IBM Spectrum Protect for ERP.

TRACEFILE ***path***
Specifies the name and location of the trace file for IBM Spectrum Protect for ERP 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 used. For example, specifying `/tmp/%BID.trace` yields a trace file `/tmp/myBackup.trace` for backup ID myBackup. A trace is written only if both **TRACE** and **TRACEFILE** are specified.

TRACEMAX ***n***
Specifies the maximum size of the trace file in KB. The valid range is 4096 (4 MB) - unlimited. If not specified, the trace file size is unlimited.

USE_AT ***days***
Specifies the days that the IBM Spectrum Protect server (specified with the corresponding **SERVER** keyword) is used. The *days* value can be numbers in the range 0 (Sunday) - 6 (Saturday). Multiple numbers can be used when separated by spaces. If not specified, the default is to use the IBM Spectrum Protect server on all days. Make sure that the same IBM Spectrum Protect server is used for

a simulation and its corresponding basis production backup. The parameter **USE_AT** must be defined with the respective **SERVER** statement as shown in the sample profile. The parameter has no effect on actions other than on a backup.

Sample profile file for UNIX or Linux

A sample profile file (`initSID.utl`) is included in the IBM Spectrum Protect for ERP installation package.

```
#----------------------------------------------------------------------
#
# Data Protection for SAP (R) interface for ORACLE
#
# Sample profile for Data Protection for SAP (R) Version 7.1
# for UNIX
#
#----------------------------------------------------------------------
#
# This file should be renamed to $ORACLE_HOME/dbs/init$ORACLE_SID.utl
# where $ORACLE_HOME is the home directory of the Oracle database and
# $ORACLE_SID is the system ID of the Oracle database.
#
# See the 'Data Protection for SAP (R) Installation &
# User's Guide' for a full description.
#
# For a comment symbol the character '#' can be used.
# Everything following this character will be interpreted as comment.
#
# Data Protection for SAP (R) V6.2 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 IBM Spectrum Protect 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 IBM Spectrum
Protect servers to be accessed.
# The valid range of MAX_SESSIONS is from 1 and 32.
# Default: none.
#----------------------------------------------------------------------
MAX_SESSIONS        1 # IBM Spectrum
Protect client sessions


#----------------------------------------------------------------------
# Number of parallel sessions to be established for the database backup.
# Note: This number must not exceed the number of tape drives simultaneously
# available to the node for a database backup on the IBM Spectrum
Protect
# servers to be accessed.
# The valid range of MAX_BACK_SESSIONS is from 1 to 32.
# Default: MAX_SESSIONS.
#----------------------------------------------------------------------
#MAX_BACK_SESSIONS    1 # IBM Spectrum
Protect client sessions for backup


#----------------------------------------------------------------------
# Number of parallel sessions to be established for the redo log backup.
# Note: This number must not exceed the number of tape drives simultaneously
# available to the node for a redo log backup on the IBM Spectrum
Protect
# servers to be accessed.
# The valid range of MAX_ARCH_SESSIONS is from 1 to 32.
# Default: MAX_SESSIONS.
#----------------------------------------------------------------------
#MAX_ARCH_SESSIONS    1 # IBM Spectrum Protect client sessions for archive
```

```
#------------------------------------------------------------------------
# Number of parallel sessions to be established for the backup of control
# files. This number is typically used to reduce the number of sessions
# to be used for the control file backup after another backup operation.
# The valid range of MAX_CONTROL_SESSIONS is from 1 to 32.
# Default: MAX_BACK_SESSIONS or MAX_ARCH_SESSIONS, depending on the type of
#          the control file backup.
#------------------------------------------------------------------------
#MAX_CONTROL_SESSIONS    1 # IBM Spectrum
Protect client sessions for control
                          # file backup.


#------------------------------------------------------------------------
# Number of parallel sessions to be established for the restore of files.
# Note: This number must not exceed the number of tape drives simultaneously
# available to the node for restore processing backup on the IBM Spectrum
Protect
# servers to be accessed.
# The valid range of MAX_RESTORE_SESSIONS is from 1 to 32.
# Default: MAX_SESSIONS.
#------------------------------------------------------------------------
#MAX_RESTORE_SESSIONS    1 # IBM Spectrum
Protect client sessions for restore


#------------------------------------------------------------------------
# Number of backup copies of redo logs.
# The valid range of REDOLOG_COPIES is from 1 to 9.
# Default: 1.
#------------------------------------------------------------------------
#REDOLOG_COPIES        2


#------------------------------------------------------------------------
# Specifies whether a null block compression of the data is to be performed
# before transmission to IBM Spectrum
Protect.
# 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
# IBM Spectrum
Protect API compression.
# Default: NO
#------------------------------------------------------------------------
#RL_COMPRESSION        YES


#------------------------------------------------------------------------
# Specifies how many files are read simultaneously and are multiplexed into
# one data stream to an IBM Spectrum
Protect server. Multiplexing is usefull
# when the data rate to an IBM Spectrum
Protect server is higher (fast
# tapes, fast network) than the I/O rate of a single disk.
# The valid range of MULTIPLEXING is from 1 to 8.
# Default: 1 (meaning no multiplexing)
#------------------------------------------------------------------------
#MULTIPLEXING        2


#------------------------------------------------------------------------
# Specifies the block size for disk I/O (in bytes).
# The default values have been chosen from our performance experiments in
# standard hardware environments.
# The valid range of BUFFSIZE is from 4KB to 32MB.
# Default: 131072 (128 KB) on UNIX, 32768 (32 KB) on Windows.
#------------------------------------------------------------------------
BUFFSIZE        131072              # block size in bytes


#------------------------------------------------------------------------
# This optional parameter controls how Data Protection for SAP(R) uses
# the internal buffers for transferring data during a backup.
# Valid values:   SIMPLE | PREVENT | AUTO
# Default: SIMPLE
#------------------------------------------------------------------------
#BUFFCOPY               AUTO


#------------------------------------------------------------------------
```

```
# Name of a program to be called before the backup task is started.
# Default: none.
#-------------------------------------------------------------------------
#FRONTEND              pgmname parameterlist


#-------------------------------------------------------------------------
