



Spectrum Protect (SP) Best Practice Guide



Version 1.05

Dr. Alexander Dunaevskiy, Stephan Peinkofer

© 2013, 2016, 2019 Leibniz Computing Center of the Bavarian Academy of Sciences and Humanities

1	Introduction.....	5
1.1	<i>Most important changes compared to the previous version 1.03.....</i>	5
1.2	<i>Your opinion is important to u.....</i>	5
1.3	<i>SP-Terms of use of LRZ.....</i>	5
1.4	<i>Purpose of these instructions.....</i>	5
1.5	<i>Important rules of conduct.....</i>	6
1.5	<i>SP-Supportmatrix</i>	6
2	Basic concepts and procedures of SP	7
2.1	<i>Definitions of terms</i>	7
2.1.1	Backup.....	7
2.1.2	Restore.....	7
2.1.3	Archive	7
2.1.4	Retrieve	7
2.1.5	Difference between backup and archives.....	7
2.1.6	Node	7
2.1.7	Filespace.....	8
2.2	<i>Backup with SP.....</i>	9
2.2.1	Backup strategies at a glance	9
2.2.1.1	Full Backup.....	9
2.2.1.2	Differential Backup	10
2.2.1.3	Incremental Backup	11
2.2.2	Backup software operation	11
2.2.3	The backup procedure of SP	12
2.2.4	The version management of SP	12
2.2.5	Regular automatic backups with SP.....	16
2.3	<i>Comparison: Archiving and Backup at SP.....</i>	16
3	SP configuration planning	17
3.1	<i>Basic considerations</i>	17
3.1.1	Backup or archive or both?	17
3.1.2	What should be secured?.....	17
3.1.3	How much data can be backed up or archived?.....	17
3.1.4	How often should you back up?	18
3.1.5	Who is allowed to backup and restore?	18
3.1.6	How confidential is my data?	18
3.2	<i>Basic configuration guidelines</i>	19
3.2.1	Location of the program files.....	19
3.2.2	Location of the configuration files.....	19
3.3	<i>Planning the system backup</i>	20
3.4	<i>Planning of the backup time window</i>	20
3.5	<i>Planning file archiving.....</i>	20
3.5.1	Division into several filesystems.....	20
3.5.2	Division into several nodes	21
3.5.3	Long-term archiving.....	21

3.5.4	Set character encoding	21
3.6	<i>Planning an operating system change/update</i>	21
4	Installing/updating/uninstalling the SP client	22
4.1	<i>Installation</i>	22
4.2	<i>Updates</i>	24
4.2.1	Why updates?	24
4.2.2	Planning and implementation of the update.....	25
4.3	<i>Uninstalling the SP Client</i>	26
5	Configuration and examples	27
5.1	<i>Archive and backup</i>	27
5.1.1	Configuration under Linux and Mac OS	27
5.1.1.1	Creating the <code>dsm.sys</code> configuration file	27
5.1.1.2	Creating the <code>dsm.opt</code> configuration file	28
5.1.1.3	<i>Include/Exclude</i> Configuration	28
5.1.1.4	Changing the initial password	29
5.1.1.5	Starting the SP Scheduler	29
5.1.1.6	Starting the SP Scheduler under Mac OS	29
5.1.2	Configuration under Windows.....	30
5.1.2.1	Initial configuration of the SP client.....	30
5.1.2.2	Advanced configuration.....	36
5.1.2.3	Configuration of the SP scheduler	36
5.2	<i>Splitting of data into multiple nodes Archive & Backup</i>	40
5.2.1	Splitting into multiple nodes under Linux, Unix and Mac	41
5.2.2	Splitting into multiple filesystems on Linux, Unix and Mac.....	41
5.2.3	Splitting the data into several nodes under Windows.....	42
6	Test the configuration	42
6.1	<i>Evaluating the preview function</i>	42
6.2	<i>Testing the backup function</i>	42
6.3	<i>Testing the Archive Function</i>	43
6.4	<i>Checking the scheduler log file</i>	43
7	Retrieve archive data	43
8	Tasks of a SP supervisor	44
9	What to do when something does not work	44
10	General tips	45
10.1	<i>How to upgrade my Linux SP client to a newer version?</i>	45
10.2	<i>I want to access the backed up data of a Linux server from my Windows notebook</i> 45	

10.3	<i>I want to replace a Linux machine and want to access the data of another Linux machine I manage from the command line. How can I do this?.....</i>	45
10.4	<i>On Scientific Linux, your instructions for setting up the SP scheduler do not work. How can I get the scheduler to work?</i>	46
10.5	<i>SP Client and NAS Backup on Windows 7, 8 and 10.....</i>	47
10.6	<i>How can you use a non "Default Management Class", E.g. B10V or B7V7D?.....</i>	49
10.7	<i>Encryption</i>	50
10.8	<i>Restore of data to a specific point in time</i>	52
10.9	<i>My computer has broken (been stolen). What is the best way to restore the backed up data to a new computer?</i>	52
10.10	<i>Related links.....</i>	53

1 Introduction

1.1 Most important changes compared to the previous version 1.03

TSM (= Tivoli Storage Manager) has been renamed to ISP (= IBM Spectrum Protect) or simply SP (= Spectrum Protect) as of version 7.1.3. This renaming is due to marketing considerations by IBM and not a fundamental change in the functionality of the software. In some examples with older versions TSM is used otherwise SP.

Security layer of SP server and client was completely redesigned in parallel in 8.X (from 8.1.2) and 7.X (from 7.1.8) version. This has a significant impact on the compatibility of the outdated TSM/SP clients with the new server versions, especially on the communication between server and client and on the security provided by the non-administrative users.

1.2 Your opinion is important to us

If you have any questions, suggestions, criticism, proposals for improvement or other requests regarding this *Best Practice Guide*, we would be very pleased if you could send us your feedback via the [ServiceDesk](#) *Service: Datenhaltung – Archiv und Backup* with the subject *BPG Feedback*.

1.3 SP-Terms of use of LRZ

The current [terms of use](#) of the LRZ archive and backup system must be observed.

1.4 Purpose of these instructions

As with many large IT applications, many paths lead to the goal with SP (= *IBM Spectrum Protect*). This guide is intended to show you how best to configure and perform backup and archiving SP. Our recommendations are based on the LRZ's many years of experience with SP and correspond to how the LRZ itself manages the backup and archiving of its data. You can benefit in many ways by following the LRZ recommendations:

- You avoid the most common configuration and operation errors of the SP Client from the very beginning.
- If problems do occur, the LRZ can usually help you more quickly, since checking the configuration is easier.
- If LRZ staff cannot solve a problem themselves and their configuration is supported, the problem can be passed on to Tivoli software support.
- You save yourself and the LRZ unnecessary work and problems.
- You increase the safety of your data.

The LRZ is aware that your IT structure and requirements are not always compatible with our recommendations. In this case, you should in any case consult with the LRZ so that we can find a solution for you together. In the event of gross deviations from our recommendations that have not been agreed with the LRZ, your configuration may not be supported by IBM/Tivoli. In this case, even the LRZ may not be able to help you. In the worst case, this can mean data loss for you.

This manual describes the most important features and functions for Windows and Unix operating systems, where Linux and other Unix-like, POSIX following operating systems have many similarities. The explanations refer to SuSE Linux, if nothing else is stated.

1.5 Important rules of conduct

Do's

- Please note the [terms of use](#) of the LRZ.
- Test the SP configuration (see chapter 6) regularly.
- Notify the LRZ of any significant changes to the planned data volume (i.e. storage space requirements) and number of files using the [ServiceDesk Service: Datenhaltung – Archiv und Backup](#).
- And also notify the LRZ of organizational changes (contact persons, etc.) using the [ServiceDesk Service: Datenhaltung – Archiv und Backup](#).

