

Reading Sample

Preparing for worst-case scenarios is just part of the job for a system administrator. With this reading sample, discover vital backup and recovery strategies for protecting your SAP system during a failure. Then, learn what to do when disaster does strike, and the steps you need to know to recover from a serious malfunction.



"Backup and Restore"
"Disaster Recovery"



Contents



Index



The Author

Sebastian Schreckenbach

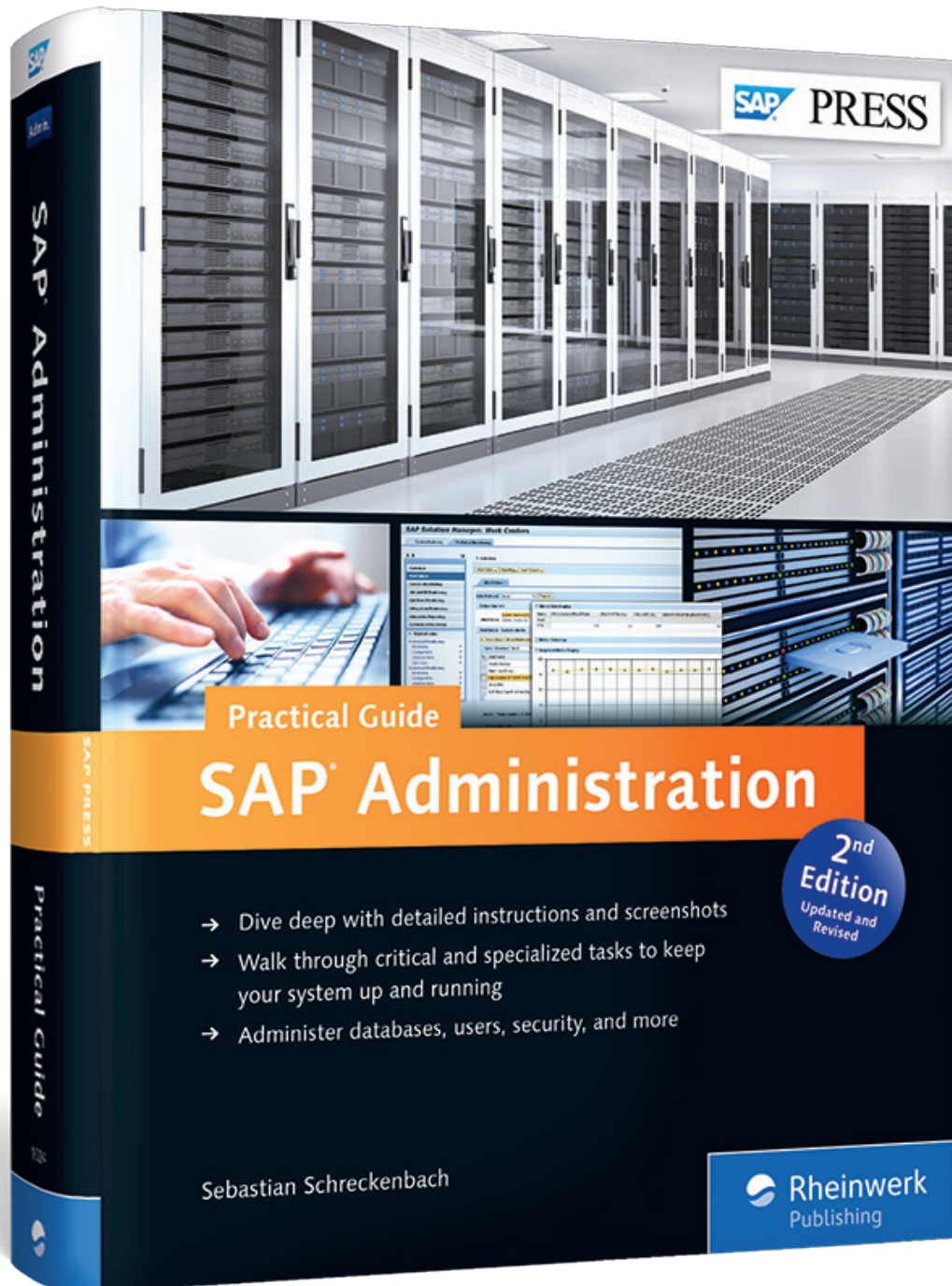
SAP Administration—Practical Guide

912 Pages, 2015, \$79.95/€79.95

ISBN 978-1-4932-1024-4



www.sap-press.com/3639



This chapter explains how to develop a backup and restore strategy. After covering the main backup methods, we'll explore the benefits and drawbacks of each. You can then use this information to develop an appropriate backup concept for your own SAP system.

6 Backup and Restore

An effective backup and restore strategy forms the backbone of SAP system operation. The goal of this strategy is to enable a full or partial recovery of the database in as short a time as possible following system failure, an emergency situation (see Chapter 7), or a hardware/software error.

The information provided in this chapter is intended to help you develop a concept to optimize the continuous backup of your data and allow you to restore your database quickly and efficiently in the event of an emergency. We begin by discussing the two aspects of backup and restore, before turning to the issue of performance. Details relating to individual databases are provided in Chapter 8.

The goal of a backup strategy is to minimize data loss in the event of an emergency, in other words, to make sure that no data are lost or to minimize the period during which data are lost. To achieve this objective, your backup strategy should be as clearly defined as possible because an unnecessarily complicated strategy may also make your backup and restore processes unnecessarily complicated. You should also ensure that your procedures and handling of problems are well documented and that your backup strategy doesn't impact negatively on your enterprise's routine business operations.

6.1 Backup

The purpose of a system backup is to allow you to access the data currently stored in the system and to import that data back into the system following an emergency. This is a safeguarding measure because you'll only need to use the backup

if your system needs to be restored, unless you plan, for example, to build a quality assurance system from a system backup. Nevertheless, backups aren't a trivial matter and shouldn't be treated as such. On the contrary, you should take a moment to consider how much data can be lost in the event of a system failure and what ramifications this may have for the enterprise. Even if you lose order data for only an hour or a day, the economic impact on your business may be huge.

6.1.1 What Has to Be Saved?

Three categories of data require backup:

- ▶ Databases
- ▶ Transaction logs
- ▶ Operating system files

You may need to use different tools to back up different data. For example, SAP tools only allow you to back up one or two of the data categories; for example, the DBA Planning Calendar (Transaction DB13; see also Chapter 8) is capable of backing up your database and transaction logs but not your system files.

Databases

The database represents the very heart of your SAP system. Without a backup of your database, you won't be able to restore the system. The frequency with which you perform a full database backup determines how far back in time you must go when restoring the system:

- ▶ If a full backup is performed every day, you require the full backup from the previous day, as well as the transaction log files from the last day or last half-day to restore the system.
- ▶ If a full backup is performed every week, you require the full backup from the previous week. However, you must also recover the log files from the last number of days to update the system.

A daily backup reduces the risk of your being unable to restore the current database status if you're unable to use the relevant log files.

If you don't perform a daily backup, you require a large number of log files to update the system. This step increases the duration of the restore process due to the volume of files involved and also increases the risk of your being unable to

restore the database to the current status due to individual defective transaction logs.

Weekly Backups

A restore is performed using the full backup from the previous week, which dates from four days ago. Keep the following in mind:

- ▶ Ten log files are created every day.
- ▶ As a result, the system must be updated with 40 files (10 log files × 4 days).
- ▶ You require 120 minutes to load the log files from the tape to the hard drive (40 files × 3 minutes per file).
- ▶ You require 200 minutes to update the database with the log files (40 files × 5 minutes per file).

The total time required for the restore—not taking account of the actual database files—is 320 minutes (or 5.3 hours).

[Ex]

Daily Backup

A restore is performed using the full backup from the night before. Keep the following in mind:

- ▶ A maximum of 10 log files are created every day.
- ▶ You require 30 minutes to load the log files from the tape to the hard drive (10 files × 3 minutes per file).
- ▶ You require 50 minutes to update the database with the log files (10 files × 5 minutes per file).

The total time required for the restore—not taking account of the actual database files—is 80 minutes (or 1.3 hours).

[Ex]

As illustrated in these examples, a restore takes much longer to perform if backups are made on a weekly rather than a daily basis. These examples also demonstrate that the time required to restore the log files depends on the size of the files and on the number of days that have elapsed since the last full backup was performed. The process can quickly become unmanageable in the case of large log files (e.g., 100MB or more per hour). By performing full database backups on a more frequent basis (i.e., by leaving fewer days between backups), you can automatically reduce the time required for a restore.

You therefore need to weigh the question of whether performing a full database backup on a daily basis with fewer files is a more viable option for your system,

based on the volume of transactions involved, than, for example, performing a full backup on a weekly basis with an accordingly higher number of transaction logs to be reloaded. Of course, this decision also depends on the importance of the SAP system in the context of your enterprise's business processes.

[+]

Daily Full Database Backups

You should have a very good reason not to perform a daily backup of your production database (e.g., your database is too big to be backed up overnight). In recent years, the cost of storage space has fallen to such a degree that a backup strategy based on a full daily backup is no longer impractical. SAP recommends that you perform a fully daily backup of the production database and that you store the 28 most recent backups.

Transaction Logs

Transaction logs form part of a database backup and are essential to performing a database restore. These logs contain all changes made to the database. They allow you to undo these changes and to restore the database to its most recent status after a system failure. It's essential to have a complete backup copy of all transaction logs. If even a single log can't be used when you need to perform a restore, the database can't be restored beyond the point at which this gap occurs.

[Ex]

Damaged Log Files

A log file from Tuesday is damaged. The system fails two days later, on Thursday. You can only restore the database up to the last error-free log from Tuesday. From the point at which the damaged log occurs, all subsequent transactions are lost.

The frequency of log backups is also a business decision, based on the following factors:

- ▶ Transaction volume
- ▶ Critical periods for the system
- ▶ Volume of data that management can tolerate losing
- ▶ Resources required for the backup

[+]

Intervals Between Log Backups

The following principle applies here: The greater the volume of transactions, the shorter the intervals that you should leave between the individual log backups. In this way, the

volume of data that can be lost in the event of a potential disaster in the data center is automatically reduced.

To back up the transaction logs, follow these steps:

1. Save the transaction log to the hard disk.
2. Copy this backup to a backup file server located at another site. You should always use verifications when you save your logs across a network.
The backup file server should ideally be located in another building or another city. A remote location increases the chances of your backup remaining intact if the primary data center (containing the SAP servers) is destroyed.
3. Save the transaction log backups from both servers (the SAP server and backup file server), together with the other files from the operating system level to tape on a daily basis.

Database Stops When the Backup Directory Is Full

Transaction logs are stored in a directory, which must have sufficient storage space. The database stops when the available memory in the directory is completely occupied by the transaction logs. If no further processing can take place in the database, the entire SAP system stops also. It's therefore important to think ahead and to back up transaction logs on a regular basis.

[!]

If a backup file server in a separate location isn't available to you, you must save the transaction log backups to tape after each log backup operation and send the tapes to another location on a regular basis.

No Backups in Append Mode

Don't back up the logs to tape in *append mode*. In this mode, several backups are written to the same tape. In the event of an emergency, all backups on this tape may be lost.

[!]

Files at the Operating System Level

You also need to back up files at the operating system level:

- ▶ Configuration of the operating environment (e.g., system and network configuration)
- ▶ SAP files (e.g., kernels)
- ▶ System profiles

- ▶ Spool files
- ▶ Transport files
- ▶ Other SAP-related applications
- ▶ Interfaces or add-on products that save their data or configurations outside of the SAP database

The data volume of these files is relatively small compared to the SAP database. Depending on how your system works, the backup of the files in the list may only comprise a few hundred megabytes to a few gigabytes. In addition, some of the files may contain static data, which remains unchanged for months at a time.

The frequency of backups at the operating system level depends on the applications involved. If you need to ensure synchronicity between these application files and the SAP system, they must be backed up with the same frequency as the logs.

[Ex]

Synchronizing Application Files and the SAP System

One example of this scenario is a tax calculation program, which stores VAT data outside of the SAP system. These files must correspond exactly to the sales orders in the system.

A quick and easy method of backing up operating system files is to copy all files to the hard drive of a second server. A range of products for backing up data at the operating system level is available on the market at the present time. You can then back up all required files to tape from the second server. This approach minimizes the periods during which files are unavailable.

6.1.2 Backup Types

We can distinguish between different types of database backups based on the following three questions:

- ▶ What is backed up? Is the backup a full or incremental backup?
- ▶ How is it backed up? Online or offline?
- ▶ When is it backed up? Is the backup scheduled or ad hoc?

You can, in principle, combine the various answers to these questions to produce a range of options. Each variant has its benefits and drawbacks, which are discussed next.

What Is Backed Up?

In terms of the scope of the database backup, you can choose between a full or partial backup, as described here:

- ▶ **Full database backup**
Note the following considerations:
 - ▶ *Advantages:* The database as a whole is backed up, which makes a database restore faster and easier to perform. Fewer transaction logs are required to update the database.
 - ▶ *Disadvantages:* A full backup takes longer to complete than an incremental backup. As a result, users are disrupted for a longer period. You should therefore only perform full backups outside of normal business hours.
- ▶ **Incremental backup with transaction logs**
Note the following considerations:
 - ▶ *Advantages:* An incremental backup is much quicker than a full database backup. Because the backup takes less time to complete, users are impacted for shorter periods and, in most cases, to a barely noticeable degree.
 - ▶ *Disadvantages:* A full backup is required to restore the database. Restoring the database with incremental transaction logs takes much longer and is more complicated than a restore based on a full backup. The most recent full backup must be used for the restore, and the system then has to be updated with all logs dating from the time when the full backup was made. If several days have elapsed since the last full backup, a very large number of logs have to be restored if the system fails. If you're unable to restore one of these logs, you'll also be unable to restore any subsequent log.

A third option may also be available to you, depending on your database and operating system (see Table 6.1):

- ▶ **Differential backup**
In this case, you only back up the changes that have been made since the most recent full backup. One commonly used approach is to perform a full backup every weekend and differential backups during the week.
 - ▶ *Advantages:* The risk of your being unable to perform a full restore because of damaged log backups is reduced. A differential backup saves all changes made to the database since the last full backup.

- ▶ *Disadvantages:* As with an incremental backup, you still require a full backup as a basis for restoring the database. A differential backup may take longer to complete than a backup of the transaction logs. Initially (after the full backup), it will take less time, but the process will gradually become longer over time as more data are changed.

[!]

Full Backup as a Basis for an Incremental Backup

Note that an incremental backup always comprises a full backup *and* a backup of the subsequent transaction logs. A restore based on incremental backups becomes problematic as soon as the underlying full backup or one of the transaction logs is damaged or lost.