# Name of a program to be called after the backup task is completed.
# Default: none.
#-------------------------------------------------------------------------
#BACKEND               pgmname parameterlist


#-------------------------------------------------------------------------
# Maximum number of data base backup versions to be kept.
# Note: Version control by Data Protection for SAP (R) is only activated
# if the R/3 release is 3.0C and higher and the parameter MAX_VERSIONS is
# not 0.
# The valid range of MAX_VERSIONS is from 0 to 9999.
# A value of 0 means no versioning.
# Default: 0, no versioning.
#-------------------------------------------------------------------------
#MAX_VERSIONS       4


#-------------------------------------------------------------------------
# Indicates whether processing is to be done unattended or whether human
# intervention is allowed.
# Default:
# YES for backup processing
# NO  for restore processing
#-------------------------------------------------------------------------
#BATCH                 YES               # unattended automated operation
#BATCH                 NO                # manual operation


#-------------------------------------------------------------------------
# Control of error situations: Indicates whether and when database backups
# and restore operations should be ended when an error occurs during
# unattended processing.
# Valid values:
# YES: Exit if a single file cannot be backed up or restored.
# NO:  Do not exit when an error occurs.
# the number of errors resulting in exiting the processing.
# The valid range of EXITONERROR is from 0 to 100.
# Default: NO.
#-------------------------------------------------------------------------
#EXITONERROR       3                  # exit after 3 errors


#-------------------------------------------------------------------------
# Control of information for reporting purposes, e.g. messages, statistics.
# Default: NO (no additional data will be reported).
#-------------------------------------------------------------------------
#REPORT            NO                # no additional messages
#REPORT            YES               # all additional messages
#REPORT            2                 # all additional messages + summary


#-------------------------------------------------------------------------
# Controls generation of a trace file.
# Note: we recommend using the trace function only in cooperation with
# Data Protection for SAP (R) support.
# Default: OFF.
#-------------------------------------------------------------------------
#TRACE           OFF


#-------------------------------------------------------------------------
# The full path of the trace file.
# Note: for an actual trace the string '%BID' will be replaced by
# the current backupid.
# (.../backint_%BID.trace changes to .../backint_SAP___9809182300.trace).
# Default: none.
#-------------------------------------------------------------------------
#TRACEFILE       /oracle/C21/dbs/backint.trace
#TRACEFILE       /oracle/C21/dbs/backint_%BID.trace


#-------------------------------------------------------------------------
# Denotes the maximum size of the trace file in KB.
# If not specified, the trace file size is unlimited.
```

```
#------------------------------------------------------------------------
#TRACEMAX           max size            # trace file size in KB

#------------------------------------------------------------------------
# Specify the full path of the configuration file.
# Default: none.
#------------------------------------------------------------------------
CONFIG_FILE        /oracle/C21/dbs/initSID.bki


#------------------------------------------------------------------------
# Number of times to retry saving/restoring a file in case an error occurs.
# The valid range of FILE_RETRIES is from 0 to 100.
# Default: 3.
#------------------------------------------------------------------------
#FILE_RETRIES        3


#------------------------------------------------------------------------
# Denotes if Data Protection for SAP (R) shall send error/status
# information to an IBM Spectrum
Protect server.
# The servername must match one of the servers listed in a SERVER statement.
# Valid values for verbosity are ERROR | WARNING | DETAIL.
# Default: none.
#------------------------------------------------------------------------
#LOG_SERVER             servername    [verbosity]
#LOG_SERVER             server_a      ERROR


#------------------------------------------------------------------------
# Denotes if Data Protection for SAP (R) shall use a manual sorting file
# for disk sorting.
# Default: none.
#------------------------------------------------------------------------
#SORT_FILE        /oracle/C21/dbs/manual_sort_file


#------------------------------------------------------------------------
# Denotes if Data Protection for SAP (R) shall use a compressed filesize
# sorting file for disk sorting.
# For backup simulations with compression (see manual) this parameter must
# be set to a valid file.
# Default: none.
#------------------------------------------------------------------------
#COMPR_INFO        /oracle/C21/dbs/initSID.cfi


#------------------------------------------------------------------------
# If IBM Spectrum Protect
Snapshot is used to offload backups to
# another host and Oracle RMAN should be utilized for these backups
# then the following parameters need to be activated. This is not
# required for Oracle RMAN backups on the production system
#------------------------------------------------------------------------
# Type of RMAN backup to perform (CUMULATIVE, DIFFERENTIAL, NO).
# Default: NO (disables the function)
#------------------------------------------------------------------------
#INCREMENTAL CUMULATIVE
#------------------------------------------------------------------------
# Number of RMAN channels to establish.
# Default: 1
#------------------------------------------------------------------------
#INCREMENTAL_CHANNELS 2
#------------------------------------------------------------------------
# Incremental level for the backup (0 or 1).
# Default: 0
# Optional time specifications can be defined with the USE_AT clause.
#------------------------------------------------------------------------
#INCREMENTAL_LEVEL 1 USE_AT MON TUE WED Thu Fri Sat
#INCREMENTAL_LEVEL 1 USE_AT SUN FROM 00:00 TO 06:00
#INCREMENTAL_LEVEL 0 USE_AT SUN FROM 06:01 TO 23:59
#------------------------------------------------------------------------
# Name of the recovery catalog database.
#------------------------------------------------------------------------
#INCREMENTAL_CATALOG_CONNECT_STRING catdb
#------------------------------------------------------------------------
# Name of the user that is used to connect against the recovery catalog database.
#------------------------------------------------------------------------
#INCREMENTAL_CATALOG_USER rman
#************************************************************************
# 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              # IBM Spectrum
Protect 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              # IBM Spectrum
Protect 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 profile (Windows)

The sample profile file (initSID.utl) is included in the installation package.