Don'ts

- Do not define more than 100 filespaces (see Section 2.1.7).
- Do not store more than 10 million files in a node.
- Do not store more than 20 terabytes in one node.
- Do not start many hundreds of restores individually.

1.5 SP-Supportmatrix

See our [SP support matrix](#) to find the SP client version recommended for your operating system.

Note: The LRZ can only provide assistance as long as you are using an IBM supported system configuration. This includes the use of a supported client version in conjunction with compliance with the hardware and software requirements. If there are valid reasons for you to use an unsupported system configuration (e.g., because a supported client for the operating system is no longer available), please contact please contact the LRZ (see chapter 8). Since the redesign of the security layer of SP (server version 8.1.2 and higher) our possibilities to help you with an unsupported system configuration are significantly limited.

2 Basic concepts and procedures of SP

SP is based on a client-server architecture. The LRZ hosts the servers. You use a client to back up and/or archive your data. The server stores your data partly on hard disks and partly on tape cartridges. Tape drives have significant advantages over hard drives in terms of energy consumption. Greater capacity at lower cost are further advantages.

2.1 Definitions of terms

2.1.1 Backup

Regular copying of files to a dedicated storage system (backup system) to protect against data loss in the event of a hardware, system or operator failure on the primary or source system (e.g. server, workstation, etc.).

2.1.2 Restore

Copy back the backed up version of files from the backup system to the primary or source system. Restore is the counterpart of Backup.

2.1.3 Archive

Copying selected files to a dedicated storage system (archive system) to keep them safe for a longer period of time. The original files can be deleted from the primary or source system after archiving to provide free storage space.

2.1.4 Retrieve

Copying archived files back to the primary or source system. Retrieve is the counterpart to archiving.

2.1.5 Difference between backup and archives

The basic difference between backup and archive is the versioning:

- Backup uses versioning.
- Archive does not use versioning.

This means that if you make two backups of a file with the same name and the same path, in the case of archives they become two independent objects, and in the case of backup they become two versions of one object. The retention rules for archives and backup are therefore structured differently and lead to the typical application patterns for the respective backup procedure:

- **Backup:** Data is stored for a short time (usually in several versions) on another medium for security purposes. Backup data is restored in the event of data loss, for example.
- **Archiving:** Data is to be stored securely for the long term. Normally, archived data will be accessed again.

2.1.6 Node

A node represents an administrative unit of SP. As a rule, a node corresponds to exactly one computer system that is to be backed up or archived from. However, multiple computer systems can also share a node if all computer systems use compatible operating systems with the same character encoding.

A computer system can also use multiple nodes. Regardless of whether the archive or backup is used, from a data volume of 20TB or file count of 10 million files, the data must be distributed across multiple nodes.

2.1.7 Filespace

A filespace is a subordinate management unit of a node. Groups of files are grouped together here. These groups are defined as follows:

- **Windows:** All files that are located together on a partition belong to a filespace. The filespace is distinguished on the basis of the so-called *Universal Naming Convention* for fixed media and on the basis of the disk/volume name for removable media.
- **Linux:** All files that are located together on a file system normally belong to one filespace. In addition, it is possible to organize a file system into several filespace by specifying so-called *virtual mount points*.

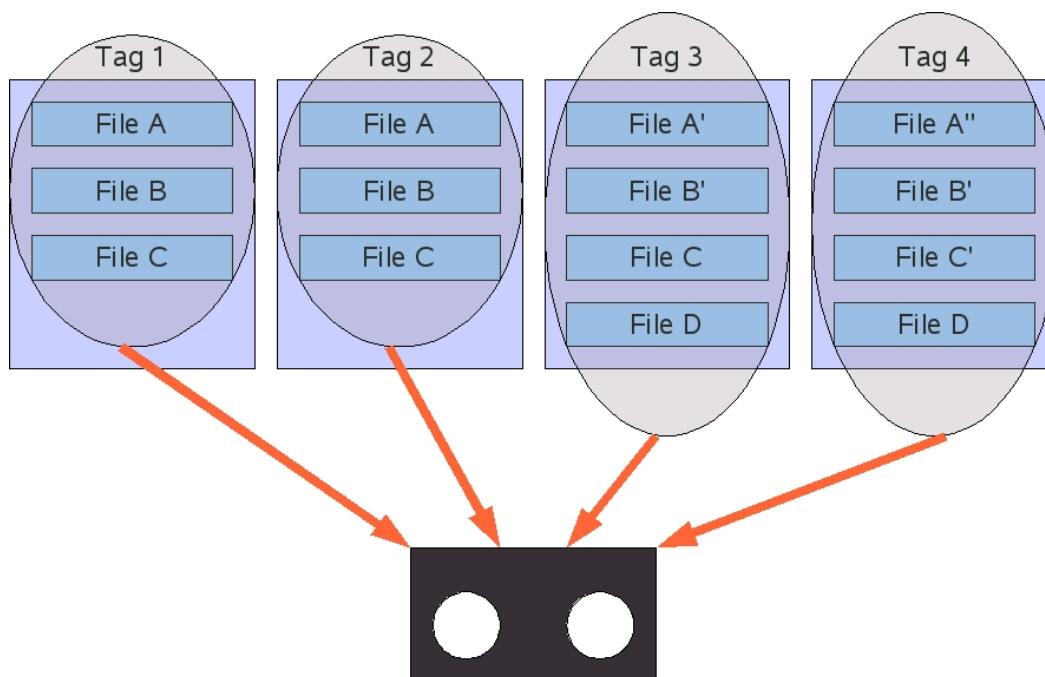
2.2 Backup with SP

2.2.1 Backup strategies at a glance

The following are the three basic strategies for backup.

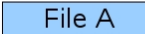
2.2.1.1 Full Backup

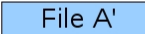
With a full backup, all files (except files in an *exclude* list) are always backed up during each backup operation. This has the advantage that in case of data loss, only the last backup has to be restored. The disadvantage of this strategy is that all files must always be transferred and saved, even if they have not changed since the last backup operation and are therefore already available in the most current version on the backup system. This results in long backup times, high storage space consumption due to redundancies and a high network load.