How Is It Backed Up?

In terms of backup mode, we can distinguish between *offline* and *online*, based on the system status of the SAP system and the database. To perform an offline backup, you must disconnect the SAP system from the database and stop work in the SAP system. An online backup, on the other hand, is performed during normal operation of the database and SAP system.

- ▶ **Offline**
Benefits
 - ▶ An offline backup is faster than an online backup.
 - ▶ There are no complications caused by changes to data in the database during the backup.
 - ▶ All files are backed up at the same time and give a consistent picture of the system; the corresponding operating system files are synchronized with the SAP database.
 - ▶ You can execute a binary verification during an offline backup. However, this doubles the time required to perform the backup.
 - ▶ An offline backup doesn't require the SAP system to be stopped. The SAP buffer is therefore preserved.

Drawbacks

- ▶ The SAP system isn't available during an offline backup.
- ▶ When the database is stopped, the database buffer is also cleared of all data. This operation has a negative impact on performance, with this effect lasting until the buffer is filled with data once again.

- ▶ **Online**
Benefits
 - ▶ The SAP system is available to users during the backup. This is essential if the system is in constant demand 24/7.
 - ▶ The buffers aren't cleared. As a result, there is no negative impact on performance following the backup.

Drawbacks

- ▶ An online backup is slower than an offline backup. The time taken to complete the backup increases over time because the backup runs during normal operation and uses system resources.
- ▶ Online performance deteriorates during the backup.
- ▶ The data in the database may change while the backup is still in progress. Transaction logs are therefore particularly important to ensure a successful restore.
- ▶ The corresponding files at the operating system level may possibly no longer be synchronized with the SAP database.

Transaction Logs in an Online Backup

If you use online backups, transaction logs are particularly important to ensure a successful restore.

[!]

When Is It Backed Up?

You can select the time at which a database backup is performed based on a backup schedule or spontaneously as the need arises in a specific situation. For more information about the tools and transactions mentioned in the following, refer to Chapter 8:

- ▶ **Planned**
Planned backups are performed on a regular basis, for example, daily or weekly. For normal operation, you can use the DBA Planning Calendar (Transaction DB13) to configure an automated backup schedule for the database and transaction logs. You can use this calendar to set up and check backup cycles. You also have the option of performing important database checks and updating the statistics. You can display the status of your backups in the DB Backup Monitor (Transaction DB12).

► Ad hoc

Ad hoc backups are spontaneous backups performed on an as-needed basis, for example, prior to large-scale system changes, in preparation for an SAP upgrade, or after a structural change to the database (such as the addition of a data file). Backups that are monitored directly by the user or are performed on an as-needed basis can either be initiated using the DBA Planning Calendar or at the database or operating system level.

The DBA Scheduling Calendar can be used for both regular, planned backups and spontaneous backups. However, tools at the database level, such as SQL Server Management Studio for Microsoft SQL Server or BR* Tools under Oracle, are more commonly used for these ad hoc backups. Regardless of the backup method you select, you should always set the following goals:

- Create a reliable backup that can be used to restore the database.
- Use a simple backup strategy.
- Reduce the number of interdependencies required for operation.
- Try to eliminate or minimize the impact on the work being done in the system by business department users.

Weigh up the needs of system security and performance to use the available options to develop the best possible backup strategy for your system.

Database System-Specific Terminology

Table 6.1 compares the terminology that is used in relation to the various methods outlined in the previous sections and for backing up various database systems. The backup methods and jobs have different names, depending on which database your system uses. However, the underlying principle is always the same. If in doubt, consult your database administrator or the documentation provided for your database system.

	Full Database Backup	Content	Partial Data-base Backup	Log Backup
DB2 UDB	Full database backup in TSM (Tivoli Storage Manager)	Offline/online tablespace backup in TSM	Incremental database backup with DB2 UDB in TSM	Archiving of inactive log files in TSM

Table 6.1 Terminology of Backups

	Full Database Backup	Content	Partial Data-base Backup	Log Backup
	Full database backup to storage device	Offline/online tablespace backup to storage device	Incremental database backup with DB2 UDB to storage device	Archiving of inactive log files on storage device
	Full database backup with vendor library	Offline tablespace backup with vendor library	Incremental database backup with DB2 UDB and vendor library	One-step archiving in storage software
SQL Server	Full database backup		Differential database backup	Transaction log backup
Oracle	Full database backup offline and new log backup	Full offline database backup	Partial offline database backup	New log backup
	Full database backup online and new log backup	Full online database backup	Partial online database backup	

Table 6.1 Terminology of Backups (Cont.)

6.1.3 Backup Strategy

Your backup strategy unites and defines all measures used to back up your system and specifies when exactly backups are to be performed, the intervals at which they are to be performed, and the backup method that is to be employed. You should document this strategy in the form of a *backup frequency table* in a backup concept and ensure that it meets the needs of management and the business departments.

You then implement your *backup strategy* with the appropriate backup tools. Ultimately, however, your choice of tool to implement the strategy is of little relevance, be it one of the SAP-internal tools mentioned previously or the standard tools provided in your database or operating system. The most important criteria when selecting tools are manageability, reliability, and the monitoring options.

To develop a backup strategy, follow these steps:

- 1. **Determine your requirements for performing a restore and your tolerance range in the event of a system failure.**
A generally acceptable system downtime can't be defined because this will differ significantly between one enterprise and the next. The costs incurred by system downtime include the cost of production downtime, plus the costs of performing a restore, such as time, money, and so on. These costs should have a sliding scale, similar to that used for insurance premiums. With insurance, the more coverage you require, the greater the premium you have to pay. If we apply this model to a system restore, we get the following rule: The faster a restore is completed, the more expensive the solution you'll have to use.
- 2. **Determine which combination of hardware, software, and processes is used in the desired solution.**
Better hardware makes a backup and restore faster, better software makes these operations easier, and well-defined processes make them more efficient. Of course, this all comes at a price, and the benefits will have to be weighed against the costs. However, it's even more important that your method be reliable.
- 3. **To test your backup method, implement the hardware, and check the actual runtimes and test results.**
Ensure that you obtain results for all backup types used in your environment and not only those you intend to use. This information will facilitate future evaluation and capacity planning decisions and, if necessary, provide a sound basis for comparison.
- 4. **Test your restore method by simulating various system failure scenarios.**
Document all aspects of the restore; include questions such as who will take care of specific tasks, which users are to be notified, and so on (see Chapter 7). You should also consider the likelihood that a restore may occur exactly when you least expect it. You should therefore conduct testing on an ongoing basis and perform additional tests whenever changes are made to hardware or software components.

Schedule additional backups on specific dates (e.g., end of the month, end of the year) alongside your daily and weekly backup cycles. These aren't strictly necessary but can, for example, be archived separately as a safeguard against a disaster (see Chapter 7).

6.1.4 Strategy Recommendations

This section provides some further tips and recommendations for developing a backup strategy.

Databases

As discussed previously, we recommend that you perform a full database backup every day, provided that the cost of doing so isn't prohibitively high. If your database is too large for a daily backup, you should perform a full backup once a week instead.

Testing Your Backups

Your backups need to be tested on a regular basis. To do this, you need to restore the system and then conduct a test to determine whether the restore has been completed to your satisfaction. Without testing your backups, you can't tell whether all of the required data has actually been backed up on the tape or hard disk.

Why Testing Your Backups Is Essential

Various files were backed up, but the APPEND switch was set incorrectly for the second file and all subsequent files. As a result, the files weren't saved to tape in sequence. Instead, the tape was rewound after each file was backed up and prior to the backup of the next file. The outcome is that all files except for the last file to be backed up were overwritten.

[Ex]

Test Finished Backups Only

You can only test a backup after *all* files have been backed up. If you test your backup after each individual file, the system will be unable to detect whether the previous file has been overwritten.

[!]

Database Integrity

You need to check the integrity of the database regularly to ensure that it contains no damaged blocks. Otherwise, defective blocks may remain undetected during a backup. If possible, conduct an integrity test once a week outside of business hours. This can be scheduled with the DBA Planning Calendar.

Transaction Logs

It's extremely important that you back up your transaction logs. The database and, therefore, also the SAP system, stops when the memory that is available for storing the transaction logs is full.

For this reason, monitor the number of transaction logs in your system, and define your own backup interval, for example, hourly, based on your monitoring findings. The intervals between the backups correspond to the maximum data volume that you can tolerate losing. The risk is naturally higher for an enterprise with a large transaction volume. In this case, it would be advisable to perform a backup every 30 minutes, for example. If your enterprise has a shipping department that starts work at 3:00am, or a production line that works until 10:00pm, you should begin making backups earlier or stop later as required. Transaction logs can be backed up during normal operation without any impact on users.

Files at the Operating System Level

The frequency of backups at the operating system level depends on the applications involved. If you need to ensure synchronicity between the application files and the SAP system, they must be backed up with the same frequency as the database and logs. If perfect synchronicity is less important, you can also back up the application files less frequently.

Backup Strategy Checklist

You need to develop an appropriate system for backing up valuable system data. You should define a suitable strategy as soon as possible to avoid a possible loss of data. You should have worked through a checklist covering all backup-relevant topics before your system goes live (see Table 6.2).

Question, Task, or Decision	Done
Decide how frequently you want to perform a full database backup.	
Decide whether partial or differential backups are required.	
Decide whether to use automatic backups. If you want to use automatic back-ups, decide where to do this (in the DBA Planning Calendar or elsewhere).	

Table 6.2 Backup Strategy Checklist

Question, Task, or Decision	Done
Decide how frequently the transaction logs are to be backed up.	
Define which backup media (hard disks, tapes, etc.) you want to use.	
Ensure that you can store a day's volume of logs on the server.	
Ensure that you have sufficient memory in the directory for transaction logs.	
Set up the authorizations required for the SAP system, the operating system, and the database.	
Consider whether you want to use the DBA Planning Calendar to schedule the backup of transaction logs.	
Work out guidelines for labeling data carriers to ensure a smooth workflow.	
Decide on the period for which your backups are to be stored.	
Acquire the required hardware (hard disks) or define the size of the tape pool required (tapes required per day × retention period + 20%).	
Take account of future growth and special requirements.	
Initialize the tapes.	
Define a storage strategy for the tapes.	
Document the backup procedures in an instruction manual.	
Train users in the backup procedures.	
Implement a backup strategy.	
Perform a backup and restore for testing purposes.	
Define a contingency plan for emergencies, and decide which users are to be contacted in the event of an emergency.	

Table 6.2 Backup Strategy Checklist (Cont.)

6.2 Restore

You usually perform a restore for one of the following reasons:

- ▶ Disaster recovery following an emergency situation (see Chapter 7)
- ▶ Testing of your disaster recovery plan (see Chapter 7)
- ▶ Copying your database into another system (see Chapter 2)

You access the backups that are made on a regular basis to perform a system restore. In the context of disaster recovery, you usually restart the database and,

if necessary, the operating system, using the most recent full backup. You then import the transaction logs that have been created since the full backup. When this procedure is successfully completed, the system once again has the status it had at the time the last error-free log backup was made. The duration of this restore is of critical importance. You want it to be completed as quickly as possible so that the system can be used again after an outage, and the disruption to business processes can be kept to a minimum.

For a *database copy* (e.g., in the context of regular updating of the QA system using a copy of the production system), you normally either import the most recent full backup or generate a live copy using data streaming. Transaction logs are usually ignored.

As in your system backup strategy, you should also have a *restore strategy* in your arsenal, which can be deployed in the event of an emergency. The following factors may influence your restore strategy:

- ▶ Business costs incurred by system downtimes
- ▶ Operational schedules
- ▶ Global or local users
- ▶ Number of transactions per hour
- ▶ Budget

The development of a restore strategy is discussed in detail in Chapter 7. The actual process of restoring the SAP system and database isn't discussed in this book because this task varies widely between different systems and databases. If in doubt, consult an expert (e.g., your database administrator or an external Basis consultant) who can provide you with operational support for this critical process. You should also collaborate with your database administrator or consultant to test and document the restore process. This transfer of knowledge will soon enable you to perform a restore on your own.

[!] **An Incomplete or Incorrect Restore**

If the restore is performed incorrectly or incompletely, it may fail and have to be restarted to avoid the possibility of some files being excluded. Certain data must be entered via your database so that it can be restored subsequently. Work with an expert to identify and document this data.

Because the restore process is one of the most important tasks in the SAP system, you need to test database restores at regular intervals. Chapter 7 provides additional information on this.

6.3 Performance

The key objectives of a database restore are to restore the data as completely as possible and to minimize the time required to do so. The length of time that the SAP system is unavailable to users and, as a result, certain business processes are halted, is of critical importance to an enterprise. System performance is therefore a key factor when performing a restore.

The performance of your backup process is also important, in particular if your system is used globally 24/7. Disruption to users should be kept to a minimum during a backup. As a result, you need to strive to reduce the duration of the backup (in particular, in the case of offline backups) and to ensure adequate system reserves to guarantee acceptable system operation during an online backup.

The performance of your backup and restore processes are largely determined by data throughput on your devices. To improve throughput, you need to identify bottlenecks or devices that are limiting the throughput and eliminate or replace these. This process is subject to economic considerations because performance enhancement with additional or more modern devices is naturally also a cost factor.

This section provides tips for improving the performance of your data backups and restores by implementing some specific measures.

6.3.1 Performance Factors

The main variables, which are provided in the following list, affect the performance of both the backup and the restore:

- ▶ **Size of the database**
The larger the database, the longer it takes to back it up.
- ▶ **Hardware throughput**
This variable determines how quickly the backup can be performed. Throughput is always determined by the weakest link in the backup chain, for example:

- ▶ Database driver array
- ▶ Input/output channel (I/O) channel used
- ▶ Hard disk or tape drive

▶ **Time of backup**

This is the time or period available to you for regular system backups. Your objective here should be to minimize disruption to users. Consider both online and offline backups:

- ▶ *Online backup*: The appropriate times for performing online backups are periods during which there is a low level of system activities, which is usually early in the morning.
- ▶ *Offline backup*: The appropriate times for performing offline backups are periods during which you can shut down the SAP system, which is usually at the weekend.

The times at which you perform system restores are less critical because the system can't run in any case unless you do so.

[+] **Take into Account the Time Differences Between Different Sites**

Remember to take into account the time differences between the various sites in which your enterprise is located. For example, when it's 12:00 midday in Central Europe, it's only 6:00am in New York.

6.3.2 Backup Performance

The following approaches to improving backup performance assume that you save your backup locally on the database server. Although a backup via the network is technically possible, performance in this case depends to a large degree on network topology, overhead, and data traffic, while the throughput values of the disk systems take a backseat. In any case, the full capacity of the network is rarely available. If you perform a backup via the network, network performance also deteriorates for other users. As a result, other applications in your enterprise may be slowed down.