```
#------------------------------------------------------------------------------
#
# Data Protection for SAP (R) interface for ORACLE
#
# Sample profile for Data Protection for SAP (R)
# Version x.x for Windows
#
#------------------------------------------------------------------------------
#
# 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
# IBM Spectrum
Protect 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 IBM Spectrum
Protect servers to be accessed.
# The valid range of MAX_SESSIONS is from 1 and 32.
# Default: none.
#-----------------------------------------------------------------------
MAX_SESSIONS        1 # IBM Spectrum
Protect client sessions


#-----------------------------------------------------------------------
# Number of parallel sessions to be established for the database backup.
# Note: This number must not exceed the number of tape drives simultaneously
# available to the node for a database backup on the IBM Spectrum
Protect
# servers to be accessed.
# The valid range of MAX_BACK_SESSIONS is from 1 to 32.
# Default: MAX_SESSIONS.
#-----------------------------------------------------------------------
#MAX_BACK_SESSIONS    1 # IBM Spectrum
Protect client sessions for backup


#-----------------------------------------------------------------------
# Number of parallel sessions to be established for the redo log backup.
# Note: This number must not exceed the number of tape drives simultaneously
# available to the node for a redo log backup on the IBM Spectrum
Protect
# servers to be accessed.
# The valid range of MAX_ARCH_SESSIONS is from 1 to 32.
# Default: MAX_SESSIONS.
#-----------------------------------------------------------------------
#MAX_ARCH_SESSIONS    1 # IBM Spectrum
Protect client sessions for archive


#-----------------------------------------------------------------------
# Number of parallel sessions to be established for the backup of control
# files. This number is typically used to reduce the number of sessions
# to be used for the control file backup after another backup operation.
# The valid range of MAX_CONTROL_SESSIONS is from 1 to 32.
# Default: MAX_BACK_SESSIONS or MAX_ARCH_SESSIONS, depending on the type of
#          the control file backup.
#-----------------------------------------------------------------------
#MAX_CONTROL_SESSIONS    1 # IBM Spectrum
Protect client sessions for control
                          # file backup.