Legende


Menge der zu
sichernden Dateien

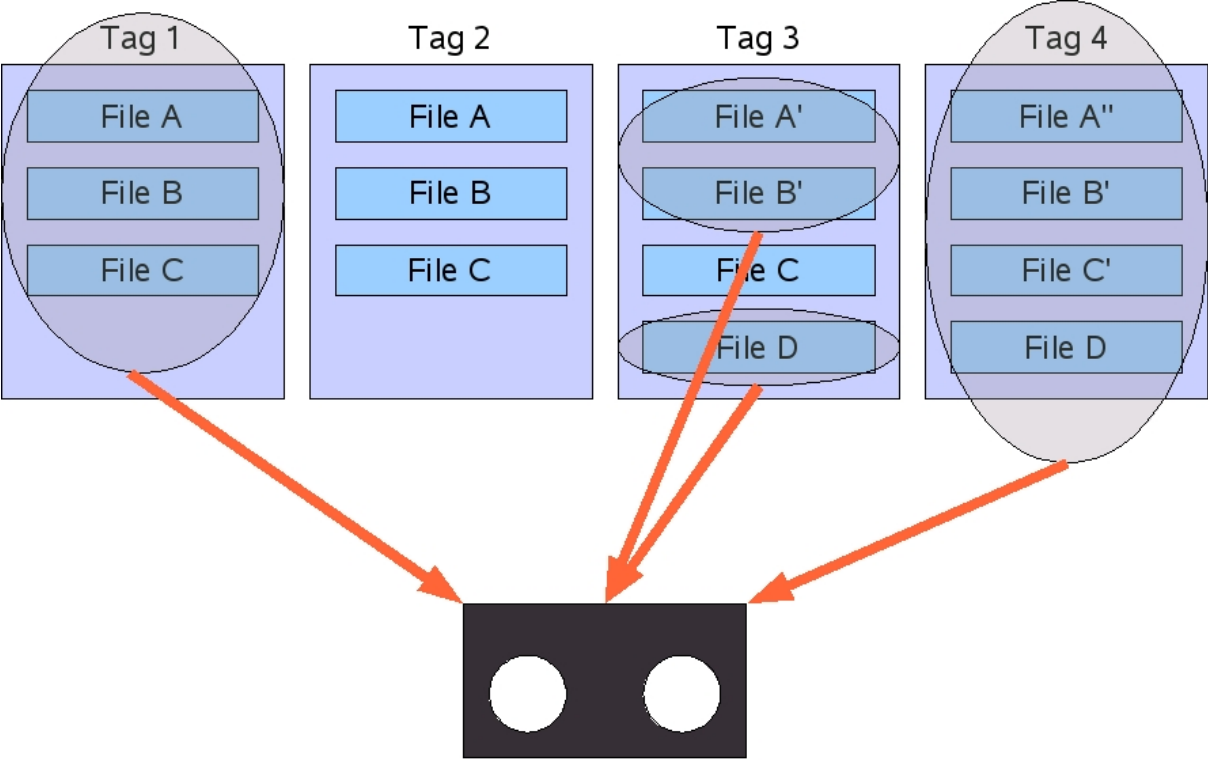

Datei A
Version 1


Datei A
Version 2


Datei A
Version 3

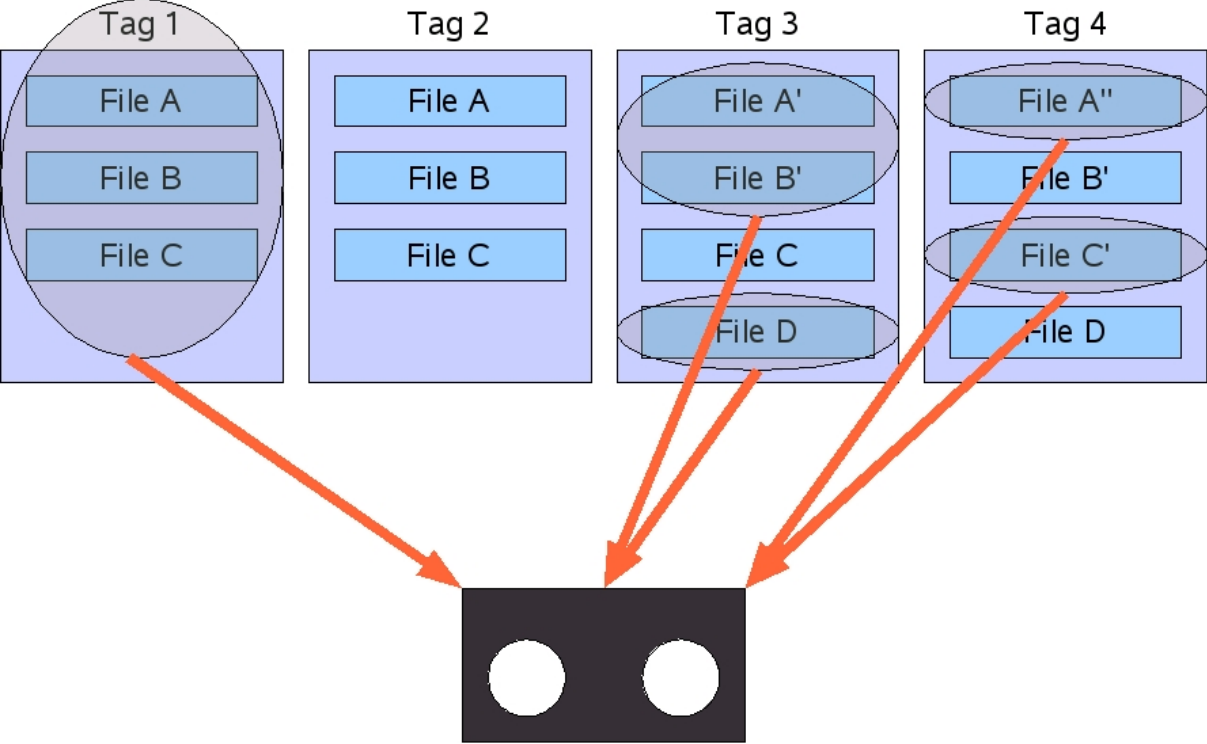
2.2.1.2 Differential Backup

With differential backup, only the files that have been changed or newly created since the last full backup are backed up during each backup operation. The advantage of this strategy is that not all files have to be transferred and saved each time. In the event of data loss, the last full backup is restored, followed by the last differential backup. Considering the required backup time and the storage space consumption, this method is not yet optimal, because a file that has been changed once is transferred and saved again and again with each differential backup until the next full backup is made.



2.2.1.3 Incremental Backup

With incremental backup, each backup operation backs up only those files that have been modified or newly created since the last backup operation (whether full or incremental). The advantage of this strategy is that it is optimal in terms of backup time and storage space consumption. The disadvantage of this strategy is the longer duration of a restore, since all incremental backups must be restored in the order in which they were created.



The following is a summary of the advantages and disadvantages of the three backup methods:

	Storage space used	Net load	Backup time	Restore time
Full backup	-	-	-	+
Differential backup	o	o	o	o
Incremental backup	+	+	+	-

2.2.2 Backup software operation

In principle, every backup application works according to a strategy or a combination of strategies, as shown in the previous section. Operational backup systems usually use a combination of full and differential or full and incremental backup.

The restore procedure of differential and incremental backups is very time-consuming, since several backups have to be restored one after the other. To solve this problem, more sophisticated backup applications use a database in which they store, among other things, where a particular version of a file is located (i.e. on which magnetic tape and at which position on the tape).

This means that the backup application does not have to go through the entire restore cycle, but can directly access the desired version of the file. This approach, of course, saves an enormous amount of time.

2.2.3 The backup procedure of SP

As mentioned above, many backup applications work according to the *Full & Differential* or *Full & Incremental* strategy. Not so SP: SP performs only incremental backups. This means that SP performs a full backup only once, during the first backup run. In all subsequent backup runs, only the change from the previous backup run is backed up. This backup method is also called progressive or *incremental forever*. To prevent excessive fragmentation of the data in the backup system, SP provides various mechanisms that ensure that the data of a node is distributed over as few tapes as possible.

2.2.4 The version management of SP

SP's incremental backup also saves all new versions of changed files. For cost reasons, these different versions of the same file are generally not kept forever, but only for a certain period of time; after all, in the event of data loss, one usually only wants to retrieve the most recent version of a file. Of course, it can happen that e.g. a file has been overwritten by mistake and that this is only noticed after a few days, although it is unlikely that such a thing is noticed only after a longer period of time.

Unlike some other backup applications, SP not only lets you set how long a particular version of a file should be kept, but also how many versions of a file are kept in the first place. In addition, SP treats files deleted on the source computer differently than files still present on the source computer when it comes to versioning.

Before we look in more detail at how SP versioning works, there are two SP-specific terms that need to be clarified, those of the active and the inactive version of a file:

- In SP, the most recent version of a file that still exists on the source machine is called the *active version*.
- All old versions of a file and also the most recent version of a file that has been deleted on the source computer are called *inactive versions*.