Backup to Faster Devices

All approaches to optimizing performance aim to prevent bottlenecks occurring on the backup device. The backup device, usually a hard disk or tape drive, is the

device that limits throughput. You should consider the following aspects in this context:

▶ **Advantages**

Faster hard disks or tape drives allow you to save an entire database within a reasonable amount of time.

▶ **Disadvantages**

Fast memory is more expensive. Hard disks or tape devices with high data throughput require willingness to invest.

Parallel Backup

A parallel backup to more than one tape drive uses a RAID-0 array (Redundant Array of Independent Disks), whereby data can be written to several media (hard disks/tapes) simultaneously. In some environments, for example, Oracle, individual tablespaces or files are backed up on separate drives at the same time. Overall performance is better than when you use a single drive.

If you have a sufficient number of tape drives that can be used in parallel, the bottleneck can be shifted from the tape drives to another component. For this reason, you also need to take account of the performance of other subsystems if you want to use the parallel backup option. These subsystems include the controller, CPU, and I/O bus. In many configurations, the controller or bus represents the limiting factor.

Restoring a Parallel Backup

When you restore a parallel backup, you need to be able to read all media in the set. If a single tape is damaged, the backup can't be used. The more tapes you have in a set, the higher the risk of one of them being damaged.

Backup to Hard Disk before Backup to Magnetic Tape

The backup on hard disks and then on tape is the fastest method to back up a database. The backup to hard disk is usually faster than the backup to tape. With this method, you can quickly save several identical copies to hard disks and, for example, store some in external enterprise locations and others at your own site.

As soon as the backup to the hard disk is complete, the impact on system performance is minimal. Because the backup to tape is made from the copy already

made on the hard disk rather than from the production database, there are no competing drains on resources from the backup and database activities. During a disaster recovery process, the data can ideally be restored from the backup on the hard disk. However, this method also has a number of disadvantages:

- ▶ You require additional hard disk space equivalent to the size of the database. If your database is large, this may give rise to immense additional costs.
- ▶ Until the backup to tape is completed, you have no protection against the risk of potential disasters occurring in the data center. In a disaster recovery scenario, you must recover the files on the hard disk first and then restore the database from the hard disk.

Other options for faster backups are also available, for example, *high availability (HA)* or modern *snapshot procedures*. However, a discussion of these options falls outside the scope of this book.

6.3.3 Restore Performance

The performance requirements for a restore are more important than those for a backup. The restore performance determines when the system will be available again and how quickly business can be resumed. Your objective in this regard is to restore the database and corresponding files quickly and make the system generally available as soon as possible.

The measures to enhance backup performance that we outlined previously also essentially result in shorter restore times. You can therefore examine these proposals from the point of view of both backup and restore performance, for example:

- ▶ **Dedicated drives**
Together with a parallel backup, restoring files and tablespaces to individual, dedicated drives accelerates the process considerably. Only one tablespace or file is written to the drive. As a result, competition for drive resources is avoided.
- ▶ **RAID systems**
RAID 0+1 is faster than RAID5, although these speeds depend on the hardware used. In more cases, the calculation of parity data for the parity drive (RAID5) is more time-consuming than writing the data twice (RAID 0+1). This option is

costly because the usable capacity only amounts to 50% of total capacity, which is significantly less with RAID5:

- ▶ $RAID\ 0+1 = [single_drive_capacity \times (number_of_drives/2)]$
- ▶ $RAID5 = [single_drive_capacity \times (number\ of\ drives - 1)]$

- ▶ **Drives with better write performance**

You can generally read data more quickly from modern drives that offer a higher write performance. Enhanced reading capacity reduces the time required to perform the restore.

- ▶ **Drive array systems with better write performance**

The benefit of a faster single drive also applies to drive arrays: As a rule, read speeds generally improve in tandem with write performance, which reduces the time required for a restore.

Measures to improve backup performance are often viewed by management as not being particularly urgent. The reason for this is that backups are usually performed out of core business hours and that enhanced performance isn't usually obvious to users. As a result, it can be difficult to obtain the additional means required for modern technology.

However, if you make the argument that clear time savings can be made in terms of the restore process, you may find that your pleas no longer fall on deaf ears. After all, you'll be able to ensure that the system is available after a disaster or emergency much sooner thanks to this technology.

6.4 Summary

The information provided in this chapter was intended to help you develop a backup strategy for your SAP systems, based on your enterprise's business framework. You can protect your systems from the worst-case scenario by combining full and incremental database backups, as well as by backing up your transaction logs and operating system files. You should aim to be able to restore the system completely within a short space of time should such a scenario arise.

The next chapter, Chapter 7, provides additional specific instructions for managing a disaster situation. Chapter 8 introduces you to the SAP-internal database tools, which you can use for automatic backups.

Even the most conscientious system administrator can become overwhelmed when faced with a system failure, a loss of data, or destruction caused by a natural disaster. For such situations, it's always good to have a plan of action and not to be caught completely off guard. This chapter suggests ways in which you can brace yourself for a disaster and prepare for a subsequent system recovery.

7 Disaster Recovery

Thousands of business processes occur on a daily basis and usually without any problems whatsoever. However, even a very brief system outage can seriously disrupt business processes and result in a loss of time, money, and resources. It's therefore advisable to plan for emergency situations so that you aren't entirely helpless when faced with such problems, irrespective of their size and complexity.

This chapter discusses a system administrator's most important task, namely *disaster recovery*, which is a form of system recovery (see Chapter 6).

7.1 Preliminary Considerations

The goal of disaster recovery is to restore the system after an *emergency* in such a way that the enterprise can continue its business processes. Because business processes come to a standstill not only during the system failure itself but also during system recovery, disaster recovery must be performed as quickly as possible. For this reason, it's even more important to have a tried-and-tested recovery plan. Furthermore, the earlier you start to plan, the better prepared you'll be in an actual emergency.

Note on the Following Explanations

This chapter isn't a guide to disaster recovery. Instead, its sole purpose is to increase your awareness of disaster recovery and to stress how important it is to develop a plan.

[!]

An emergency is anything that will damage an SAP system or cause a system failure. This includes damage to a database (e.g., accidental loading of test data into a production system), a serious hardware failure, or a complete loss of the SAP system and the infrastructure (e.g., as a result of a natural disaster or fire). In the event of such an emergency, the most important task of the system administrator is to successfully restore the SAP system. Above all else, however, the administrator should ensure that such an emergency doesn't occur in the first place.

A system administrator should be prepared for the worst and have suitable "emergency plans" in place. Disaster recovery isn't the time to try out something new because unwelcome surprises could ruin the entire recovery process.

When developing a plan, ask yourself the following questions:

- ▶ If the SAP system fails, will the entire business process fail?
- ▶ How high is the loss of earnings, and how high are the resulting costs during a system failure?
- ▶ Which important business functions can no longer be performed?
- ▶ How are customers supported?
- ▶ How long can a system failure last before an enterprise is incapable of conducting business?
- ▶ Who will coordinate and manage a disaster recovery?
- ▶ What will users do while the SAP system is down?
- ▶ How long will the system failure last?
- ▶ How long will it take to restore the SAP system?
- ▶ Which SAP system components need to be restored so that a remote recovery is possible?

Careful planning will ensure that you're less stressed in the event of an emergency because you'll already know that the system can be restored and the length of time it will potentially take to perform this system recovery.

If you discover that the time required for a system recovery is too long, and the associated losses are too high, management should consider making an additional investment in equipment, facilities, and personnel. Even though a *high availability* (HA) solution is often costly, these costs may not be as high as those associated with possible losses incurred during a disaster.

7.2 Planning for an Emergency

Creating a disaster recovery plan is considered a large project because development, testing, and documentation require a great deal of time, possibly more than a year. The documentation alone may be very extensive, possibly comprising several hundred pages.

Seek advice from experts if you don't know how to plan for an emergency. A plan that doesn't work is worse than having no plan at all because poor planning lulls an enterprise into a false sense of security. Third-party disaster recovery consultants and suppliers can support you during disaster recovery planning.

7.2.1 Which Measures Apply to Disaster Recovery?

The requirements for disaster recovery can be derived directly from the requirements for system availability, which are laid down by management. The guidelines for the requisite system availability are based, for example, on the losses that an enterprise is expected to incur in the event of a system disaster. The monetary loss is usually calculated by management and specified in USD per time unit, while the failure costs depend not only on the enterprise or sector (e.g., industry/public administration) but also on the division in which the software is used (e.g., production/purchasing).

The desired system availability is usually agreed upon in *Service Level Agreements* (SLAs) that you, as an administrator, must fulfill. Therefore, from your perspective, it's also important to know which investments (e.g., for technical equipment or service personnel) are needed to ensure a certain level of availability for the relevant system. Note that the higher the recovery costs, the less time it will take to perform a recovery. However, you can influence these costs through preventive measures (see Chapter 10) and a good recovery plan.

When it comes to technical business units, you must bear in mind that HA comes at a price. If savings are made in the wrong areas, you could be in for a rude awakening. Such costs must be included in the administrative or IT budget.

Financial Effects of a Disaster

The following discusses three examples of how to calculate financial and entrepreneurial impacts for a disaster:

[Ex]

► Example 1

When forecasting the monetary loss associated with a system failure, your enterprise discovered that transaction data can only be lost for a period of one hour. The resulting costs assume that 1,000 transactions (entered in the SAP system and not restored) will be lost each hour. Such a loss in transactions can lead to a loss in sales as well as extremely annoyed customers. If orders urgently required by customers disappear, the situation can become critical. In this case, you must ensure that the frequency with which data is backed up is sufficiently high (e.g., an hourly backup of the transaction logs).

► Example 2

In your enterprise, you discovered that a system can't be offline for more than three hours. The resulting costs (e.g., at an hourly rate of USD \$20,000) are based on the fact that no sales can be posted. In this case, you require a sufficiently efficient emergency strategy or infrastructure to ensure that the system is operational again within three hours.

► Example 3

In the event of an emergency (e.g., the loss of a building that houses the SAP data center), the enterprise can only survive a downtime of two days. After two days, customers start to conduct their business elsewhere. Consequently, an alternative method must be found to continue business (e.g., an alternative data center is built, or an emergency contract is agreed upon with an external provider).

7.2.2 When Should the Disaster Recovery Procedure Begin?

For each disaster recovery plan, you must use a unique set of criteria to determine when such a plan will come into effect and when the procedure will begin. Ask yourself the following questions:

- Which characteristics define an emergency?
- Have these characteristics been fulfilled in the current situation?
- Who must be consulted to assess the situation? The relevant person should know not only how a failure can impact the business process but also be aware of the problems associated with a recovery.

These considerations should help you decide whether or not to initiate your disaster recovery procedure. Alternatively, form a committee that will contribute and assess all of the information required to make a decision within the shortest possible time as well as make a decision in relation to implementing the recovery procedure.

7.2.3 Expected Downtime

Downtime is the period during which a system is unavailable. Even though you can only estimate downtime, it's usually longer than the restore time because, after a system recovery, some tests must be performed, user master records must be unlocked, and notifications must be sent, among other things. It's even more important to have an accurate idea of the restore time.

During downtime, it isn't possible, for example, to process orders or dispatch products. The resulting losses are just one part of the costs associated with a disaster recovery. To minimize disruption, you need to examine alternative processes that can be used while the SAP system is being restored.

During downtime, the following factors generate costs:

- The time during which the SAP system can't be used. The longer the system doesn't work, the longer it will take, after a successful recovery, to make up for the losses incurred during downtime. The transactions from the alternative processes deployed during downtime must be fed into the system to update it. This situation may be problematic in an environment that has extensive transactions.
- A failed system generates more costs than an operational system because additional technology or personnel must be used.
- Customers who can't be served or supported by the enterprise may conduct their business elsewhere.
- If follow-up processes also come to a standstill, your customers may have a claim for recourse.

What is deemed to be an acceptable downtime depends, to a large extent, on the enterprise and the nature of its business.

7.2.4 Restore Time

Restore time is the time required to restore lost data and system operability. Different emergency scenarios have different restore times, depending on the operational needs (e.g., the volume of data to be restored).

The restore time must be adapted to the requirements of the enterprise. If the current restore time exceeds the time limit for these measures, the relevant

managers must be informed of this disparity. Such a disparity can be resolved as follows:

- ▶ By investing in equipment, processes, and facilities that will shorten the restore time
- ▶ By changing the requirements of the enterprise so that longer restore times are possible

[Ex] **Minimizing Restore Times via Additional Resources**

In an enterprise, it would take a week to restore the system if just one employee was entrusted with this task. The enterprise can't afford the resulting costs or losses in revenue because, during this time, customers would conduct their business elsewhere, vendor invoices would fall due, and invoices would not be paid. In such situations, the management would have to provide additional resources to reduce the restore time to an acceptable level.

If you don't test your recovery procedure (see Section 7.8), the required restore time simply remains an estimate. Use basic testing to ensure that, in the event of an emergency, you can accurately state how much time a system recovery will require (assuming that you have a broad range of experience in this area). You can then also make more accurate statements (to the users) in relation to the expected downtime.

7.2.5 Communication in the Event of a Disaster

A communication concept should form part of your emergency plan. Even if a system failure is usually very noticeable, users can find it annoying if they are left in the dark about their situation.

In certain enterprise areas, a system failure may cause the entire operation to come to a standstill. However, those responsible can't respond appropriately if they aren't informed about when the system is expected to be available again.

If necessary, discuss the following factors with end users:

- ▶ Who is affected in the event of a system failure?
- ▶ What are the implications of a system failure for the user departments, or which particular dependencies arise?
- ▶ What is the timeframe during which information about the system failure must be imparted?

- ▶ Which information should be provided (e.g., type, cause, and extent of the disruption, and anticipated downtime)?
- ▶ Which contact persons should be informed?
- ▶ How should the information be conveyed, or what are the chains of communication?
- ▶ Which paths of communication are still available in the event of a disaster? How does communication occur if, for example, the email system is also down?
- ▶ After a system has been restored, how do we convey that the system is available again?
- ▶ To what extent is information about incident analysis and processing conveyed?

Actively incorporate communication into your recovery plan and coordinate this with the user departments. Good communication can have a calming effect in the event of an emergency because you don't have to deal with complaints and can instead concentrate on restoring the system.