#-----------------------------------------------------------------------
# Number of parallel sessions to be established for the restore of files.
# Note: This number must not exceed the number of tape drives simultaneously
# available to the node for restore processing backup on the  IBM Spectrum Protect
# servers to be accessed.
# The valid range of MAX_RESTORE_SESSIONS is from 1 to 32.
# Default: MAX_SESSIONS.
#-----------------------------------------------------------------------
#MAX_RESTORE_SESSIONS    1 # IBM Spectrum
Protect client sessions for restore


#-----------------------------------------------------------------------
# Number of backup copies of redo logs.
# The valid range of REDOLOG_COPIES is from 1 to 9.
# Default: 1.
#-----------------------------------------------------------------------
#REDOLOG_COPIES        2


#-----------------------------------------------------------------------
# Specifies whether a null block compression of the data is to be performed
# before transmission to IBM Spectrum
Protect.
# 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
# IBM Spectrum
Protect API compression.
```

```
# Default: NO
#------------------------------------------------------------------------
#RL_COMPRESSION        YES


#------------------------------------------------------------------------
# Specifies how many files are read simultaneously and are multiplexed into
# one data stream to an IBM Spectrum
Protect server. Multiplexing is usefull
# when the data rate to an IBM Spectrum
Protect server is higher (fast
# tapes, fast network) than the I/O rate of a single disk.
# The valid range of MULTIPLEXING is from 1 to 8.
# Default: 1 (meaning no multiplexing)
#------------------------------------------------------------------------
#MULTIPLEXING        2


#------------------------------------------------------------------------
# Specifies the block size for disk I/O (in bytes).
# The default values have been chosen from our performance experiments in
# standard hardware environments.
# The valid range of BUFFSIZE is from 4KB to 32MB.
# Default: 131072 (128 KB) on UNIX, 32768 (32 KB) on Windows.
#------------------------------------------------------------------------
BUFFSIZE        32768             # block size in bytes


#------------------------------------------------------------------------
# This optional parameter controls how Data Protection for SAP(R) uses
# the internal buffers for transferring data during a backup.
# Valid values:   SIMPLE | PREVENT | AUTO
# Default: SIMPLE
#------------------------------------------------------------------------
#BUFFCOPY               AUTO


#------------------------------------------------------------------------
# Name of a program to be called before the backup task is started.
# Default: none.
#------------------------------------------------------------------------
#FRONTEND               pgmname parameterlist


#------------------------------------------------------------------------
# Name of a program to be called after the backup task is completed.
# Default: none.
#------------------------------------------------------------------------
#BACKEND                pgmname parameterlist


#------------------------------------------------------------------------
# Maximum number of data base backup versions to be kept.
# Note: Version control by Data Protection for SAP (R) is only activated
# if the SAP R/3 release is 3.0C and higher and the parameter
# not 0.
# The valid range of MAX_VERSIONS is from 0 to 9999.
# A value of 0 means no versioning.
# Default: 0, no versioning.
#------------------------------------------------------------------------
#MAX_VERSIONS        4


#------------------------------------------------------------------------
# Indicates whether processing is to be done unattended or whether human
# intervention is allowed.
# Default:
# YES for backup processing
# NO  for restore processing
#------------------------------------------------------------------------
#BATCH                  YES                # unattended automated operation
#BATCH                  NO                 # manual operation


#------------------------------------------------------------------------
# Control of error situations: Indicates whether and when database backups
# and restore operations should be ended when an error occurs during
# unattended processing.
# Valid values:
# YES: Exit if a single file cannot be backed up or restored.
# NO:  Do not exit when an error occurs.
# the number of errors resulting in exiting the processing.
```

```
# The valid range of EXITONERROR is from 0 to 100.
# Default: NO.
#-------------------------------------------------------------------------
#EXITONERROR        3                  # exit after 3 errors