The behavior of the SP versioning is controlled by the following four parameters:

- `Versions Data Exists` specifies how many versions of a file still present on the source computer are stored.
- `Versions Data Deleted` specifies how many versions of a file deleted on the source machine are stored. This parameter is always less than or equal to the value of `Versions Data Exists`.
- `Retain Extra Versions` specifies how long an inactive version of a file is stored on the backup system before it is deleted. This parameter does not apply to the last inactive version of a file remaining on the backup system.
- `Retain Only Version` specifies how long the last inactive version of a file remaining on the backup system is stored before it is permanently deleted.

2. Basic concepts and procedures of SP

Notes:

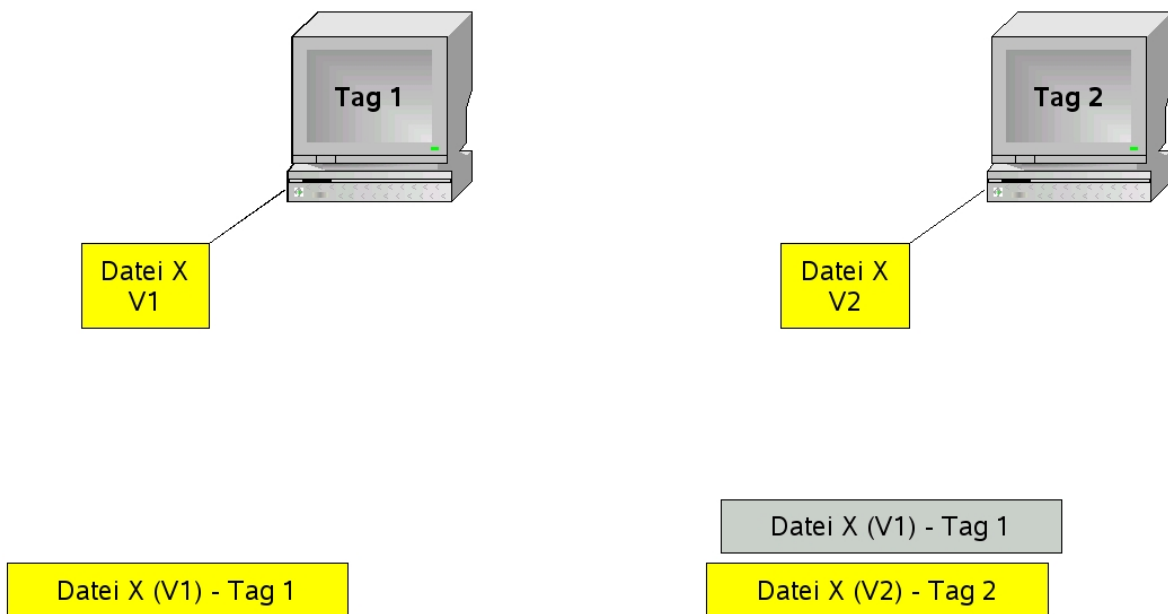
- The active version of a file is never deleted from the backup system.
- The above parameters cannot be changed by the user, but are predefined by the LRZ.

The following example will help to better illustrate how the parameters work. Let us assume that a user saves file X once a day. The following (fictitious) settings are given:

```
Versions Data Exists      =    3
Versions Data Deleted    =    2
Retain Extra Versions    =    5
Retain Only Versions     =    7
```

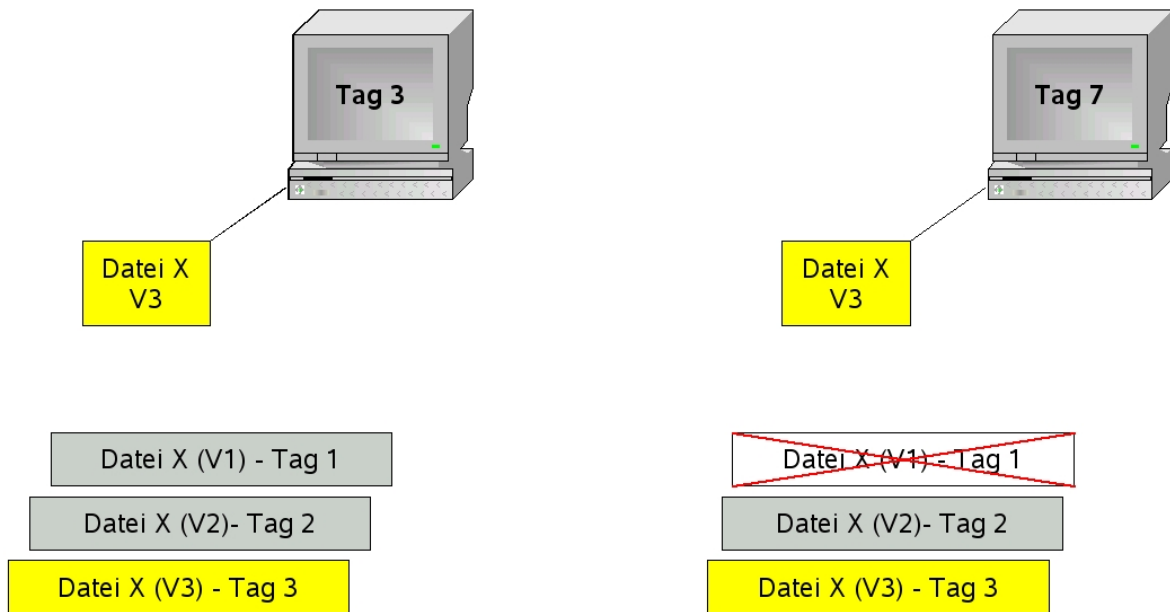
You can find out the actual values of your system with the following command:

```
dsmc query mgmt -detail
```



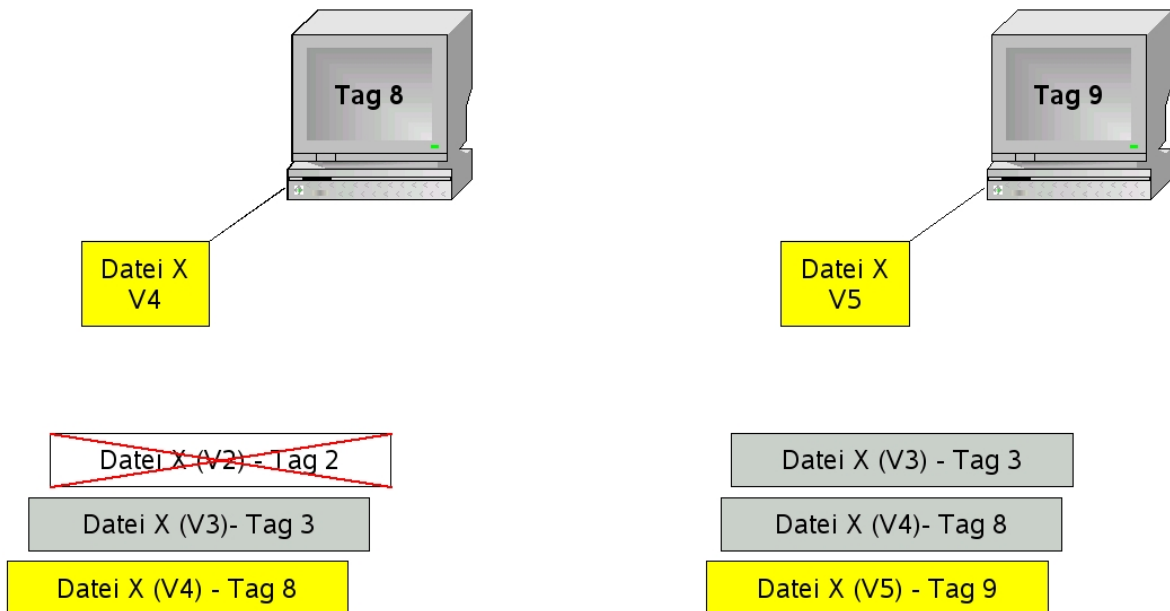
1. Tag: A copy of file X is created in the backup system as an active copy in version V1.
2. Tag: Changing the file X creates a new copy of the file in the backup system, setting the old version V1 to inactive and the new version V2 to active.