7.3 Recovery Team and Role Distribution

Several people, known collectively as the *recovery team*, are usually involved in a system recovery. A highly coordinated team is the secret to implementing disaster recovery as quickly and as efficiently as possible. There are four key roles within a recovery team:

- ▶ **Recovery manager**
The recovery manager, who coordinates all activities, is responsible for the complete technical recovery.
- ▶ **Communications officer**
The communications officer looks after the users (by telephone, email, etc.) and informs upper management about the current recovery status. If one person assumes responsibility for all communication, the rest of the group can devote themselves to the actual recovery procedure without any interruptions.
- ▶ **Technical recovery team**
This team works to restore the system. If the original plans need to change during the recovery, the technical recovery team must manage such changes and coordinate the technical system recovery.

► **Test and acceptance manager**

After a recovery has taken place, the test and acceptance manager coordinates and plans the test and acceptance procedures.

The number of employees who assume these roles varies depending on the size of the enterprise. In a small enterprise, for example, one person can assume the role of recovery manager and communications officer. In addition, the descriptions and range of tasks will most likely vary depending on the needs of your enterprise.

Structure your disaster recovery concept in such a way that each team member and each role knows exactly which tasks are to be performed and when. Describe the dependencies and coordination processes between the roles, and create checklists for each team member.

[+]

Status Notice

To prevent incidents involving employees working on the recovery, we recommend that you create a status notice. Key points in the recovery plan are listed here as well as estimates in relation to when the system will be restored and operational again.

Also bear in mind that key employees may not be available in the event of an emergency (e.g., due to vacations or sick leave). Therefore, the team must also be able to perform a successful recovery without these people. In an actual emergency, this issue can be very urgent.

[!]

Planning with Employees from Other Locations

If the emergency is a major natural disaster, your on-site employees will be extremely concerned about their own families as well as the enterprise itself. In some cases, key employees may be badly or even fatally injured. You should also prepare for such situations and formulate plans accordingly. Allow for the fact that employees would have to be flown in from other locations and integrated into the recovery team.

7.4 Types of Disaster Recovery

Disaster recovery scenarios can be divided into two types:

► **In-house recovery**

In-house recovery is disaster recovery that you perform yourself at your enterprise location. The in-house infrastructure must remain intact as far as possible

(this is usually the case). Ideally, the recovery is made using the original hardware. In the worst-case scenario, the original hardware must be replaced with a backup system.

► **Remote recovery**

Remote recovery is disaster recovery performed at a special disaster recovery location. In this scenario, the entire hardware and infrastructure has been destroyed as a result of a fire, flood, earthquake, or similar. Consequently, the new servers have to be configured from scratch.

In the case of a remote recovery, you must bear in mind that a second system recovery must take place at the original location as soon as the original facility has been rebuilt. Plan and schedule the second recovery in such a way that as few users as possible are inconvenienced by the fact that the system won't be operational during this recovery.

7.5 Emergency Scenarios

Although numerous emergency scenarios are conceivable, it's impossible to develop plans for all possible scenarios. Therefore, to keep this task manageable, you should limit yourself to approximately three to five probable scenarios. If an emergency occurs, you can adhere to the scenario that best corresponds to the actual emergency. An emergency scenario comprises the following points:

- Description of the emergency
- Planning the main tasks at a high level
- Estimated downtime

The best way to prepare for an emergency is to use emergency scenarios:

1. Use Section 7.5.1 through Section 7.5.3 as a starting point, and prepare three to five scenarios that cover the largest possible range of emergencies.
2. For each scenario, create a plan for the main tasks at a high level.
3. Test the planned scenarios by simulating different emergencies and checking whether your scenarios could be applied to the actual emergency.
4. If this isn't the case, change the scenarios or develop new ones.
5. Repeat the process.

The following three examples are arranged in order of increasing severity. Note that the downtimes cited are merely examples to illustrate the situations you may encounter. Your own downtime will differ from those specified here. You must therefore replace the sample downtime with a downtime that applies to your environment. It will become clear that, depending on the specific emergency, various extensive measures must be taken and that extremely long downtimes may occur even if the damage appears to be minor.

7.5.1 Damaged Database

A database may be damaged if test data are inadvertently loaded into the production system or if data incorrectly transported into the production system causes a crash. If such an incident occurs, the SAP database and associated operating system files must be restored. The downtime is, for example, four hours.

7.5.2 Hardware Failure

The following hardware can fail:

- ▶ Processors
- ▶ Hard disks or their control unit
- ▶ RAID controller (known as an array failure)

If such a failure occurs, the following steps are necessary:

1. Replace the failed hardware.
2. If required, rebuild the server (operating system and programs).
3. Restore the SAP database and associated files.

The downtime is, for example, three days, broken down as follows:

- ▶ Two days to procure replacement hardware
- ▶ One day to rebuild the server (by one person), that is, eight working hours in total

[+]

Planning a Production Server Replacement

Plan and test the use of your test system (QAS) as a backup server if the production server (PRD) fails.

7.5.3 Complete Loss or Destruction of the Server Facility

The following components may be destroyed if a catastrophe occurs:

- ▶ The servers
- ▶ The entire supporting infrastructure
- ▶ All of the documentation and materials in the building
- ▶ The building itself

Such a complete loss of facilities may be the result of a natural disaster such as a fire, flood, hurricane, or a manmade catastrophe. If such a catastrophe occurs, the following steps are necessary:

1. Replace the destroyed facilities.
2. Replace the destroyed infrastructure.
3. Replaced the destroyed hardware.
4. Rebuild the server and the SAP environment (hardware, operating system, database, etc.).
5. Restore the SAP database and associated files.

The downtime is, for example, eight days, broken down as follows:

- ▶ At least five days to procure the hardware. If it's a regional catastrophe, it may take longer to procure the hardware because vendors may also be affected by the catastrophe.

National Vendors

Turn to national vendors that have several regional distribution centers. As an additional backup measure, you should look for alternative vendors in distant regions.

[+]

- ▶ Two days to rebuild the server (by one person), that is, 16 working hours in total.
- ▶ While the hardware is being procured and the server is being rebuilt, an alternative facility in which a minimal emergency network can be constructed must work. The integration into the emergency network may take one day, for example.

A complete loss makes it necessary to perform a recovery in a new facility or in a different building. Depending on the size of the enterprise, how important the

SAP system is for the enterprise's business processes, and the regional risk of a natural disaster, it may make sense to build a redundant data center. If one of your data centers is destroyed, operation of the system landscape can then switch to the other data center. However, both of these data centers must be built at least a few kilometers apart from each other. If housed in the same building, it's highly likely that both data centers would fail in the event of a disaster.

If your enterprise doesn't have or want to use the resources necessary for a redundant data center, you can agree on a contract for a disaster recovery location with an external provider. Then, if a disaster occurs, the provider's hardware will be available for your emergency use.

[!]

Recovery Location in an Emergency

Having a contract for a disaster recovery location doesn't guarantee that this location will be available in the event of an emergency. If a catastrophe that affects an entire region occurs, many other enterprises will want to access the same disaster recovery locations as you. In such a situation, you may have to cope without a recovery location because other enterprises will have booked the location before you.

Sometimes, the equipment in a disaster recovery location or emergency data center isn't as efficient as your production system. Therefore, when making plans, bear in mind that you'll be faced with lower performance and limited transactions. For example, reduce background jobs to only the most urgent jobs. Alternatively, only grant recovery system access to those users who need to perform essential business tasks.

7.6 Recovery Script

A recovery script is a document that contains step-by-step instructions for the following aspects:

- ▶ The procedure for restoring the SAP system
- ▶ The individuals responsible for each step
- ▶ The estimated time required for lengthy steps
- ▶ The interdependencies between steps

A script helps you implement suitable steps for restoring the SAP system and avoids the risk of any steps being omitted. If you inadvertently omit an important

step, you may have to start the entire procedure from scratch, thus delaying the system recovery.

To create a recovery script, you need the following:

- ▶ A checklist for each step
- ▶ A document that contains screenshots that explain the instructions (if required)
- ▶ Flow charts if the sequence in which the steps or activities are performed is complex or confusing

If the main person responsible for the recovery is unavailable, a recovery script will help his representative fulfill this task. The script must therefore fully describe all tasks in an easy-to-understand manner.

Important Steps in the Recovery Procedure

If you want to shorten the recovery process, you can define a procedure whereby as many tasks as possible are handled concurrently. Provide a schedule for each step. The most important steps are as follows:

1. During an emergency, you can support the recovery by doing the following:
 - ▶ Gather facts.
 - ▶ Retrieve the backup tapes from the remote storage location.
 - ▶ Have the crash kit ready (see Section 7.7).
 - ▶ Notify all relevant employees (e.g., the in-house SAP team, key users affected by the emergency, infrastructure support, IT, facilities, on-call consultants, etc.).
 - ▶ Prepare functional organizations (sales, accounting, and shipping) for alternative procedures for important business transactions and procedures.
 - ▶ Notify non-SAP systems that have interfaces from and to the SAP system about the system failure.
2. Minimize the effects of the failure by implementing the following measures:
 - ▶ Stop all additional transactions into the system (e.g., interfaces from other systems).
 - ▶ Collect transaction documents that will have to be entered again manually.

- 3. Start the planning process by implementing the following measures:
 - ▶ Analyze the problem.
 - ▶ Select the scenario plans that best correspond to the emergency that has actually occurred.
 - ▶ Change the plans, if necessary.
- 4. Decide when the disaster recovery procedure will begin:
 - ▶ Which criteria formed the basis for determining that an emergency had occurred? Were these criteria satisfied?
 - ▶ Who makes the final decision in relation to confirming that an emergency has occurred?
- 5. Ascertain whether an emergency has occurred.
- 6. Implement the recovery procedure.
- 7. Test and approve the restored system. Key users should conduct the relevant tests. Such users use a checklist to clarify whether the system has been restored to a satisfactory level.
- 8. Update the system with transactions that alternative processes handled during the system failure. As soon as this step is complete, the outcome should be approved again.
- 9. Notify users that the system is operational again.
- 10. Arrange a postmortem meeting to ascertain why the disaster occurred.
- 11. Assess the recovery team's experience of the system recovery, and optimize your disaster recovery plans accordingly.

The recovery script must be easily accessible in the event of a disaster. It must not be stored on a server that may no longer be accessible in the event of a network failure. Also bear in mind that a paper copy could be destroyed in a fire. Prepare yourself for such emergency scenarios and store the recovery script redundantly. Make sure that the storage location is widely known and accessible to those individuals responsible for a recovery in the event of an emergency.

Dependency on Other Applications

Your SAP system is usually connected, via interfaces, to other upstream or downstream systems. If the SAP system fails, feeder systems may also come to a standstill because RFCs accumulate en masse and can't be processed. In addition,

downstream systems may not work because your SAP system doesn't make the necessary data available. You can therefore see how easy it is to experience a chain reaction that will have far-reaching consequences for the system landscape and business processes.

In your recovery script, give some thought to communication with those individuals responsible for the applications connected to the SAP system. Make sure that the interfaces are stopped or stop them yourself. Decide how the data will be resynchronized after a system recovery.

7.7 Crash Kit

A *crash kit* contains everything you need to rebuild the SAP server, reinstall the SAP system, and restore the SAP database, including all related files. You must therefore store everything you need to restore your SAP environment in one or more containers physically—in the form of backup tapes, hardware, and documents—and/or digitally. If your location needs to be evacuated, you won't have any time to gather everything you need at the last minute.

You should therefore check your crash kit regularly and check whether all of the elements are still up to date and operational. A service agreement is a good example of a crash kit component that requires such a regular check. If the agreement is no longer valid because its validity period wasn't extended in time, you may not be able to access the services provided by external providers in an emergency, or you may have to enter into negotiations first.

Updating the Crash Kit

If a (hardware or software) component on the server is changed, replace the obsolete component in your crash kit with the latest, tested element.



The crash kit should be stored in a room separate from the servers. If the crash kit is stored in the server room, the crash kit will also be affected if servers are lost. Examples of suitable storage options include the following:

- ▶ A commercial data storage location outside the enterprise's location
- ▶ Other enterprise locations
- ▶ Another secure part of the building

Next, we'll name the most important items that should form part of any crash kit. You can add or omit items, depending on your particular environment. The inventory is sorted according to documentation and software.

Documentation

A crash kit must contain the following documentation:

- ▶ A disaster recovery script.
- ▶ A test and verification script for functional user groups, which is used to ascertain the functionality of the restored system.
- ▶ Installation instructions:
 - ▶ Operating system
 - ▶ Databases
 - ▶ SAP system
- ▶ Special installation instructions for the following:
 - ▶ Drivers that must be installed manually
 - ▶ Programs that must be installed in a certain way
- ▶ Copies of the following:
 - ▶ SAP licenses for all instances
 - ▶ Service agreements (with telephone numbers) for all servers

[!]

Checking the Validity of the Service Agreements

Make sure that the service agreements are still valid. You should perform this check regularly.

- ▶ Instructions for retrieving backup tapes from external data stores outside the enterprise's location.
- ▶ A list of individuals authorized to retrieve backup tapes from data stores outside the enterprise's location. This list must correspond to the list available at the external data store.
- ▶ A parts list that contains enough information to ensure that new hardware can be purchased or leased if the server is destroyed. After a certain length of time, original parts may no longer be available. You should then draft an alternative parts list. At this time, you should also give some thought to updating your equipment.

- ▶ Layout of the file system.
- ▶ Layout of hardware.
- ▶ Telephone numbers of the following:
 - ▶ Key users
 - ▶ Information service employees
 - ▶ Facilities personnel
 - ▶ Other infrastructure personnel
 - ▶ Consultants (SAP, network, etc.)
 - ▶ SAP hotline
 - ▶ Data stores outside the enterprise's location
 - ▶ Security department or security employees
 - ▶ Contact partners within the framework of service agreements
 - ▶ Hardware vendors

Software

The crash kit should contain all of the software components required to completely rebuild a server.

- ▶ Operating system:
 - ▶ Installation kit
 - ▶ Hardware drivers not contained in the installation kit (e.g., network cards or SCSI controllers)
 - ▶ Service packs, updates, and patches
- ▶ Database:
 - ▶ Installation kit
 - ▶ Service packs, updates, and patches
 - ▶ Recovery script for automating a database recovery
- ▶ SAP system:
 - ▶ New installation files of the SAP release used and the database
 - ▶ Currently installed kernel
 - ▶ System profile files

- ▶ *tpparam* file
- ▶ *saprouttab* file
- ▶ *saplogon.ini* files (for SAP GUI)
- ▶ Other programs integrated into the SAP system (e.g., a control package)
- ▶ Other software for the SAP installation:
 - ▶ Auxiliary programs
 - ▶ Backup
 - ▶ UPS control program
 - ▶ Hardware monitor
 - ▶ FTP client
 - ▶ Remote control program
 - ▶ System monitors



Crash Kit Inventory

The person who seals the crash kit should also compile a signed and dated inventory. If the seal is broken, you must assume that some items have been removed or changed, and, as a result, the kit could be completely useless in an emergency.