#-------------------------------------------------------------------------
# Control of information for reporting purposes, e.g. messages, statistics.
# Default: NO (no additional data will be reported).
#-------------------------------------------------------------------------
#REPORT             NO                 # no additional messages
#REPORT             YES                # all additional messages
#REPORT             2                  # all additional messages + summary


#-------------------------------------------------------------------------
# Controls generation of a trace file.
# Note: we recommend using the trace function only in cooperation with
# Data Protection for SAP (R) support.
# Default: OFF.
#-------------------------------------------------------------------------
#TRACE             OFF


#-------------------------------------------------------------------------
# The full path of the trace file.
# Note: for an actual trace the string '%BID' will be replaced by
# the current backupid.
# (...\backint_%BID.trace changes to ...\backint_SAP___9809182300.trace).
# Default: none.
#-------------------------------------------------------------------------
#TRACEFILE         x:\oracle\C21\database\backint.trace
#TRACEFILE         x:\oracle\C21\database\backint_%BID.trace


#-------------------------------------------------------------------------
# Denotes the maximum size of the trace file in KB.
# If not specified, the trace file size is unlimited.
#-------------------------------------------------------------------------
#TRACEMAX           max. size             # trace file size in KB

#-------------------------------------------------------------------------
# Specify the full path of the configuration file.
# Default: none.
#-------------------------------------------------------------------------
CONFIG_FILE         x:\oracle\C21\database\initSID.bki


#-------------------------------------------------------------------------
# Number of times to retry saving/restoring a file in case an error occurs.
# The valid range of FILE_RETRIES is from 0 to 100.
# Default: 3.
#-------------------------------------------------------------------------
#FILE_RETRIES        3


#-------------------------------------------------------------------------
# Denotes if Data Protection for SAP (R) shall send error/status
# information to an IBM Spectrum
Protect server.
# The servername must match one of the servers listed in a SERVER statement.
# Valid values for verbosity are ERROR | WARNING | DETAIL.
# Default: none.
#-------------------------------------------------------------------------
#LOG_SERVER             servername    [verbosity]
#LOG_SERVER             server_a      ERROR


#-------------------------------------------------------------------------
# Denotes if Data Protection for SAP (R) shall use a manual sorting file
# for disk sorting.
# Default: none.
#-------------------------------------------------------------------------
#SORT_FILE         x:\oracle\C21\database\manual_sort_file


#-------------------------------------------------------------------------
# Denotes if Data Protection for SAP (R) shall use a compressed filesize
# sorting file for disk sorting.
# For backup simulations with compression (see manual) this parameter must
# be set to a valid file.
# Default: none.
```

```
#------------------------------------------------------------------------
#COMPR_INFO        x:\oracle\C21\database\initSID.cfi


#*****************************************************************************
# Statement for servers and paths.
# Multiple servers may be defined.
#*****************************************************************************


SERVER         server_a                 # Servername, as defined in dsm.sys
  SESSIONS            2                 # Maximum number of sessions
                                        # to server_a
  PASSWORDREQUIRED    YES               # Use a password
  ADSMNODE            NODE              # IBM Spectrum
Protect 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              # IBM Spectrum
Protect 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
```

Locating sample files

Use the file samples to assist you with Data Protection for SAP operations.

Procedure

- Review the out put samples for `dsm.opt`, the include/exclude statement, and `dsm.sys`.
- Use the planning sheet to help you plan the installation parameters for Data Protection for SAP.

Save and delete redo logs, batch file sample

```
@echo off
rem ------------------------------------------------------------------------
rem file name: archive.cmd
rem ------------------------------------------------------------------------
rem Sample BRArchive batch file
rem ------------------------------------------------------------------------
rem Task:
rem Invokes the SAP utility BRArchive in order to save ORACLE's archived
rem redo logs (using Data Protection for SAP (R) ) and deletes the redo
rem logs from their original location. After completing this, the BRArchive
```

```
rem protocol is saved separately.
rem ------------------------------------------------------------------------
rem ***** NOTE ***** NOTE ***** NOTE *****
rem
rem This script is intended only as a model and should be
rem carefully tailored to the needs of the specific site.
rem
rem ***** NOTE ***** NOTE ***** NOTE *****
rem ------------------------------------------------------------------------
rem
rem Remarks on the parameters of BRArchive:
rem
rem -u system/manager ORACLE username/password
rem -sd save and delete archived redo logs
rem -c run BRArchive in quiet mode
rem (-n number of redo logs to be saved,
rem default is 10000,
rem which means all available)
rem
rem The following should be configured within the SAP profile
rem initC21.sap:
rem
rem backup_dev_type = util_file
rem causes BRBACKUP to use the external program
rem Data Protection for SAP (R)
rem util_par_file = %ORACLE_HOME%\database\initC21.utl
rem Data Protection for SAP (R) profile
rem ------------------------------COMMAND---------------------------------
brarchive -u system/manager -sd -c
```

Save and delete redo logs, shell script sample