2. Basic concepts and procedures of SP



3. Tag: Further modification of file X creates another copy of the file in the backup system, setting the previous, active version V2 to inactive and the new version V3 to active.

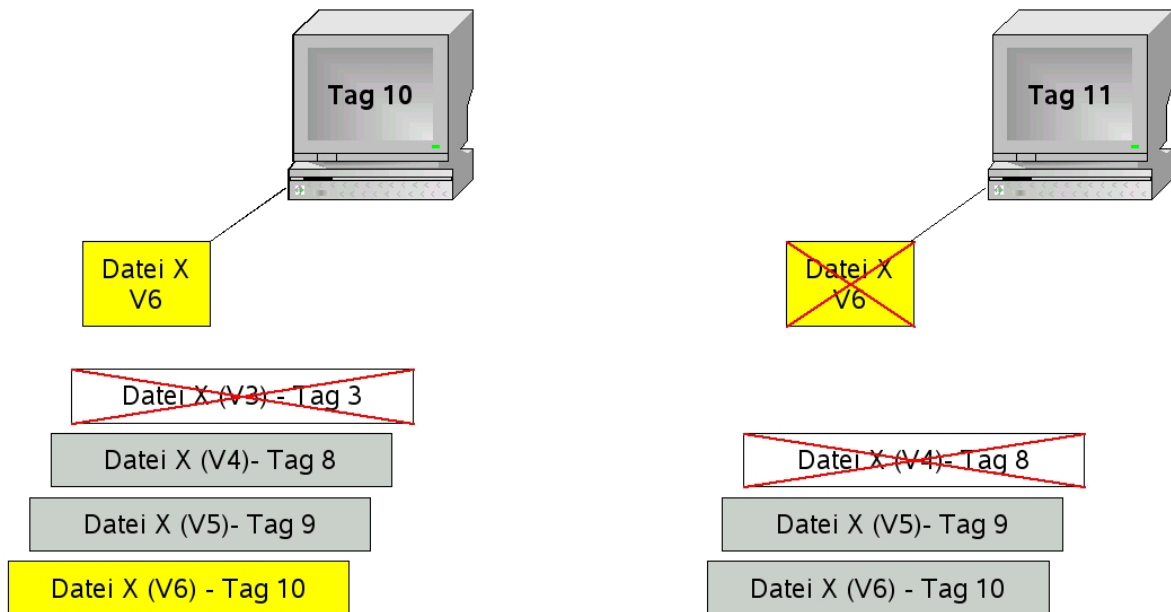
7. Tag: Since version V1 of file X has already been in the inactive state for 5 days (Tag 2 bis Tag 6) it will be deleted due to the set `Retain Extra Versions` (inactive files are kept for 5 days) parameter.



8. Tag: File X is changed again (V3 is set inactive, V4 active). Since version V2 of file X was already in the inactive state for 5 days (day 3 to day 7), it is deleted because of the parameter `Retain Extra Versions` (inactive files are kept for 5 days).

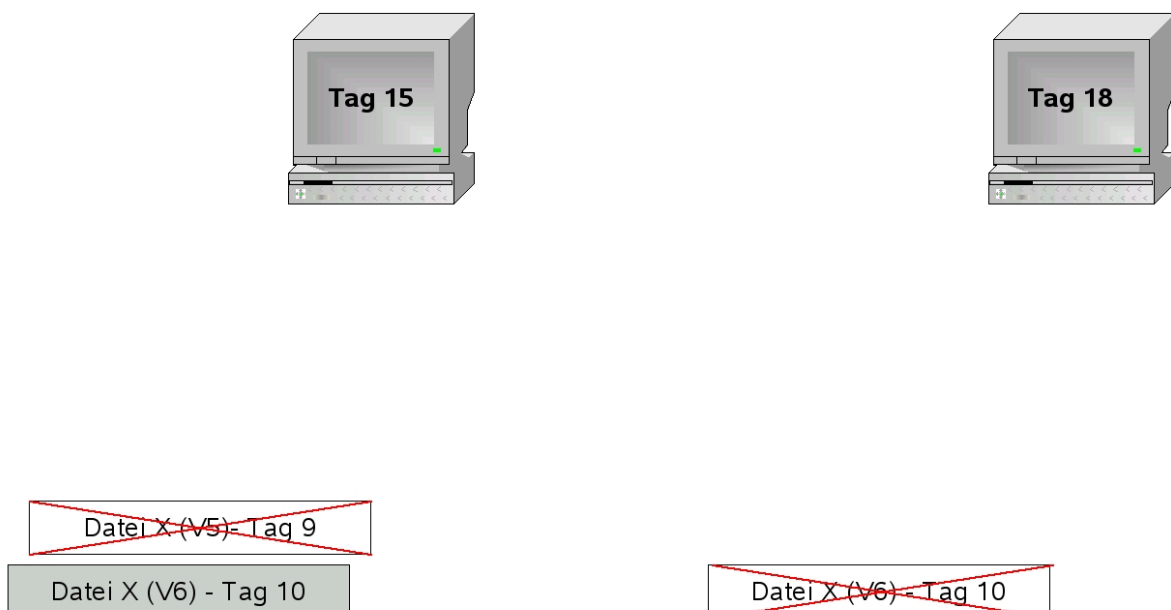
2. Basic concepts and procedures of SP

9. Tag: Changing the file X creates a new copy of the file in the backup system, setting the old active version V4 to inactive and the new version V5 to active.



10. Tag: Changing the file X creates a new copy of the file in the backup system, setting the previous active version V5 to inactive and the new version V6 to active. Since version V3 of the file is the oldest inactive copy and the `Versions Data Exists` parameter specifies that a maximum of 3 versions of a file are kept, this version is deleted.

11. Tag: Deleting the file X on the source computer sets the active version V6 of the file to inactive and deletes version 4 of the file on the backup system, as the `Versions Data Deleted` parameter specifies that at most the 2 most recent versions of a deleted file are kept.



15. Tag: Since version V5 of file X has already been in inactive state for 5 days, it is deleted from the backup system due to the `Retain Extra Versions` parameter.

18. Tag: Since version 6 of file X has already been in the inactive state for 7 days, it is deleted from the backup system due to the `Retain Only Versions` parameter.

2.2.5 Regular automatic backups with SP

In order to perform regular automatic backups with SP, there are basically two methods:

1. Using the SP scheduler program
2. Call the SP-Backup command with another e.g. operating system's own scheduler i.e. `cron` under Linux or the "scheduled tasks" under Windows.

The LRZ recommends the first variant: using the SP Scheduler program:

The SP Scheduler program is based on a time window method. This means that the backup does not start at an exact time, but in a certain time window. This procedure is usually more reliable, because if errors occur during the first start attempt, SP will try to restart the backup at a later time within the window.

The start time of the backup is adjusted to the current load situation of the backup system. This results in an optimized backup time for the application.