7.8 Testing the Disaster Recovery Procedure

By simulating a disaster recovery, you can ensure that your system can actually be restored and that all of the tasks listed in the disaster recovery plan can be executed. By performing a simulation, you can ascertain whether the following are true:

- ▶ Your disaster recovery procedure works
- ▶ Changes have occurred, steps haven't been documented, or the necessary updates haven't been performed
- ▶ Some steps require additional explanation
- ▶ Steps that are quite clear to the person writing the documentation are also clear to other individuals
- ▶ Older hardware is no longer available

If one of these scenarios arises, you must revise your recovery plan. You may also have to upgrade your hardware so that it's compatible with the equipment currently available. Furthermore, you should draft an alternative procedure in response to inconsistencies that previously went unnoticed in an emergency.

Because many factors influence the actual recovery time, it can only be determined through testing. As soon as you have actual time values instead of estimates, your emergency plan will become credible. If the procedure is practiced on a regular basis, everyone will know what to do in an emergency, thus making it possible to avoid the worst-case scenario.

To test your disaster recovery procedure, follow these steps:

1. Implement your disaster recovery plan in a backup system or at a remote location.
2. Envisage a random emergency scenario.
3. Implement your emergency plan to see if it's effective in such a situation.
4. Perform disaster recovery at the same location where it will occur in the event of an emergency. If you have more than one recovery location, run the tests in each of these locations. The equipment, facilities, and configurations may differ from location to location. Document all of the steps that need to be executed at each location. You're now immune to not being able to restore the system at a certain location in the event of an emergency. Other options for locations where you can test your disaster recovery scenario include the following:
 - ▶ A backup server at your location
 - ▶ Another enterprise location
 - ▶ Another enterprise with which you have a mutual support agreement
 - ▶ An enterprise that provides disaster recovery locations and services

During a real disaster recovery, your permanent employees will carry out the relevant tasks. However, you should take precautions in case some of your key employees are unavailable during the disaster recovery. A test procedure can therefore include the random selection of an individual who won't be available and won't participate in the test procedure. This procedure reflects a real situation in which a key employee is absent or has been seriously injured, for example.

Furthermore, employees from other locations should also participate in testing. Integrate these individuals into the tests because you may also require them

during a real disaster recovery. These employees can fill the gap arising from unavailable personnel.

At least once a year, you should run through your disaster recovery from start to finish. However, the frequency with which you do this is a commercial decision that should be made while considering the costs involved.

[!]

Maintaining the Production System

Note that during disaster recovery testing, employees are still needed to maintain the real production system.

7.9 Minimizing the Risk of Failure

There are many ways to minimize the risk of failure. Some of the suggestions listed here may seem obvious. In reality, however, they are frequently ignored.

7.9.1 Minimizing the Risk of Human Error

Many emergencies are triggered by human error (caused, for example, by an exhausted operator). For potentially dangerous tasks (such as deleting the test database, moving a file, or formatting a new drive), a script should be created with a checklist that can be used to verify the individual steps.

[+]

Critically Assessing Your Own Capabilities

Don't perform any dangerous tasks if you feel tired. If you nevertheless have to do it, seek a second opinion before you start.

7.9.2 Minimizing Single Points of Failure

A *single point of failure* occurs when the failure of a single component causes the entire system to fail. You can minimize the risk as follows:

- ▶ Ascertain the situations in which a single point of failure can occur.
- ▶ Devise a forecast of what happens when this component or process fails.
- ▶ Eliminate as many single points of failure as possible.

Single points of failure may include the following:

- ▶ The backup SAP server is in the same data center as the production SAP server. If the data center is destroyed, the backup server will also be destroyed.
- ▶ All SAP servers are connected to the same power supply. If the power supply is interrupted, this affects all of the equipment connected to this power supply. In other words, all servers crash.

Cascading Failures

A *cascading failure* occurs if one failure triggers a whole series of failures, thus making the problem even more complex. In this case, the recovery comprises a coordinated solution for numerous problems.

Cascading Failure

The following is an example of a cascading failure:

- ▶ A power outage that affects the air conditioning unit can cause the air-conditioning controls in a server room to fail.
- ▶ If the server room can't be cooled, the temperature in the room rises above the permissible operating temperature for the equipment.
- ▶ Overheating causes a hardware failure on the server.
- ▶ The hardware failure causes damage to the database.
- ▶ Overheating can also affect numerous other pieces of equipment and systems (e.g., network devices, the telephone system, and other servers).

[Ex]

A system recovery after a cascading failure can be complex because, when solving one problem, you may discover other problems or other damaged pieces of equipment. Alternatively, some equipment can't be tested or repaired until other pieces of equipment become operational again. In the air-conditioning example, a system could monitor the air-conditioning unit or the temperature of the server room and notify the relevant employees when a certain threshold value is exceeded.

7.10 Continuing Business During a System Recovery

During disaster recovery, any affected business processes must continue as soon as possible to avoid or minimize an enterprise's financial losses. Give some thought to which alternative procedures can support key business processes when an SAP system fails, for example:

- ▶ Collection of cash
- ▶ Order processing
- ▶ Product shipping
- ▶ Invoice payments
- ▶ Payroll
- ▶ Alternative locations for continuing business

If there's no alternative process, your business operations will decline or come to a complete standstill, which may result in the following problems:

- ▶ Orders can't be entered
- ▶ Products can't be shipped
- ▶ Cash can't be collected

The following alternative processes are conceivable:

- ▶ Manual data entry in paper form (e.g., handwritten purchase orders)
- ▶ Working on standalone PC systems

Together with your end users, plan how certain business processes can continue to run during a system recovery. Define when or during which expected downtime an alternative process will enter into force. Furthermore, give some thought to how data generated during the emergency process can be transferred to the SAP system after the system recovery.

7.11 Summary

Disaster recovery is a special type of system recovery that requires proper advance preparation. An in-depth concept, the necessary tools, and planned testing on a regular basis will all contribute to helping you prepare for an emergency. This chapter helps you think of everything you need.

Calculate the costs that your enterprise and systems would incur as a result of a system failure or the losses that would arise if a system were unavailable for a period of one hour. Concrete figures are the easiest way to convince everyone of the need to invest in disaster recovery.

Contents

Preface	17
1 Fundamentals of SAP System Administration	23
1.1 System Administrator Tasks	23
1.2 Guiding Principles for System Administrators	25
1.3 Definitions	31
1.4 Summary	33
2 SAP System Administration	35
2.1 Starting and Stopping the SAP System	35
2.1.1 Starting the SAP System	36
2.1.2 Stopping the SAP System	40
2.2 Instances and Operation Modes	46
2.3 Maintaining Profile Parameters	61
2.4 Specific Monitoring Transactions	68
2.4.1 System Log	69
2.4.2 ABAP Dump Analysis	71
2.4.3 Checking Application Servers and Work Processes	76
2.4.4 Lock Entries	78
2.4.5 Canceled Update Requests	81
2.5 System Messages	85
2.6 Connections	88
2.6.1 RFC Destinations	88
2.6.2 SAP Gateway Monitor	97
2.6.3 SAPconnect	98
2.6.4 Message Server Monitor	103
2.6.5 Internet Communication Framework	105
2.6.6 ICM Monitor	108
2.7 Client Administration	111
2.7.1 Creating Clients	111
2.7.2 Copying Clients	115
2.7.3 Deleting Clients	128
2.7.4 Checking the Client Copy Log	130

2.8	System Copy	132
2.8.1	A Database Copy of the Production System	133
2.8.2	Client Copy with Data	134
2.8.3	Client Copy without Data	134
2.9	Summary	135
3	System Monitoring	137
3.1	CCMS Alert Monitor	137
3.2	System Monitoring with the Standard CCMS Alert Monitor	139
3.3	Adapting the CCMS Monitor Sets	148
3.3.1	Hiding Monitor Sets	149
3.3.2	Defining a New Monitor Set	154
3.3.3	Adding a Monitor to a Monitor Set	156
3.3.4	Deleting a Monitor from a Monitor Set	159
3.3.5	Changing Alert Thresholds	162
3.4	Auto-Reaction Methods	165
3.4.1	Changing an Auto-Reaction Method	165
3.4.2	Assigning an Auto-Reaction Method to a Monitor Object	170
3.5	Summary	176
4	System Administration Using SAP Solution Manager	177
4.1	Functional Spectrum of SAP Solution Manager	178
4.2	Maintaining the System Landscape	180
4.2.1	Transferring System Data to SAP Solution Manager	180
4.2.2	Creating a Product System	185
4.2.3	Creating a Logical Component	189
4.2.4	Solutions	193
4.2.5	Configuring Managed Systems	197
4.3	System Administration	206
4.3.1	Technical Monitoring and Alerting	206
4.3.2	End-to-End Analysis	223
4.3.3	Configuration Validation	230
4.3.4	SAP EarlyWatch Alert	236
4.3.5	System Recommendations	243
4.3.6	Managing Service Connections	245
4.3.7	License Administration	249
4.4	Maintenance Optimizer	251
4.5	Summary	262

5	Scheduled Tasks	263
5.1	Critical Tasks	264
5.1.1	Check Whether the SAP System Is Running	264
5.1.2	Checks to Determine Whether Your Backups Have Been Successful	264
5.2	Daily Tasks	267
5.2.1	Critical Tasks	268
5.2.2	SAP System	268
5.2.3	Databases	271
5.2.4	Operating System	271
5.2.5	Other	271
5.3	Weekly Tasks	272
5.3.1	SAP System	272
5.3.2	Databases	272
5.3.3	Operating System	273
5.3.4	Other	273
5.3.5	Overview of Transactions	274
5.4	Monthly Tasks	274
5.4.1	SAP System, Database, Operating System, Other	274
5.4.2	Checking Consumable Items	276
5.5	Quarterly Tasks	277
5.5.1	SAP System	277
5.5.2	Databases	278
5.5.3	Operating System	278
5.5.4	Other	279
5.6	Yearly Tasks	279
5.6.1	SAP System	279
5.6.2	Databases	281
5.6.3	Operating System	281
5.6.4	Other	281
5.6.5	Overview of Transactions	282
5.7	Summary	283
6	Backup and Restore	285
6.1	Backup	285
6.1.1	What Has to Be Saved?	286
6.1.2	Backup Types	290
6.1.3	Backup Strategy	295
6.1.4	Strategy Recommendations	297

6.2	Restore	299
6.3	Performance	301
6.3.1	Performance Factors	301
6.3.2	Backup Performance	302
6.3.3	Restore Performance	304
6.4	Summary	305
7	Disaster Recovery	307
7.1	Preliminary Considerations	307
7.2	Planning for an Emergency	309
7.2.1	Which Measures Apply to Disaster Recovery?	309
7.2.2	When Should the Disaster Recovery Procedure Begin?	310
7.2.3	Expected Downtime	311
7.2.4	Restore Time	311
7.2.5	Communication in the Event of a Disaster	312
7.3	Recovery Team and Role Distribution	313
7.4	Types of Disaster Recovery	314
7.5	Emergency Scenarios	315
7.5.1	Damaged Database	316
7.5.2	Hardware Failure	316
7.5.3	Complete Loss or Destruction of the Server Facility	317
7.6	Recovery Script	318
7.7	Crash Kit	321
7.8	Testing the Disaster Recovery Procedure	324
7.9	Minimizing the Risk of Failure	326
7.9.1	Minimizing the Risk of Human Error	326
7.9.2	Minimizing Single Points of Failure	326
7.10	Continuing Business During a System Recovery	327
7.11	Summary	328
8	Database Administration	329
8.1	Planning Database Administration Tasks	330
8.1.1	Planning Database Tasks	330
8.1.2	Changing and Deleting Database Tasks	335
8.1.3	Checking the DBA Planning Calendar	338
8.2	Checking Database Actions	340
8.3	Performing a Database Analysis	346
8.4	Monitoring Database Performance	351
8.5	Database Administration—DB2	356

8.5.1	DB2 Command Line Processor	357
8.5.2	Establishing a Connection to the DB2 Database	358
8.5.3	Starting and Stopping the Database	360
8.5.4	Executing SQL Statements	362
8.5.5	Updating and Checking the Database Manager Configuration	362
8.5.6	Updating and Checking the Database Configuration	365
8.5.7	Automatic Storage Management	366
8.5.8	Backing Up the Database	367
8.5.9	Restoring the Database	370
8.5.10	DBA Cockpit for DB2 for LUW	373
8.6	Database Administration—Oracle	376
8.6.1	SQL*Plus	376
8.6.2	Starting and Stopping the Database	379
8.6.3	Executing SQL Statements and SQL Scripts	386
8.6.4	Managing the Database Using SQL*Plus	387
8.6.5	Managing the Database Using the BR*Tools	388
8.6.6	Backing Up the Database	402
8.6.7	Restoring the Database	406
8.6.8	Checking the Database	409
8.7	Database Administration—Microsoft SQL Server	413
8.7.1	SQL Server Management Studio	414
8.7.2	Starting and Stopping the Database	417
8.7.3	Files and Logs	419
8.7.4	Initiating a Backup Process	424
8.7.5	Setting Up Maintenance Plans for a Backup	428
8.7.6	Backing Up System Databases	433
8.7.7	SQL Server Logs	436
8.8	Database Administration—SAP MaxDB	437
8.8.1	Database Studio	437
8.8.2	Starting and Stopping the Database	438
8.8.3	Database Monitoring	440
8.8.4	Backing Up the Database	444
8.9	Database Administration—SAP HANA	448
8.9.1	Technical Background	449
8.9.2	SAP HANA Studio	450
8.9.3	Starting and Stopping the Database	459
8.9.4	Database Monitoring	463
8.9.5	Configuring the Database Backup	467
8.9.6	Backing Up the Database	469
8.9.7	Restoring the Database	471
8.10	Summary	475

9	Operating System Administration	477
9.1	Checking the Memory Usage of the File System	477
9.1.1	Monitoring the File System Using the CCMS Alert Monitor	478
9.1.2	Changing Alert Thresholds	481
9.1.3	Releasing Memory at the Operating System Level	482
9.2	Retrieving Operating System Information	486
9.3	Summary	491
10	Security Administration	493
10.1	What Is Security?	493
10.1.1	Protecting Data against Damage or Loss	494
10.1.2	Adhering to Legal or Quasi-Legal Provisions	494
10.2	Security Levels	495
10.2.1	Access Security	495
10.2.2	Operational Security	497
10.2.3	Data Security	498
10.3	Safeguarding the SAP System	499
10.3.1	Preventing Multiple User Logons	500
10.3.2	Passwords	501
10.3.3	Limiting Access for SAP* or DDIC Users	504
10.3.4	Locking Critical Transactions	505
10.3.5	Preventing Changes in the Production System	508
10.3.6	Operational Security	513
10.4	Audits	514
10.4.1	Auditing Aspects	515
10.4.2	Auditing Tasks for SAP Administrators	516
10.5	Auditing Tools	517
10.5.1	Audit Information System	517
10.5.2	Security Audit Log	519
10.6	Summary	535
11	Performance	537
11.1	Short-Term Remedy of Performance Problems	537
11.2	Detailed Analysis of Performance Problems	542
11.2.1	System Load Analysis	543
11.2.2	Buffer Analysis	548
11.2.3	Memory Defragmentation	550