```
#!/bin/ksh
# ------------------------------------------------------------------------
# archive.ksh:
# Sample BRARCHIVE shell script
# ------------------------------------------------------------------------
# Task:
# Invokes the SAP utility brarchive in order to save ORACLE's archived
# redo logs (using Data Protection for SAP (R) ) and deletes the redo
# logs from their original location. After completing this, the brarchive
# protocol is saved separately.
# ------------------------------------------------------------------------
#      *****     NOTE     *****     NOTE     *****     NOTE     *****
#
#          This script is intended only as a model and should be
#          carefully tailored to the needs of the specific site.
#
#      *****     NOTE     *****     NOTE     *****     NOTE     *****
# ------------------------------------------------------------------------
#
# Remarks on the parameters:
#
# -u system/manager     Oracle username/password
# -sd                   save and delete archived redo logs
# -c                    run BRARCHIVE in unattended mode
# (-n                   number of redo logs to be saved, default is 10000,
#            which means all available)
#
# The following should be configured within the SAP profile initC11.sap:
#
# backup_dev_type = util_file
#        causes brbackup to use the external program backint
# util_par_file =  initC11.utl
#        Data Protection for SAP profile
#
# -------------------------------COMMAND---------------------------------
brarchive -u system/manager -c -sd
```

Client user options file sample (UNIX, Linux)

```
*********************************************************************
* IBM Spectrum
Protect                                        *
*                                                                   *
* Sample Client User Options file for Unix platforms                *
```

```
*****************************************************************************

SErvername       server_a
Tapeprompt       No
DOM              /usr/sap /sapmnt/C11 /usr/sap/trans /oracle/C11
```

Client user options file sample (Windows)

Data Protection for SAP requires a client options file `dsm.opt` to be present in the location indicated by environment variable **DSMI_CONFIG**. The specific options that are used by Data Protection for SAP for each server are taken from file *server*`.opt` in the same path.

```
*****************************************************************************
*
* DSM.OPT (for Data Protection for SAP)
*
* 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
*            IBM Spectrum
Protect clients.
*
*****************************************************************************
```

Client system options file sample (dsm.sys)

The system options file lists information that includes the **buffersize** and compression status. The following sample shows the typical output.

```
*****************************************************************************
* IBM Spectrum Protect                                              *
*                                                                           *
* 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 and exclude list sample (UNIX, Linux)

The include and exclude list shows the files and directories that are included or excluded for backup operations.

```
* ------------------------------------------------------------------------
* inclexcl.list:
* Sample include/exclude list
* ------------------------------------------------------------------------
* Task:
* Include/Exclude list of files and directories for IBM Spectrum
Protect
* incremental backups
* ------------------------------------------------------------------------
*      *****     NOTE     *****     NOTE     *****     NOTE     *****
*
*          This file is intended only as a model and should be
```

```
*          carefully tailored to the needs of the specific site.
*
*      *****     NOTE     *****     NOTE     *****     NOTE     *****
* ------------------------------------------------------------------------
*
* For all AIX systems
*
exclude /unix
exclude /.../core
exclude /u/.../.*sh_history
exclude /home/.../.*sh_history
*
* Note: It is recommended to perform system backups on a regular
*       basis (e.g. using 'smit mksysb'). Consequently, you can exclude
*       at least the following directories (which make up about 30 MB).
*
exclude /usr/games/.../*
exclude /usr/bin/.../*
exclude /usr/lbin/.../*
exclude /usr/mbin/.../*
exclude /usr/sbin/.../*
* ------------------------------------------------------------------------
*
* For those using AFS, exclude the cache filesystem or file
*
* exclude /usr/vice/cache/*
* exclude /var/vice/cache/*
* or
* exclude /afscfs
* ------------------------------------------------------------------------
*
* This stuff is either not worthwhile to be included or should be backed up
* using SAP's BR*Tools utilities brbackup/brarchive.
*
exclude /oracle/C11/saparch/.../*
* exclude /oracle/C11/sapbackup/.../*
* exclude /oracle/C11/sapreorg/.../* (There may be important scripts
*                                     located, check it out and decide.)
exclude /oracle/C11/sapdata*/.../*
exclude /oracle/C11/sapraw*/.../*
* ------------------------------------------------------------------------
*
* With the above include/exclude list we implicitly include everything not
* excluded above. Especially for DP for SAP (R), this means including:
*      /sapmnt/C11     > 270 MB
*      /usr/sap        > 14 MB
*      /oracle/stage   > 89 MB
*      /oracle/C11     > 90 MB
* and  OS  related     > 220 MB
* ------------------------------------------------------------------------
```