2.3 Comparison: Archiving and Backup at SP

The SP Archive function, unlike the Backup function, is used to store data for a longer period of time. The main purpose of the Archive function is to give the user the possibility to swap out files that are not needed all the time and to store them safely. The way archiving works is quite different from the way backing up works. These differences are summarized in the following table:

	Backup	Archiving
Variations	complete, differential or incremental, or a combination of the three basic types	always complete
Limitation of the number of versions of a file	yes Versions Data Exists	no
Version management	defined by <code>Retain Only Version</code> for the last inactive version of a file, by <code>Retain Extra Versions</code> for all remaining inactive versions	set for all inactive versions of a file by <code>Retain Version</code>
Behavior for deleted files	last saved file version is marked as inactive	No effect

Since archive files can be deleted from the source system until they are needed again, the LRZ takes special precautions for this data to keep the probability of data loss as low as possible. For security reasons, all archive files are stored not only in the LRZ archive system, but also in the archive system of another data center. However, depending on the volume of data, it takes up to 4 weeks for the secondary copy to be created. Therefore, we recommend that you delete archived data from the source system after 4 weeks at the earliest.

The archiving service of the LRZ is used for longer-term storage of data from the field of research and teaching. Use for storing data of other types, in particular system files of computers, is not supported by the LRZ, since it makes much more sense to use the backup function to secure this data.

3 SP configuration planning

Before you back up or archive data at the LRZ, you should think about the configuration of your backup and archive client. The following chapter shows you which questions you should definitely answer for yourself before you start backing up or archiving.

3.1 Basic considerations

3.1.1 Backup or archive or both?

The first question you should ask yourself is whether you want to use the SP system for backup or archiving. Although you can usually perform both backup and archiving with any SP node, under certain conditions (see 3.1.3) it makes sense or is even necessary to use dedicated nodes for backups and for archiving. The difference between backup and archiving has already been explained in Section 2.1.5.

3.1.2 What should be secured?

One of the most important questions you should ask yourself is what you do not need to back up. The LRZ is aware that it is most convenient for you to back up all files on your system, and you are free to do so. However, excluding "backup unworthy" files from backup also has some advantages:

- You can drastically shorten the backup time.
- You can drastically shorten the restore time.
- They relieve both your systems and those of the LRZ.
- Should the SP service become chargeable for you one day due to changes in the user regulations, you will save yourself unnecessary costs.

3.1.3 How much data can be backed up or archived?

Information about how much data you will be backing up or archiving is very important for LRZ planning. This is the only way we can offer you the best possible performance and support, as we distribute the nodes on our server farm due to the expected data growth. The "how much" refers not only to the total volume, but also to the number of files. We realize that this is often the most difficult question to answer, as it is very difficult to predict data growth.

If you want to backup or archive more than 20 TB or more than 10 million files, you should consider the following:

Splitting into multiple nodes or at least multiple filesystems is advisable if more than 20 TB or more than 10 million files are backed up or archived.

Please contact in time our [ServiceDesk](#) *Service: Datenhaltung – Archiv und Backup*.

This is due to the following reasons:

- The more files are managed under a node, the slower the search accesses to the SP database become for this node. This can lead to SP needing several days for a complete restore in the worst case.
- The more data volume is managed under a node, the longer a node relocation takes. From time to time, the LRZ must migrate the data of all nodes to a newer system. During this migration process, no access to the node is possible and, since a migration of a large node can take several days (up to weeks), it may make more sense to migrate several smaller nodes in succession instead of one large one.

3.1.4 How often should you back up?

Normally, you should back up your system once a day. However, for some systems, backing up several times a day is unavoidable. In this case, you should really only back up "backup-worthy" files to keep backup times as short as possible. In some cases, however, a weekly backup of your data may be sufficient. The decision of the backup frequency can only be made best by yourself.

3.1.5 Who is allowed to backup and restore?

As a rule, administrative users, such as root under UNIX or administrator under WINDOWS, are allowed to perform the backup and restore. However, it is possible to give this possibility to the other users by specific configuration adjustment. The notes on configuration adaptation can be found further in chapter 5.

3.1.6 How confidential is my data?

Another very important question you should ask yourself is to what extent you need to protect your data from access by third parties. SP offers access protection mechanisms to prevent third parties from accessing your data. However, you should consider the following points:

1. Anyone who knows the node name of your computer and the corresponding password can access the stored data. Do not share this information!
2. All data exchanged between older versions of the SP client and server is sent over the network unencrypted by default.

The newer client and server versions with the newly designed security layer (of the 7th versions from 7.1.8 and the 8th from version 8.1.2), on the other hand, communicate using TLS/SSL encryption based on the very secure AES procedure.

3. All data is stored unencrypted at the LRZ by default. However, only authorized employees have access at the data center. The data carriers after the end of their lifetime are destroyed.

You can counteract the first vulnerability by changing the initial password for your node, which was given to you by the LRZ, the first time you contact the system, and by repeating this at regular intervals. Of course, the password must be kept secret.

You can close the second vulnerability by using newer clients.

To counteract the third vulnerability and possibly the second when using the older clients, the SP client offers the option of encrypting all data and only then sending it to the SP server. This ensures that, on the one hand, no unencrypted data is sent over the network and, on the other hand, that the data is not stored unencrypted at the LRZ. The SP client optionally uses the encryption algorithms 56-bit DES, 128-bit AES and 256-bit AES. The LRZ recommends that you always use the strongest encryption algorithm offered by your SP version. If you use encryption, you are responsible for the key used to encrypt and decrypt the files. If you lose or forget it, neither you nor the LRZ nor the vendor IBM can recover your data. It should also be noted that the computationally intensive encryption process puts a load on the client. It should not be encrypted without reason, because encrypted data on magnetic tapes cannot be compressed as well as unencrypted original data. Thus, the necessary storage space requirement increases. In order to be able to offer the backup and archiving service free of charge in the future, we ask for a sustainable use of the LRZ's resources.

For more information about the encryption feature of the SP client, please refer to IBM's official installation and user manual for your SP version; where to find this is in section 9. If you have any further questions, please contact the LRZ.

3.2 Basic configuration guidelines

In the following, we present the basic configuration guidelines of the LRZ. We urge you to adhere to them, as it will then be considerably easier for us to support you in the event of a problem.

3.2.1 Location of the program files

Please always install the program files into the directory recommended by the SP installation routine.

3.2.2 Location of the configuration files

Please always place all configuration files where the SP Client expects them to be by default for your system:

System	Configuration directory
Windows	C:\Program Files\Tivoli\TSM\baclient
Linux	/opt/tivoli/tsm/client/ba/bin/
Mac OS	/Library/Application Support/tivoli/tsm/client/ba/bin

3.3 Planning the system backup

SP is not particularly suitable for backing up the operating system, since an already running operating system with SP client is required for the restore. As a rule, it is easier, faster and often better to reinstall the operating system than to restore the system with SP.

If you cannot do without *Bare-Metal-Restore-Function*, i.e. a backup of your operating system that can be restored to an "empty" computer, we recommend that you use so-called image software. This allows you to create a local backup after successfully installing and configuring the operating system, which you can restore to a new computer in the event of a disaster. Afterwards, you can restore the changes made to your operating system installation via SP since the creation of the imported image. One way to further reduce the restore time then is to create an image of your operating system disk at regular intervals.

3.4 Planning of the backup time window

When registering your node via the LRZ [DATWEB-Interface](#), you must select a time window. It defines approximately when your node should be backed up. Currently, the LRZ offers the following time windows by default:

- morning (daily, weekdays or weekly)
- evenings (daily, weekdays or weekly)
- at night (daily, weekdays or weekly)

You should consider when your system is least loaded and place the backup window in this period. If you have other requirements, please ask the LRZ [ServiceDesk Service: Datenhaltung – Archiv und Backup](#).

3.5 Planning file archiving

3.5.1 Division into several filesystems

As already mentioned in Chapter 3.1.1, it makes sense for larger archives to distribute the archived files across several filesystems. This way retrieve operations and node relocations can be performed much faster. To use multiple filesystems, you must create a separate directory for each filesystem and distribute the data to the directories in a suitable manner. According to which rules you do this, you have to decide yourself, as it mainly depends on your application and/or your data. At the LRZ, for example, there are archives in which a directory is created for each year or for different categories of data. The technical implementation of the division into filesystems is then done via virtual mount points, which are described in chapter 5.2.2.