11.3	Analysis at Other Levels	551
11.3.1	Analysis at the Database Level	551
11.3.2	Analysis at the Operating System Level	551
11.3.3	Analysis at the Hardware Level	552
11.4	Summary	552
12	SAP GUI	553
12.1	Installation Requirements	553
12.1.1	Minimum Requirements for the User's PC	553
12.1.2	Network Functions	554
12.2	Installation Scenarios	554
12.2.1	Installing SAP GUI from an Installation Medium	555
12.2.2	Installing SAP GUI from an Installation Server	558
12.3	Adding Systems to SAP Logon	574
12.4	Summary	578
13	User Administration	579
13.1	General	579
13.2	Setting Up New Users	582
13.2.1	Copying Existing Users	582
13.2.2	Creating a New User	591
13.3	Maintaining Users	591
13.4	Mass Changes	592
13.5	Resetting the Password	594
13.6	Locking or Unlocking a User	596
13.7	Central User Administration	597
13.7.1	Setting Up a Central User Administration	598
13.7.2	Creating and Maintaining Users via a Central User Administration	616
13.7.3	Troubleshooting	620
13.7.4	Deactivating or Deleting a Central User Administration ...	623
13.8	User Groups	632
13.9	Deleting User Sessions	635
13.9.1	Displaying Active Users	635
13.9.2	Deleting User Sessions	637
13.10	System Administration	638
13.10.1	Special User IDs	638
13.10.2	Special Authorizations	639
13.10.3	User Passwords	640
13.11	Summary	641

14 Authorization Management	643
14.1 Authorization Check Process	643
14.2 Authorization Roles	644
14.2.1 Creating and Maintaining Single Roles	645
14.2.2 Creating and Maintaining Composite Roles	656
14.3 Authorization Profiles	662
14.4 Utilities for Authorization Management	667
14.4.1 Default Values and Check Indicators	667
14.4.2 Authorization Trace	672
14.4.3 Infosystem Authorizations	677
14.5 Summary	679
15 Background Processing	681
15.1 Creating Background Jobs	681
15.1.1 General	682
15.1.2 Creating and Scheduling Background Jobs	684
15.2 Monitoring Background Jobs	691
15.3 Graphical Job Scheduling Monitor	694
15.4 Performance Factors for Background Jobs	695
15.5 Summary	697
16 Output Management	699
16.1 Setting Up the Spool Servers	699
16.2 Setting Up Printers	703
16.2.1 Configuring Network Printers	703
16.2.2 Setting Up Frontend Printers	709
16.2.3 Transporting Output Devices	712
16.3 Outputting Data	714
16.4 Output Control	716
16.5 Deleting Old Spool Requests	724
16.6 Checking the Spool Consistency	724
16.7 Checking the TemSe Consistency	726
16.8 Summary	728
17 Change and Transport Management	729
17.1 General Notes on Change Management	730
17.2 Transporting Objects	732

17.2.1 Creating a Transport Request	733
17.2.2 Recording Changes in a Transport Request	736
17.2.3 Releasing a Transport Request	738
17.2.4 Importing Transport Requests	742
17.2.5 Checking the Transport Log	748
17.2.6 Checking the History	750
17.3 Direct Table Maintenance	752
17.4 Summary	758

18 System Maintenance 759

18.1 Downloading SAP Support Packages	760
18.1.1 Determining the System's Current Support Package Level	761
18.1.2 Finding Support Packages	766
18.1.3 Downloading Support Packages	781
18.2 Important Notes on Preparing and Executing System Maintenance	783
18.3 Performing a Kernel Update	784
18.3.1 Kernel Backup	785
18.3.2 Unpacking a New Kernel	786
18.3.3 Stopping the SAP System	787
18.3.4 Replacing Kernel Files	788
18.3.5 Starting the SAP System and Checking the Logs	789
18.4 Applying the SPAM/SAINT Update	790
18.5 Importing ABAP Support Packages	794
18.5.1 Making the Support Packages Available	794
18.5.2 Importing the Support Packages	799
18.5.3 Performing a Modification Adjustment	810
18.5.4 Regenerating Objects	811
18.5.5 Performing Regression Tests	814
18.6 Installing Add-Ons	814
18.7 Summary	821

19 Diagnostics and Troubleshooting 823

19.1 Basic Procedure	823
19.2 Troubleshooting with the SAP Support Portal	826
19.2.1 Searching for SAP Notes with the SAP Support Portal	827
19.2.2 Customer Incident Messages	831
19.3 Creating a Remote Service Connection	850

19.4	Implementing SAP Notes	859
19.5	Summary	866
Appendices		867
A	Useful Transactions	869
B	Security-Relevant Transactions	875
C	Useful Tables	881
D	Forms	885
E	Bibliography	891
F	The Author	893
Index		895

Index

A

- ABAP dump, 71, 270
- Access
 - method*, 705, 710
 - security*, 495
- Account audit, 514
- Action pattern, 335
- Activate service, 106
- Add-on
 - download*, 814
 - install*, 814
 - Installation Tool*, 814
 - log*, 820
- Administration
 - update*, 85
- AIS, 507, 517
 - role*, 518
- ALE, 135
 - Central User Administration*, 598, 607
 - distribution model*, 607
 - monitoring*, 622
- Alert, 138, 213, 454
 - change threshold value*, 481
 - complete*, 146
 - email*, 463
 - group*, 214
 - notification*, 165
 - open*, 141, 144
 - threshold value*, 162
- Alert Monitor, 137, 479
 - activate maintenance function*, 149
 - adapt*, 148
 - adding a monitor*, 156
 - auto-reaction method*, 165
 - changeability*, 140
 - check*, 269
 - current status*, 140
 - email notification*, 165
 - graphical representation*, 145
 - maintain threshold value*, 162
 - modifiability*, 155
 - MTE class*, 172
 - my favorites*, 150
- Alert Monitor (Cont.)
 - operating system command*, 165
 - start*, 139
 - template*, 140
 - threshold value*, 142
 - view*, 141
 - visibility*, 150
- Append mode, 289
- Application
 - data*, 36
 - security*, 497
 - server*, 32, 46, 76
- Application Service tools, 239
- Area menu AUTH, 677
- ASM, 366
- Audit, 517
 - account audit*, 515
 - aspect*, 515
 - Audit Information System*, 517
 - report*, 517
 - security audit*, 514
 - Security Audit Log*, 519
 - tool*, 517
 - type*, 514
 - user*, 516
- Audit Information System, 507, 517
- Authorization, 497, 644
 - administration*, 643
 - check indicator*, 667
 - checking*, 280, 643
 - concept*, 644
 - critical*, 518
 - dual control principle*, 643
 - field*, 644
 - full authorization*, 652
 - infosystem*, 677
 - profile*, 662
 - SAP_ALL*, 639
 - SAP_NEW*, 639
 - trace*, 672
- Authorization administration
 - audit*, 516
 - Profile Generator*, 645
 - report*, 677
 - role*, 644

Authorization check
 activity, 644
 authorization object, 644
 check indicator, 648
 evaluation, 675
 log, 676
 process, 643
 return code, 675
 source text, 644
Authorization management, 643
 utilities, 667
Authorization object
 authorization, 644
 default value, 650, 667
 field value, 644
 object class, 644
 S_TCODE, 644
Authorization profile, 644, 662
 assign, 666
 composite profile, 662, 664
 display, 663
 generate, 653
 single profile, 662
Authorization role, 644
 AIS, 518
 assign user, 654
 authorization profile, 648
 change, 886
 composite role, 645, 656–657
 field value, 650
 menu maintenance, 646
 single role, 645
 user comparison, 654
Autoextend, 399
Automatic storage management, 366
Auto-reaction method, 165
 assign, 170
 change, 165
 copy, 167

B

Background processing, 681, 695
 create job, 684
 expiry date, 485
 graphical job monitor, 694
 job class, 685

Background processing (Cont.)
 job conflict, 696
 job log, 693
 job monitoring, 691
 Job Wizard, 690
 performance, 695
 periodic execution, 689
 schedule job, 684
 start condition, 688
 time, 696
 user ID, 686
 variant, 683
backint interface, 467
Backup, 404, 499
 ad hoc, 294
 additional, 296
 append mode, 297
 checklist, 298
 concept, 285
 daily, 287
 data, 286
 database, 286, 498
 DB Backup Monitor, 293
 dedicated drive, 304
 device, 302
 differential, 291, 369
 effectiveness, 287
 frequency, 286
 frequency table, 295
 full, 291–293
 hard disk, 303
 incremental, 369
 master database, 434
 mode, 292
 offline, 292, 368
 online, 293, 369
 operating system level, 289, 298
 parallel, 303
 performance, 301–302, 304
 planned, 293
 recommendation, 297
 redo log, 288
 SAP HANA, 467
 scope, 291
 snapshot, 370
 spontaneous, 294
 strategy, 285, 295
 tape, 303

Backup (Cont.)
 template, 446
 terminology, 294
 testing, 264, 297
 time, 293, 302
 tool, 286
 transaction log, 288, 298
 type, 290
 weekly, 287
Batch, 681
Batch input, 266
 log, 270, 484
Batch job
 background processing, 681
Batch work process, 681
BR*Tools, 376
 database administration, 388
 standard key, 389
BRBACKUP, 402
BRSPACE, 382, 385
Buffer
 analysis, 548
 hit ratio, 548
 monitoring, 270
 program buffer, 548, 550
 Program Execution Area, 550
Business blueprint, 179
Business Process Analysis, 240

C

CA Wily Introscope Enterprise Manager, 206–207
CA Wily Introscope Workstation, 221
Cascading failure, 327
CCMS, 137–138, 178, 478
 agent, 169, 787
CCMS Alert Monitor → Alert Monitor
Central instance, 32
Central User Administration, 597
 ALE, 598, 607, 622
 central system, 607
 child system, 607
 communication user, 598
 create RFC connection, 603
 create user, 617
 deactivate, 623

Central User Administration (Cont.)
 delete, 623, 627
 distribution model, 607
 distribution option, 615
 emergency deactivation, 630
 error search, 620
 field selection, 614
 generate password, 619
 IDoc monitoring, 622
 initial password, 619
 lock, 620
 logical system, 600
 maintain user, 619
 partner profile, 623, 626
 processing log, 620
 recipient, 607
 redistribution, 616
 remove system, 624
 reset password, 619
 sending system, 607
 set up, 598
 standard role, 599
 synchronization, 609
 unlock, 620
Central user maintenance
 mass maintenance, 619
Change
 analysis, 226
 client-specific, 510
 enter, 736
 prevent, 508
 request, 729
 tablespace, 387
 threshold value, 162
Change and Transport Organizer, 732
Change management, 179, 249, 252, 729
 approval, 730
 process, 730
 table maintenance, 752
Check
 authorization, 516
 indicator, 667
 items, 276
 transport tool, 803
Checklist, 27, 263
 annual tasks, 279
 database, 271–272, 278, 281
 operating system, 271, 273, 278–279, 281

Checklist (Cont.)
 quarterly tasks, 277
 SAP system, 268, 272, 277, 279
 using, 267
 weekly tasks, 272
Client
 administration, 111
 assign logical system, 601
 copy by transport request, 120
 copy log, 130
 copy profile, 117
 copy without data, 134
 copying, 114–115, 134
 create, 111
 definition, 33
 delete, 128
 export, 123
 import, 126
 local copy, 116
 lock, 510
 logon, 115
 remote copy, 120
 transport, 116, 123
Client copy
 profile, 117
 TemSe consistency check, 726
Client table, 112
Column-based storage, 449
Communication
 type, 98
 user, 598
Company address
 synchronize, 609
 user assignment, 610
Component logical, 189, 192
Composite
 profile, 662
 role, 656
Computing Center Management System →
 CCMS
Configuration store, 232
Configuration validation, 178, 230
 target system, 231
Connection, 88
 test, 93
 type, 90
Consumable items
 checking, 276

Controller, 303
Copy changes, 864
Core dump, 541
Correction and Transport System, 732
Correction instructions, 859, 862
CPS, 691
CPU
 usage, 163, 552
Crash kit, 321
 content, 322
 documentation, 322
 inventory, 324
 software, 323
 storage, 321
CTO, 732
CTS, 732
CUA log, 270
Customer incident
 create, 832
 error description, 831
 message, 830
Customer message
 sent, 841
Customizing, 36
 table maintenance, 753

D

Data
 backup, 468
 integrity, 494
 loss, 36, 498
 protect, 494
 security, 495, 498
 volume management, 178, 240
Data center
 loss, 318
 redundant, 318
Database, 36
 action, 331
 action log, 340
 action parameter, 332
 action pattern, 335
 administration, 329
 analysis, 346
 backup, 286, 340

Database (Cont.)
 consistency check, 272, 351
 copy, 133, 300
 damaged, 316
 delete occurrence, 336
 direct access, 31
 file, 163
 fill level, 354
 growth rate, 346
 integrity, 297
 job log, 338
 manager configuration, 362
 performance, 351, 551
 plan administration task, 330
 planning calendar, 330
 recovery Oracle, 406
 server, 31
 starting, 37
 stopping, 43
 table size, 349
 task, 330
Database administration
 daily tasks, 271
 DB2, 356
 Microsoft SQL Server, 413
 Oracle, 376
 SAP HANA, 448
Database management
 MaxDB, 437
Database Manager GUI, 437
Database Studio, 437
DB2, 360
 administration, 356
 backup, 367
 Command Line Processor, 357
 Common Server, 357
 Control Center, 356
 database configuration, 365
 DB2 command, 357
 db2set, 366
 Log Manager, 369
 Profile Registry, 366
 restore, 370
 SQL statement, 357
 start, 360
 stop, 361
 Universal Database, 357
DB6 → DB2
DBA action log, 340
DBA Cockpit, 329, 356, 373
DBA Planning Calendar, 293, 330
DDIC, 638
Deadlock, 47
Decimal Notation, 587
Default
 profile, 62
 value, 667
Defragmentation (memory), 550
Delete
 date, 485
 partner profile, 626
 spool file, 484
 transport files, 486
Development system, 731
Diagnostics agent, 201
Dialog
 box, 85
 instance, 32
 process, 538
Disaster recovery, 299, 307, 498
 check, 314
 communication, 312–313
 continuing business, 327
 dependent applications, 320
 downtime, 311
 emergency scenario, 315
 external provider, 318
 hardware failure, 316
 in-house recovery, 314
 location, 318
 manager, 313
 plan, 308–309
 process, 319
 remote recovery, 315
 requirement, 309
 restore time, 311
 risk of failure, 326
 role, 313
 script, 318
 start, 310
 status, 314
 team, 313
 test, 324
 type, 314