Include/exclude list sample (Windows)

The include/exclude list is intended for the standard client user option file. The purpose is to exclude files that are easy to restore. Also, exclude files that are already saved by Data Protection for SAP from routine IBM Spectrum Protect incremental backups. Typically, such files are Windows system files and database files.

```
************************************************************************
* This Include-Exclude list is used for incremental backups of file
* systems by the IBM Spectrum
Protect command-line backup client.
* Therefore the name of this file has to be set under the keyword InclExcl
* in the standard IBM Spectrum
Protect client user option file "dsm.opt".
*
* Since the backup of the ORACLE database is done by
* Data Protection for SAP (R) and not by IBM Spectrum
Protect
* command-line backup client, the ORACLE database should be excluded
* from backups by the IBM Spectrum
Protect command-line backup client.
*
* Note 1:
* The environment variable DSM_CONFIG contains the full file name of
* the IBM Spectrum
Protect client user option file "dsm.opt".
* Note 2:
```

```
* This Include-Exclude is not used by Data Protection for SAP (R).
*
************************************************************************
Exclude *:\...\*.swp
Exclude *:\...\*.obj
Exclude *:\...\*.csm
Exclude *:\...\*.dsk
Exclude *:\...\*.bak
Exclude *:\...\win386.swp
Exclude *:\...\386spart.par
Exclude *:\...\pagefile.sys
Exclude *:\...\*.par
Exclude *:\...\SYSTEM32\CONFIG\*.*
Exclude *:\...\SYSTEM32\CONFIG\...\*
Exclude *:\IBMBIO.COM
Exclude *:\IBMDOS.COM
*
*Exclude the following ORACLE database files:
*
Exclude *:\oracle\C21\saparch\...\*
Exclude *:\oracle\C21\sapbackup\...\*
Exclude *:\oracle\C21\sapreorg\...\*
Exclude *:\oracle\C21\sapdata*\...\*
```

Client options files sample

Data Protection for SAP requires a corresponding client option file *server*`.opt` for each IBM Spectrum Protect server. These files must be in the same directory. This directory must also contain the client options file `dsm.opt`, which is specified in the environment variable DSMI_CONFIG.

```
************************************************************************
*
* SERVER.OPT
*
* Data Protection for SAP (R) obtains the necessary information about
* an IBM Spectrum
Protect server 'server' from a client option file
* called 'server.opt'. For each IBM Spectrum
Protect server a
* corresponding client option file is required.
*
* Note: This file contains the client options for the IBM Spectrum
Protect
* server called 'server_a'.
*
* Please see the IBM Spectrum
Protect documentation for details.
*
************************************************************************
COMMmethod         TCPIP
COMPression        OFF
*NODEname           C21
TCPPort            1500
TCPServeraddress   xxx.xxx.xxx.xxx
PASSWORDACCESS     PROMPT
TCPBUFFSIZE        31
TCPWINDOWSIZE      32
```

Planning sheet for the base product

Use the planning sheet to assist you when you are installing and configuring Data Protection for SAP.

Collect the information in this planning sheet before you install Data Protection for SAP.

This table is also provided in file form as `planning_sheet_oracle` for UNIX and Linux and `planning_sheet_oracle.txt` for Windows.

Table 7. Installation parameters for Data Protection for SAP		
UNIX or Linux	**Windows**	**Installation parameter**
X	X	Oracle database SID
X	X	IBM Spectrum Protect server name or IP address:
X	X	IBM Spectrum Protect node name: IBM Spectrum Protect node that is configured on the IBM Spectrum Protect server that is named for the backup of the SID previously listed.
X	X	IBM Spectrum Protect management classes for database and redo log backups. Management classes that are configured for the database backup and for the backup of redo logs. Default: MDB for database backups, MLOG1 and MLOG2 for redo log backups.
	X	Path where the IBM Spectrum Protect API are in (contents of environment variable **DSMI_DIR**): Default: `C:\Program Files\Common Files\tivoli\TSM\api64`
	X	Path to client option file of IBM Spectrum Protect (contents of environment variable **DSMI_CONFIG**).
	X	Path to IBM Spectrum Protect log files (contents of environment variable **DSMI_LOG**): The IBM Spectrum Protect API creates the file `dsierror.log` in this path. Default: `C:\temp`
	X	Installation path for Data Protection for SAP executable files: `C:\Program Files\Tivoli\TSM\tdp_r3\ora64`
X	X	Path for Data Protection for SAP configuration files (directory for SAP configuration files): During the installation, the Data Protection for SAP configuration files are saved to this path. If old configuration files are found, they are renamed to *filename*`.nnn`, where nnn is a three-digit decimal number. This path must not contain blanks. Default: `/oracle/`*SID*`/dbs` or `C:\orant\database`