Please note that a split of a physical filesystem into several virtual filesystems must be performed before data was archived there. Also note that this option is only available on Linux. If you intend to build a large archive with a Windows client, or if you have problems finding a suitable distribution scheme, please contact the LRZ so that we can work out a solution together.

3.5.2 Division into several nodes

In the case of very large archives, distribution over several filesystems may not be sufficient, since too many filesystems per node can lead to performance problems. In this case you have to split the archive data to several nodes. If you are planning to create such a large archive, please contact the LRZ so that we can work out a concept together.

3.5.3 Long-term archiving

Normally, archive files from SP are deleted from the archive system after a certain period of time, which you can read about in the current usage guidelines; currently this is ten years. If this period seems too short for your data, you can submit an informal request for long-term archiving to the LRZ. In particular, you should explain in your application why there is a need to archive your data for an even longer period. Please note in particular the section on long-term archiving in the usage guidelines.

3.5.4 Set character encoding

The SP Client supports umlauts in directory and file names only in certain *character encodings*. If you want to use umlauts in directory and file names, you may have to change some configuration settings of your operating system. You have to make sure that the directory and file names are created in the character encoding ISO-8859-15 or UTF-8. To do this, you must set at least the environment variables LANG and LC_CTYPE to the value de_DE@euro for ISO-8859-15 and to the value de_DE.UTF-8 for UTF8. If you use *File Sharing* via Samba or similar, you must also set the character encoding there using the appropriate configuration mechanisms to restrict the character encoding to ISO-8859-15 or UTF-8. Please note that these two character encodings are not compatible with each other and therefore the configuration of all Linux installations must be adapted to a character encoding as described above if you want to use umlauts in file and directory names.

If you create directory and file names with umlauts in a character encoding other than ISO-8859-15 or UTF-8, it may happen that:

- the corresponding files or directories are not backed up,
- the entire backup aborts with an error message.

In the worst case, this can mean that you have no backup of your system.

3.6 Planning an operating system change/update

If you have used your SP node for backup and want to change your operating system or upgrade the major version (see Section 4.2), you should note that continued use of your old node with a new operating system is not supported. The reason is that unforeseen side effects have occurred repeatedly in the past. To avoid these, the LRZ supports you in case of an operating system change or updates of the major version by means of two procedures:

1. You apply for a new node.
2. You contact the [ServiceDesk](#) *Service: Datenhaltung – Archiv und Backup* and tell us that you want to change your operating system. The LRZ renames your previous node to <NODENAME>.OLD and reinitializes a new node <NODENAME>.

4. Installing/updating/uninstalling the SP client

If you have stored archive data in addition to backup data in your old node, you are responsible for migrating the data from the old node to the new node. If you have a large archive, please consult the LRZ beforehand.

If you have stored only archive data in your node, the LRZ supports switching from one major version to the next major version of the same operating system. However, changes of the operating system are not supported for archives either. It is your responsibility to find out whether IBM supports the intended change of operating system version. If you need help from IBM in this regard, please contact the [ServiceDesk](#) *Service: Datenhaltung – Archiv und Backup*.

In this context, we would also like to point out the *character encodings* used by the respective operating system version (see Section 3.5.4). If you want to use a node over several operating system generations, it is absolutely necessary to retain the original character encoding of the first operating system version that stored archive data in it. Otherwise, in the best case, the file names will no longer be readable; in the worst case, you will no longer be able to access your archived data. Since recently more and more operating systems use a character encoding in Unicode UTF-8 by default, it is important that you are aware of this limitation.

4 Installing/updating/uninstalling the SP client

4.1 Installation

To use SP, you must first download and install the appropriate SP client software for your operating system. The following URL leads to the download pages of the SP client:

https://doku.lrz.de/display/PUBLIC/Download?showLanguage=en_US

After downloading the appropriate file, you may need to unzip it.

The unzipped directory of the Linux client of architecture AA (x86_64, ppc64, s390x, etc.) contains the following files:

Packages	Content	Installation directory
gskcrypt64-8.x.x.x.linux.AA.rpm gskssl64-8.x.x.x.linux.AA.rpm	Encryption	/usr/local/ibm/gsk8_64
TIVsm-API64.AA.rpm	Application Programming Interface (API) that contains the shared libraries and examples for the SP API.	/opt/tivoli/tsm/client/api/bin64
TIVsm-BA.AA.rpm	SP client for backup and archiving, command line (dsmc), administrative client	/opt/tivoli/tsm/client/ba/bin

4. Installing/updating/uninstalling the SP client

	(dsmadm), web client and the documentation	
TIVsm-APIcit.AA.rpm TIVsm-BACit.AA.rpm	Optional. These files provide the <i>IBM Tivoli Common Inventory Technology</i> components that you can use to obtain information about the number of client and server units that are connected to the system and the utilization of processor value units (PVUs) by server units. For more information, see the section on estimating processor value units in the <i>IBM Spectrum Protect for Linux-Administrator's Guide</i> .	APIcit is to be installed in the directory /opt/tivoli/tsm/client/api/bin64/cit/ BACit is to be installed in the directory /opt/tivoli/tsm/client/ba/bin/cit/
TIVsm-filepath-Distribution.AA.rpm TIVsm-JBB.AA.rpm	Files needed to support journal-based backups.	/opt/filepath /opt/tivoli/tsm/client/ba/bin
TIVsm_BAhdw.AA.rpm	Provides snapshot backup support for NetAPP and N-Series NAS servers.	/opt/tivoli/tsm/client/ba/bin/plugins
TIVsm-msg.xx.xx.AA.rpm	Additional languages including client messages; xx_xx defines the installed language.	/opt/tivoli/tsm/client/lang/xx_xx

The unzipped directories contain the following files for Windows and Mac OS:

OS	Content	Files
Windows	Installer	spinstall.exe
Mac OS	Installer	<SP-Version>-TIV-TSMBAC-Mac.dmg

The installation of the client software is started as follows:

OS	Start the installation
Linux	rpm -ivh gskcrypt64-8.x.x.x.linux.AA.rpm \ gskssl64-8.x.x.x.linux.AA.rpm rpm -ivh TIVsm-API64.AA.rpm TIVsm-APIcit.AA.rpm \ TIVsm-BA.AA.rpm TIVsm-BACit.AA.rpm

4. Installing/updating/uninstalling the SP client

	<p>Using the most common PC architecture as an example (AA=x86_64), x.x.x please refer to your unpacked directory:</p> <pre>rpm -ivh gskcrypt64-8.0.50.57.linux.x86_64.rpm \ gskssl64-8.0.50.57.linux.x86_64.rpm \ rpm -ivh TIVsm-API64.x86_64.rpm TIVsm-APIcit.x86_64.rpm \ TIVsm-BA.x86_64.rpm TIVsm-BAcit.x86_64.rpm</pre> <p>With some SP versions it may be necessary to specify the rpm option <code>--nodeps</code> if the above commands report an error that the <code>ksh</code> package is needed, but the <code>ksh</code> package is certainly already installed.</p>
Windows	Right click on <i>setup.exe</i> and left click on <i>Run as administrator</i>
Mac OS	<ul style="list-style-type: none">• Open the <i>icons</i> to start the <i>wizard</i> and• install backup/archive client component.• You will be prompted to specify an account with <i>superuser</i> privileges during the installation. <p>The configuration of the Mac OS SP client is performed in the same way as for Linux.</p>

More detailed installation instructions can be found in the IBM/Tivoli documentation referenced in the README files (see Section 1.7).