Distribution model
 ALE, 607
 delete, 627
Documentation, 27
Domain controller, 743
Download basket, 257, 781
Download Manager, 259, 782
Downtime, 35, 296, 311
dpmon, 539
Drive array, 305
Dump analysis, 824
DVM, 178, 240

E

EarlyWatch Alert → SAP EarlyWatch Alert
eCATT, 135, 814
Email, 98
 distribution list, 169
Emergency, 307
 scenario, 315
 user, 639
End-to-end analysis, 223
End-User Experience Monitoring, 212
Enhancement package, 759
EPS inbox, 796
Error
 message, 824
 program, 825
 user, 825
Error search
 Central User Administration, 620
Event scripting, 566
Exception, 228
 analysis, 228
Export history, 751
External auditor, 514

F

Fax, 98
File, 421
 group, 421
 system full alert, 163
Form
 approval procedure, 885
 authorization role change, 886

Form (Cont.)
 detailed list of SAP Notes, 888
 sample transport request, 887
 user request, 885
Frontend printer, 709
Full authorization, 639
Functional
 enhancement, 759
 separation, 513

G

Gateway, 97
Generate
 load, 811
 object, 811
GRC, 517

H

Hacker, 496
Hard disk, 302
Hard shutdown, 44
Hardware, 296
 performance, 552
 resource, 36
 throughput, 301
High availability, 304, 308, 499
Hit ratio, 548
Host agent, 201
Host name, 49
Host spool, 699, 705, 710
 transfer, 720
HotNews, 243
HTTP, 105, 108
HTTPS, 105, 109

I

ICF, 105
 activation, 373
ICM, 108, 373
 Monitor, 109
 restart, 111
 thread, 109

IDoc
 monitoring, 622
IGS, 775
Import
 condition, 817
 history, 750
 option, 746
 postprocessing, 127
 queue, 742
Incident
 accelerate processing, 846
 application component, 837
 attachment, 838
 close, 846
 draft, 841
 priority, 837
 service connection, 850
 status, 841
 Support Desk Evaluation, 846
Information broadcasting, 98
Infosystem authorization, 677
In-house recovery, 314
Initial password, 583
 generate, 583, 595
 parameters, 583
Initialization parameter, 392
In-memory technology, 449
Insider trading, 494
Instance, 32, 46
 cluster, 46
 creating definition, 47
 profile, 62
Interface, 88
Internet Communication Framework, 105
Internet Communication Manager → ICM
Internet Graphics Service, 775
Issue Management, 178

J

Job, 681
 active, 540
 class, 685
 creator, 682
 critical, 682
 log file, 484

Job (Cont.)
 monitoring, 691
 regular, 681
 Scheduling Monitor, 694
 step, 685
 wizard, 690

K

Kernel, 777
 authorization, 789
 backup, 785
 library, 788
 part, 778
 patch, 785
 patch level, 763
 release, 763
 replace, 788
 stopping the SAP system, 787
 unpack, 786
 update, 760, 784
KISS principle, 26

L

Landscape Management Database, 178, 180
Legacy System Migration Workbench, 135
License administration, 249
Lifecycle management, 178
LMDB, 178, 180
Load analysis, 543
Local Security Handling, 558, 573
Lock
 Central User Administration, 620
 data record, 78
 entry, 78
 global, 620
 local, 620
 monitoring, 270
 server, 32
 transaction, 505
 user, 596
Log client copy, 130
Log file, 288, 458
 archive, 369
 backup, 468

Logical system
 Central User Administration, 600
 client assignment, 601

M

MAI, 178, 206
Main memory, 548
Maintenance Optimizer, 251, 760, 780
Maintenance → System maintenance
Mass maintenance
 user, 592, 619
master database, 434
MaxDB → SAP MaxDB
MCC, 37, 43
Memory, 449
 defragmentation, 550
 extension, 478
 medium, 478
 operating system, 477
 paging, 552
 release, 482
 space, 179
Message server, 103
Metric monitor, 220
Metrics, 207
Microsoft SQL Server, 413
 agent, 418
 data backup, 424
 file, 420
 log, 422, 436
 maintenance plan, 428
 page, 421
 refreshing the statistics, 273
 server type, 415
 system database, 433
 transaction log, 422
Mini LSN, 423
Minimum Recovery Log Sequence Number, 423
Mode
 NOARCHIVELOG, 391
model database, 434
Modification adjustment, 802, 810
Monitor, 68, 137–138
 add, 156
 attribute, 138
 content, 209

Monitor (Cont.)
 copy, 154
 create, 154
 delete, 159
 hide, 149
 object, 138
 show, 152
 technical, 207
 transport, 161
 tree element, 138
Monitoring and Alerting Infrastructure, 178, 206
msdb database, 434
MTE, 138
 class, 172
Multiple logon, 500

N

Network
 function, 554
 printer, 703
 security, 495–496
Node maintenance, 99
Note Assistant, 861
Notification management, 239

O

Offline backup, 368, 402
Online
 backup, 369, 404
 documentation, 824
Operating system, 36
 administration, 477
 CCMS monitoring, 479
 daily tasks, 271
 file archiving, 478
 information, 486
 kernel update, 785
 log, 271, 487
 memory monitoring, 477
 memory usage, 477
 monitor, 486, 551
 register command, 175
 reorganization, 485

Operation mode, 46–47, 51
 calendar, 56
 manual switching, 60
 production, 52
 special, 52
 switching, 56
 test, 52
Oracle, 376
 autoextend, 399
 check database, 409
 database configuration, 392
 database parameter, 396
 Listener, 379, 386
 offline backup, 402
 online backup, 404
 reset database, 408
 restore, 406, 408
 start, 379–380
 stop, 384
OSS Note → SAP Note
Output
 control, 716, 824
 device, 699, 703
 request, 699, 714
Output management, 699
 output control, 716
 output data, 714
 spool consistency check, 724
 spool request, 717
 spool server, 699
 TemSe consistency check, 726

P

Page header, 421
Paging, 162
Password
 generate, 583, 595
 guideline, 501
 lock, 501
 minimum length, 501
 misuse, 500
 parameter, 501
 random number generator, 583, 595
 reset, 594, 619
 rule, 640
 security, 501

Password (Cont.)
 system administration, 638, 640
 system password, 503
 trivial, 502
Peak load, 538
Performance, 537
 analysis, 543, 552
 background job, 695
 backup, 301–302
 buffer, 270, 548
 CPU time, 546, 552
 database, 351, 551
 hard disk, 552
 hardware, 552
 main memory, 552
 network, 552
 operating system analysis, 551
 process, 540
 restore, 301, 304
 statistics, 270
 swapping, 539
 system monitor, 539
 task type, 545
 transaction profile, 546
 troubleshooting, 537
 Workload Overview, 545
Point-in-time recovery, 408
Principles of system administration, 25
Print, 699
 access method, 705, 710
 default Windows printer, 709
 device attribute, 704, 709
 frontend printer, 709
 local, 709
 location, 705
 network printer, 703
 operating system level, 703
 output attribute, 707
 output control, 716
 presetting, 715
 set up, 703
 spool server, 704
 test, 709, 712
 time, 716
 transport, 699, 712
 tray info, 707
 troubleshooting, 716
 type, 703, 709
 USB printer, 712

Process
 overview, 538
 terminate, 541
Product
 instance, 189
 system, 185
Production data, 135
Production system, 731
 prevent changes, 282, 508
Profile file, 62
Profile Generator, 645, 656
 upgrade tool, 671
Profile parameter, 61
 administrative data, 63
 basic maintenance, 63
 create, 63
 default value, 65
 DIR_AUDIT, 521
 displaying, 68
 dynamic, 68
 FN_AUDIT, 521
 login/disable_multi_gui_login, 500
 login/multi_login_users, 501
 login/no_automatic_user_sapstar, 505
 maintaining, 62
 rdisp/wp_no_spo, 700
 rsau/enable, 521
 rsau/max_diskspace/local, 521
 rsau/max_diskspace/per_day, 521
 rsau/max_diskspace/per_file, 521
 rsau/selection_slots, 521
 rsau/user_selection, 521
 stat/as_max_files, 534
 stat/max_files, 534
Program
 BRARCHIVE, 404
 BRCONNECT, 409
 BRRECOVER, 406
 BRRESTORE, 406
 BRSPACE, 390, 393
 buffer, 548, 550
 dpmon, 78, 539
 error, 825
 log, 271
 RSADRCK2, 610
 RSCCUSND, 613
 RTCTOOL, 239
 SAP_COLLECTOR_FOR_PERFMONITOR, 542

Program (Cont.)
 sapcpe, 789
 SAPlpd, 710
 saposcol, 486
Protocol
 SMTP, 109
PXA buffer, 548, 550

Q

Quality assurance
 advanced, 733
 prevent change, 508
Queue, 799
Quick link, 829

R

RAID, 303–304, 499
RAID-0 array, 303
RCA, 178, 223
Recipient list, 239
Recovery → Disaster recovery
Redo log, 288, 404
Regression test, 759, 814
Remote
 copy, 116, 120
 logon, 93
 recovery, 315
 service connection, 850
Remote Function Call, 88
Reorganization, 485
Replenishment lead time, 277
Report
 PFCG_TIME_DEPENDENCY, 655
 RSAUDITC_BCE, 507
 RSPO1043, 726
 RSTS0020, 726
 SAP_REORG_SPOOL, 724
Request for change, 729
Restore, 291, 299, 371, 408
 duration, 300
 strategy, 300
 testing, 301
 time, 311

Return code, 742, 748
RFC
 interface, 88
 system comparison, 134
RFC connection, 88, 180
 create, 603
 gateway, 97
 logon data, 90
 remote logon, 93
 test, 93, 606
 type, 90
RFC destination → RFC connection
Roadmap, 179
Role
 authorization role, 644
Rollforward, 371
Root cause analysis, 178, 223
Row offset, 421
Runtime error, 71

S

SAP Business Workplace, 103
SAP Central Process Scheduling, 691
SAP components
 SAP Basis layer, 19
SAP DB → SAP MaxDB
SAP Download Manager → Download Manager
SAP EarlyWatch Alert, 178, 236
 check, 272
 configure, 237
 display, 241
 report, 239
SAP enqueue server, 32
SAP ERP, 23, 32
SAP Gateway, 97
SAP Global Support, 831
SAP GUI, 553–554
 add systems, 574
 installation medium, 555
 installation package, 563, 567
 installation requirements, 553
 installation scenario, 554
 installation server, 558, 567
 SAProuter, 576

SAP HANA, 448
 backup, 467
 configuration, 456
 monitoring, 463
 performance, 454
 stop, 459
 system information, 456
 system landscape, 454
SAP Help Portal, 824
SAP IGS, 775
SAP Installation Server Administration Tool, 562
SAP kernel → Kernel
SAP Load Generator, 811
SAP Logon, 574
SAP Management Console, 37, 43
SAP MaxDB, 437
 backup, 444
 monitoring, 440
SAP Note, 759, 824, 827
 correction instructions, 859, 862
 documentation, 860
 download, 861
 implement, 243, 859, 861–862
 imported, 888
 processing status, 865
 release, 830
 reset implementation, 866
 search, 827
 status, 865
 support package, 830
 undo, 866
SAP Passport, 829
SAP Service Connector, 850, 855
SAP Service Marketplace, 826
SAP Solution Manager, 177
 configuration validation, 230
 configure manage systems, 197
 end-to-end analysis, 223
 function, 178
 maintain system landscape, 180
 Maintenance Optimizer, 251
 notification management, 239
 product system, 185
 root cause analysis, 178, 223
 SAP HANA support, 466
 service connection, 245

SAP Solution Manager (Cont.)
 setup, 183
 SLD, 178
 solution, 193
 system management, 206
 system monitoring, 178
 system recommendation, 243
 technical monitoring and alerting, 206
 test management, 814
 transfer system data, 180
 Work Mode Management, 209
SAP Support Portal, 249, 251, 485, 823, 826
 customer incident, 831
 logon, 827
 service connection, 850
 single sign-on, 829
 support package, 760
 user ID, 826
SAP system
 architecture, 46
 layer, 35
 starting, 35–36, 789
 stopping, 40, 42, 787
SAP system administration → System administration
SAP_ALL, 639
SAP*, 638
SAPCAR, 787
SAPconnect, 98, 174
SAPDBA, 278, 388
saplogon.ini, 578
SapLogonTree.xml, 578
saposcol, 542, 787
SAPOSS, 856
SAProuter, 576, 788, 850, 855
Scale-out solution, 449
SCN, 824
Script event, 566
Security, 493
 access, 495
 application, 495, 497
 audit, 514
 concept, 499
 data, 495, 498
 guidelines, 230
 level, 495
 network, 495–496

Security (Cont.)
 operational, 495, 497, 513
 physical, 495
 SAP Note, 517
 share user ID, 635
Security administration, 493–494
 audit, 514
 concept, 499
 legal provision, 494
 password, 501
 report, 517
 system, 499
 transaction, 505
Security Audit Log, 519, 533
 analysis, 532
 check, 272
 configuration, 521
 data protection, 533
 deleting a file, 534
 directory, 520
 dynamic, 522
 file, 520
 filter, 522
 profile, 523
 profile parameter, 521
 static, 522
Segregation of duties, 497, 513
Send job, 100
Server, 36
 destruction, 317
 loss, 317
 room, 496
 status, 104
Service, 105
 definition, 239
 preparation check, 239
Service connection, 850
 close, 858
 connection type, 852
 costs, 850
 overview, 249
 routestring, 854
 SAP Solution Manager, 245
 set up, 851
 status, 857
Service Data Control Center, 237
Service Level Agreement, 309