Network settings for IBM Spectrum Protect

When you are using IBM Spectrum Protect with Data Protection for SAP, you can improve performance by making updates to the configuration files. Before you edit configuration files, save a backup copy.

The performance adjustments for IBM Spectrum Protect are completed by editing the following files:

- IBM Spectrum Protect server option file `dsmserv.opt`
- IBM Spectrum Protect backup-archive client option file `dsm.sys` (UNIX and Linux systems), or `server.opt` (Windows systems).

This table shows the corresponding IBM Spectrum Protect configuration file attributes with the values.

Table 8. Tuning IBM Spectrum Protect configuration file attributes		
Attributes	**Value**	**Description**
TCPBuffsize	32	Specifies the size, in KB, of the buffer that is used for TCP/IP send requests. This option affects whether IBM Spectrum Protect sends the data directly from the session buffer or copies the data to the TCP buffer. A buffer size of 32 KB forces IBM Spectrum Protect to copy data to its communication buffer and flush the buffer when it fills.
TCPNODelay	YES	Specifies whether the server is to send small amounts of data or allow TCP/IP to buffer the data. Disallowing buffering might improve throughput but more packets are sent over the network.
TCPWindowsize	640 (AIX) 63 (others)	Specifies the size, in KB, which is used for the TCP/IP sliding window for the client node. This size is used when data is sent or received. The range of values is 0 - 2048.

Networks with large bandwidth delay

For networks with a large bandwidth-delay, activate the TCP enhancements as specified in RFC1323.

For example, the network on an AIX system can be configured with the **no** command. This command sets or displays current network attributes in the kernel. For more information, see the man page.

This table shows the network attributes with their advised values:

Table 9. 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 attempts to negotiate the RFC enhancements.
sb_max	131072	Specifies the maximum buffer size that is allowed for a socket. The default is 65536 bytes. From the point of view of performance recommendations, the sb_max value is to be twice the TCPWindowsize set within the IBM Spectrum Protect configuration file dsm.sys.

Set these values by issuing these commands by the root user on the appropriate system:

```
no -o rfc1323=1
no -o sb_max=131072
```

The **no** command does not do range checking. It accepts all values. If used incorrectly, the command might cause the system to become inoperable. These changes are lost at system restart. To permanently change the values, edit the /etc/rc.net file.

SP switch (RISC 6000)

If an SP switch (RISC 6000) is used, the `rpoolsize` and `spoolsize` values must be set as shown in the following table.

Table 10. 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 by using the **hgcss** command. After the changes are made, restart the node.

Appendix A. Accessibility features for the IBM Spectrum Protect product family

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

Overview

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

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

The IBM Spectrum Protect family of products uses the latest W3C Standard, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), to ensure compliance with US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) and Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by the product.

The product documentation in IBM Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described in the Accessibility section of the IBM Knowledge Center help (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

Keyboard navigation

This product uses standard navigation keys.

Interface information

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

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

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

Vendor software

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

Related accessibility information

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

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

For more information about the commitment that IBM has to accessibility, see IBM Accessibility (www.ibm.com/able).

© Copyright IBM Corp. 1995, 2020

Notices

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

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

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

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

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

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

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

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

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

© Copyright IBM Corp. 1995, 2020

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

Terms and conditions for product documentation

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

Applicability

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

Personal use

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

Commercial use

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

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

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

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

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

Privacy policy considerations

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

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

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

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

Glossary

A glossary is available with terms and definitions for the IBM Spectrum Protect family of products.

See the IBM Spectrum Protect glossary.

© Copyright IBM Corp. 1995, 2020

Index

A

accessibility features 97

B

BACKINT
    interaction with Data Protection for SAP 2

C

client options file 40

D

disability 97

I

IBM Knowledge Center xi

K

keyboard 97
Knowledge Center xi

P

publications xi

S

SID 68

Product Number: 5725-X03