Service level reporting, 178
Service Marketplace, 826
Shell, 787
Short dump, 71, 270
 SPAM/SAINT *update*, 793
Shutdown type, 44, 460
SIGINT, 44
Single point of failure, 30, 326
Single profile, 662
Sizing, 537
SLA, 309
SLD, 178, 180
SMS message, 99
SMTP, 98, 103, 105
Snapshot, 370
Soft shutdown, 44
Software, 296
Software Update Manager, 255, 784
Solid state disk, 449
Solution, 192
Solution Directory, 195
Solution Manager → SAP Solution Manager
Solution tool plug-in, 206
SPAM/SAINT, 760
 update, 790
 version, 760, 779, 790
SPAU adjustment, 811
SPDD adjustment, 811
Special operation mode, 52
Spool consistency check, 724
Spool control → output management
Spool request, 699
 clean up, 724
 create, 714
 delete, 724
 file, 724
 minimum retention period, 724
 presetting, 715
 property, 714
 reorganize, 724
 request attributes, 718
 server, 724
 status, 717
Spool server, 699
 alternative server, 699, 702
 assign printer, 704
 load balancing, 702
 logical, 699

Spool server (Cont.)
 real, 699
 server class, 702
 set up, 699
 transport, 714
Spool system, 699
Spool work process, 699–700
SQL script, 386
SQL Server Integration Services, 432
SQL Server Management Studio, 414
SQL Server → Microsoft SQL Server
SQL statement, 357, 362
SQL Studio, 437
SQL*Plus, 376, 386
ST-A/PI, 239
Standard job, 485
Start
 log, 39
 profile, 62
 timeout, 38
startdb, 381
startsap, 37
Step, 685
stfk.oez, 855
stopsap, 43
Storage
 automatic management, 366
Stored procedure, 450
SUM, 255, 784
Support, 823
Support package, 251, 759
 component information, 762
 confirm queue, 809
 delete file, 485
 determine current level, 761
 download, 760, 766, 781
 download basket, 772
 downtime-minimized, 808
 EPS inbox, 796
 find, 766
 import, 794, 799, 807
 kernel, 777, 784
 level, 251, 761
 load from application server, 796
 load from front end, 791, 795
 log, 807
 modification adjustment, 802, 810

Support package (Cont.)
 naming convention, 763
 queue, 799
 regenerate object, 811
 regression test, 814
 SAP Download Manager, 782
 SAP Load Generator, 811
 sequence, 783
 SPAM/SAINT version, 760, 779, 790
 SPDD adjustment, 811
 stack, 251, 759
 store on server, 794
 temporary directory, 795
 test, 804, 814
 unpack, 795
Support Package Manager, 794
Swapping, 162, 270, 539, 548
SysLog, 69
System
 add, 574
 availability, 309
 changeability, 508
 check status, 264
 copy, 132
 data, 180
 database, 433
 failure, 307
 load, 539
 log, 40, 59, 69, 228, 269, 824
 maintenance, 251
 managed, 180, 197
 message, 41, 85
 monitoring, 137, 207, 213, 539
 overload, 538
 prevent changes, 282
 profile, 61
 protection, 25
 recommendation, 178, 243
 recovery, 307
 risk of failure, 326
 SAP ERP, 32
 setting, 36
 status, 141, 761
 stop, 41
System administration, 35, 638
 application server, 76
 DDIC, 638
 lock, 78

System administration (Cont.)
 monitoring, 137
 password, 638, 640
 SAP Management Console, 37, 43
 *SAP**, 638
 security, 499
 transaction, 68
 work process, 76
System administrator, 23
System landscape
 administration, 178
 maintain, 180
System Landscape Directory, 178, 180
System maintenance, 759
 certificate, 249
 concept, 760
 error correction, 759
 execute, 783
 procedure, 783
 strategy, 760
 transaction, 252
System management
 SAP Solution Manager, 206
System recommendation, 243
System trace
 authorization trace, 672

T

Table
 authorization management, 882
 background processing, 883
 Change and Transport Management, 884
 database administration, 882
 database table, 881
 diagnostics and troubleshooting, 884
 operating system administration, 882
 output management, 884
 performance, 882
 PRGN_CUST, 610
 SAP Solution Manager, 881
 security administration, 882
 system administration, 881
 system maintenance, 884
 system monitoring, 881
 transparent, 881
 TSP01, 724

Table (Cont.)
 TSP02, 724
 TSP02F, 724
 TSP0E, 724
 TST01, 724, 726
 TST03, 724, 726
 TSTCT, 505
 user administration, 882
 USR40, 502
Table maintenance, 752
 Customizing activity, 753
 maintenance dialog, 753
 maintenance view, 752
 transport, 756
Tablespace, 354
Tape drive, 302
Target
 client, 116
 system, 732
Task
 annual, 279
 critical, 264, 268
 daily, 267
 database, 271–272, 278, 281
 execution frequency, 263
 monthly, 274
 operating system, 271, 273, 278–279, 281
 quarterly, 277
 release, 738
 SAP system, 268, 272, 277, 279
 scheduled, 263
 weekly, 272
TCP/IP, 97
Technical monitoring, 207
tempdb database, 434
TemSe, 699, 714
 consistency check, 272, 726
 database, 726
 object, 724, 726
Test
 data, 135
 management, 179
 script, 322
Thread, 109
Three-system landscape, 732
Threshold value, 138
Throughput, 301
Time differences, 302

TMS, 732
tp, 733, 746
Trace, 458
 authorization trace, 672
 delete file, 482
Transaction
 AL08, 41, 81, 265, 270, 637
 authorization management, 873
 background processing, 873
 backup and restore, 871
 BD54, 600
 BD87, 622
 Change and Transport Management, 874
 critical, 505
 database administration, 871
 DB02, 271–272, 274–275, 346, 551
 DB12, 268, 293, 340
 DB13, 268, 278, 293, 330, 335, 338
 DB14, 343
 DBACOCKPIT, 329, 356, 373
 diagnostics and troubleshooting, 874
 LMDB, 183
 lock, 505, 507
 LSMW, 135
 operating system administration, 871
 OS06, 265, 271, 551
 OS07N, 488
 output management, 874
 performance, 872
 PFCG, 280, 645, 656
 PFUD, 655
 RZ01, 265, 694
 RZ03, 60
 RZ04, 48, 51, 54
 RZ10, 62, 278, 500, 522
 RZ11, 68
 RZ20, 137, 139, 149, 154, 156, 160, 170, 266, 269, 273–274, 479
 RZ21, 138, 165
 RZ70, 181
 SA38, 280, 609
 SAINT, 790, 815
 SAP Solution Manager, 870
 SBWP, 103, 169
 SCC1, 120
 SCC3, 120, 130
 SCC4, 112, 129, 282, 510, 601
 SCC5, 128–129
 SCC7, 127

Transaction (Cont.)

SCC8, 123
SCC9, 121, 134
SCCL, 116
SCOT, 99, 174
SCUA, 607, 624
SCUG, 611
SCUL, 270, 620
SCUM, 615
SDCCN, 237
SE01, 733
SE03, 280, 282, 508, 510, 734
SE06, 510
SE09, 733
SE10, 733, 738
SE16, 881
SE38, 280
SECR, 518
security administration, 872
security-relevant, 875
SGEN, 811–812
SICF, 105
SICF_INST, 373
SIGS, 775
SM_WORKCENTER, 180, 193, 198, 213, 224, 231, 241, 243, 249
SM01, 280, 282, 506
SM02, 41, 86
SM04, 41, 81, 265, 270, 539, 636–637, 799
SM12, 79, 266, 270
SM13, 81–82, 266, 269, 824
SM14, 85, 824
SM18, 534
SM19, 522
SM20, 272, 532
SM21, 40, 59, 69, 71, 266, 269, 824
SM30, 278, 503, 752–753
SM31, 752
SM35, 266, 270
SM36, 485, 684
SM37, 41, 81, 120, 265, 269, 278, 485, 540, 799, 813
SM50, 41, 61, 76–77, 81, 266, 269, 483, 538
SM51, 41, 76, 266, 269
SM59, 88, 603
SM63, 56
SM66, 77, 81

Transaction (Cont.)

SM69, 175
SMGW, 41, 97
SMICM, 109
SMMS, 103
SMSY, 180
SMT1, 200
SMT2, 200
SNOTE, 859, 861
SOLMAN_CONNECT, 245
SOLMAN_SETUP, 183, 206–207, 237
SOLMAN_WORKCENTER, 180, 193, 198, 213, 224, 231, 241, 243, 249
SP01, 266, 270, 272, 274, 716–717, 824
SP12, 272, 274, 726
SPAD, 700, 703, 712, 725
SPAM, 764, 790, 794, 796, 799, 814
SPAU, 811
SPDD, 811
ST01, 672
ST02, 266, 270, 548
ST03, 267, 270
ST03N, 543
ST04, 267, 271, 351–352, 551
ST06, 487, 539
ST11, 541
ST22, 72, 267, 270, 824
STAD, 533
STMS, 267, 270, 743
SU01, 277, 282, 582, 591, 596, 613, 661, 666
SU02, 280, 663
SU03, 280, 282
SU10, 592, 619
SU24, 667
SU25, 671
SU53, 675
SUCOMP, 586
SUGR, 633
SUIM, 677
system administration, 869
system maintenance, 874
system monitoring, 870
user administration, 872
WE20, 626
Transaction log, 288
virtual log file, 422
Transport, 732
approve, 887

Transport (Cont.)

file, 740
history, 750
management, 179, 729
printer, 712
queue, 126
spool server, 714
Transport directory
check, 486
Transport Management System, 732
Transport request, 729
create, 733, 737
Customizing request, 735
enter a change, 736
export, 740
import, 742
log, 748
release, 738
request type, 735
return code, 742, 748
task, 736, 738
workbench request, 735
Transport system, 729
Change and Transport Organizer (CTO), 732
Correction and Transport System, 732
create a transport request, 737
export a transport request, 740
log, 748
monitoring, 270
return code, 742, 748
task, 738
tp, 733, 746
Transport Management System (TMS), 732
Troubleshooting, 178, 823
analyze the problem, 824
documentation, 825
gather data, 824
Trusted system, 200

U

Unconditional mode, 746
Uninterrupted power supply (UPS), 271, 499
Unlock
Central User Administration, 620
reset password, 594
user, 596

Update, 81

administration, 85
asynchronous, 82
cancellation, 81
module, 84
performance, 811
record, 85
system, 824
terminated update records, 269

Upgrade, 179

UPS, 499

User

active, 635
add, 580
assigned role, 654, 661
authorization profile, 666
change, 580, 592
copy, 582
create, 591, 617
DDIC, 504
delete, 282
group, 632
ID, 635
incorrect logon, 501
initial password, 595
lock, 596, 620
maintain, 591, 619
mass maintenance, 592, 619
profile comparison, 661
reset password, 594
SAP*, 504
session, 635
setup, 582
synchronize, 609
template, 582
unlock, 596, 620
validity date, 581

User administration, 579

audit, 516
central, 597
ID naming convention, 580
leaving employees, 581
mass maintenance, 592
policy and procedure, 579
validity date, 581

User comparison, 654

PFCG_TIME_DEPENDENCY, 655
Transaction PFUD, 655

User error, 825
User group, 632
 create, 633
 create automatically, 610
User ID, 682
 delete, 516
 lock, 516
 multiple usage, 500
 system administrator, 503
User logoff
 automatic, 267
User logon
 multiple, 500

V

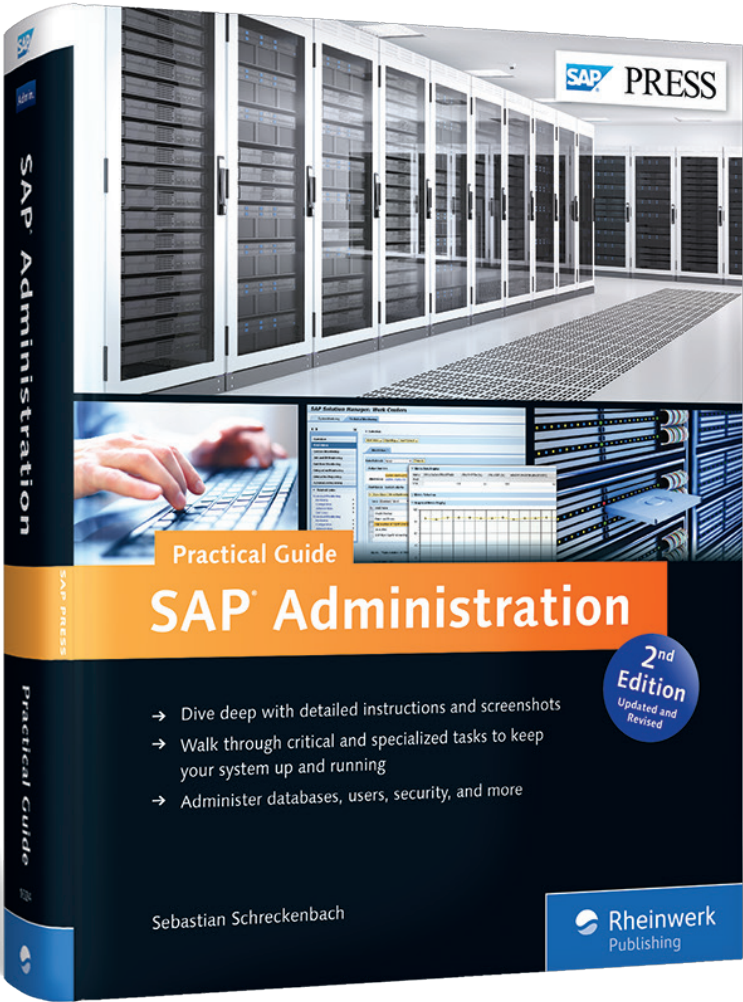
Variant, 683
Verification script, 322
Version differences, 19
Virtual log file, 422
Visual Administrator, 182
VPN, 496

W

Web User Interface, 179
Work center, 180
Work Mode Management, 209
Work process, 46, 76
 batch, 681
 distribution, 54
 dynamic, 47
 minimum number, 55
 runtime, 538
 trace, 789
 type, 46
Write lock, 724
Write performance, 305

X

xSearch, 828



Sebastian Schreckenbach works as a senior consultant in SAP Basis administration at Steria Mummert Consulting AG in Leipzig, Germany. Prior to this, he worked as an SAP Basis administrator for many years in the SAP Competence Center in Dresden, Germany.

Sebastian Schreckenbach
SAP Administration—Practical Guide

912 Pages, 2015, \$79.95/€79.95
ISBN 978-1-4932-1024-4

 www.sap-press.com/3639

We hope you have enjoyed this reading sample. You may recommend or pass it on to others, but only in its entirety, including all pages. This reading sample and all its parts are protected by copyright law. All usage and exploitation rights are reserved by the author and the publisher.

© 2015 by Rheinwerk Publishing, Inc. This reading sample may be distributed free of charge. In no way must the file be altered, or individual pages be removed. The use for any commercial purpose other than promoting the book is strictly prohibited.