For the Windows SP client, the LRZ recommends installing the *Open File Support* feature, which allows SP to also back up open files. To do this, you must select *Custom Installation* in the installation dialog and select *Open File Support* with in the next dialog box.

4.2 Updates

In the course of product maintenance and development, IBM releases new versions of the SP product line at certain intervals. The SP version number consists of four digits, each separated by a dot. The first number represents the SP version, the second number the release and the last two numbers the so-called level. 8.1.2.100 means version 8, release 1, level 2.100. You have to distinguish between *major* and *minor* updates. The first two digits represent the major version number, the last two the minor version number. While minor updates usually serve the elimination of errors, new or improved program functions are usually delivered with the major versions.

Of course, it is most convenient to use a client version that has been installed once and found to be good for the entire lifetime of a system. Unfortunately, the LRZ cannot recommend this approach to you. Why updates are necessary and how you can most easily and safely perform a version update are explained in the next two subchapters.

4.2.1 Why updates?

There are 4 main reasons for performing regular updates of your SP client:

1. Program errors from the older version are corrected. In the case of correcting security-related errors, an update is especially important.

4. Installing/updating/uninstalling the SP client

2. New versions may have new useful program features.
3. If you always use the latest major version of a client, you can be sure that you are using a version supported by IBM.
4. If you always use the latest minor version of a still supported major version of a client, you save yourself having to update to the latest minor version in case of a problem (*Nota bene*: from our many years of experience with IBM support, we know that IBM usually first asks customers to update to the latest minor version of the deployed and still supported major version and to check whether the problem still exists in this version).

You can of course decide not to perform regular updates of your SP client. However, the LRZ can only help you with problems if your SP client version is supported by IBM. Since IBM only supports an SP version for 2 years on average, you should check at regular intervals whether this still applies to your version.

4.2.2 Planning and implementation of the update

"Updating" an SP client consists of completely uninstalling the old client and installing the new client.

You should only update to a new major version if this version is also linked on the [LRZ-Downloadmatrix](#). This is because the LRZ only guarantees that this client version is also compatible with the server version currently in use at the LRZ. After you update your SP client, you should perform the steps in Chapter 6 to verify that your client is working properly.

Before performing an update, please make copies of your most important SP client configuration files (`dsm.opt`, `dsm.sys` and `incl excl-Datei`). Usually, only the `dsm.opt` is important for Windows. For Linux SP clients, you can determine the name and path to the `incl excl` file using the command:

```
cat dsm.sys | grep -i incl excl
```

The output from this command then looks something like the following and gives the full path to the *Include/Exclude* file:

```
incl excl      /opt/tivoli/tsm/client/ba/bin/dsm.excl.local
```

If you do not know exactly where the SP client configuration files are located on Linux, first look in the directory

```
/opt/tivoli/tsm/client/ba/bin
```

If you don't find the files there, the Linux command

```
locate dsm.sys
```

can be useful to find `dsm.sys`.

4.3 Uninstalling the SP Client

Uninstalling the SP client on Windows and Mac-Os can be done through Software Management.

Under Linux, proceed as follows. Determine by

```
rpm -qa | grep -v alternatives | grep -i tiv
rpm -qa | grep -i gsk
```

which packages are installed and find out from them which SP package groups and which language extension (value of `xx_xx`, e.g. `DE_DE`) is installed and uninstall them with `rpm -e`:

```
rpm -e TIVsm-BAcit
rpm -e TIVsm-BA
rpm -e TIVsm-msg.xx_xx
rpm -e TIVsm-APIcit
rpm -e TIVsm-API64
rpm -e gskcrypt64
rpm -e gskssl64
```

The uninstallation of client versions older than 6.3 may differ from the procedure described above. The TSM version 6.2 contains in addition to 64Bit versions also 32Bit packages and compatibility packages, namely `gskssl32`, `gsk7bas64` and `gskcrypt32`. Please search for the installed packages if necessary.

```
rpm -qa | grep -v alternatives | grep -i tiv
rpm -qa | grep -i gsk
```

The versions before 6.2 had no support for SSL encryption and no packages of type `gsk*.rpm`, that means the command

```
rpm -qa | grep -i gsk
```

should not return a response.

A minor upgrade of the SP client may work on the basis of a major release, so the versions of the client and API may differ slightly.

An example for TSM client 6.2.2-0:

```
rpm -e gskssl32
rpm -e gskcrypt64
rpm -e gsk7bas64
rpm -e gskcrypt32
rpm -e gskssl64
rpm -e TIVsm-BA-6.2.0-0
rpm -e TIVsm-API-6.2.2-0
rpm -e TIVsm-API64-6.2.2-0
```

5 Configuration and examples

5.1 Archive and backup

5.1.1 Configuration under Linux and Mac OS

5.1.1.1 Creating the `dsm.sys` configuration file

The `dsm.sys` file is the most important configuration file of your SP client. It should have at least the following content:

```
defaultserver      local
nodename           TESTNODE
servername         local
tcpserveraddress  <s44>.abs.lrz.de
tcpport           <1616>
inclexcl          /opt/tivoli/tsm/client/ba/bin/dsm.excl.local
schedlogretention 7 D
errorlogretention 7 D
errorlogname      <Path to the Error-Logfile>
schedlogname      <Path to the Scheduler-Logfile>
passwordaccess    generate
passworddir       < Path >
```

The specifications in angle brackets (`<...>`) are to be understood as placeholders and must be supplemented by suitable values.

- `defaultserver` defines which SP server is addressed by default.
- `nodename` defines which ISP node is to be addressed
- `servername`, `tcpserveraddress` and `tcpport` belong together and define an SP server. The name for `servername` is freely selectable. The values of `tcpserveraddress` and `tcpport` are determined by the information given to you by the LRZ when you registered your node. Please make sure that your firewall is enabled for `tcpport`. If necessary, ask your local administrator.
- `inclexcl` sets the path to the configuration file for files that are not to be backed up.
- `schedlogretention` and `errorlogretention` specify how many days the scheduler log messages and error log files should be retained.
- `schedlogname` specifies where in the directory tree the scheduler log file should be created.
- `passwordaccess generate` is only needed if client should backup/restore without direct input of password. Password is stored encrypted in file `TSM.PWD` if client version $< 8.1.2$ or $7.1.8$ or `user = root` and the client version is $\geq 8.1.2$ or $7.1.8$. This is often required for backup by scheduler.
Remark: Verify if `TSM.PWD` has been created, e.g. with `locate TSM.PWD`
- `passworddir < Path to Directory >` is only used in case of client version $\geq 8.1.2$ or $7.1.8$ for a non-administrative user (\neq root) who wants to use `passwordaccess generate`. In the specified directory three files `TSM.IDX`, `TSM.KDB`, `TSM.sth` are created. These files contain encrypted password similar to `TSM.PWD` and the necessary settings for the non-root user.

Attention: The user must have read/write permissions for the specified directory, otherwise the above mentioned TSM.* files will not be created and `passwordaccess generate` will not work.

Remark: After the first client access verify if the files have really been created:

```
cd < Path to Directory > ;ls TSM.IDX, TSM.KDB, TSM.sth
```

5.1.1.2 Creating the `dsm.opt` configuration file

Unlike Windows, the Linux SP client has not only a `dsm.opt` configuration file, but also a `dsm.sys` configuration file. Under Linux, the settings are distributed: In the `dsm.sys` file the system-wide configuration is made. The `dsm.opt` file can be seen as a supplement to the `dsm.sys` file. With it the users of the system can make own settings. Even if you don't want to

do this, you have to create a `dsm.opt` file under `/opt/tivoli/tsm/client/ba/bin/dsm.opt` when configuring the client. Then just leave this file empty. Enter the only file systems to be backed up in the `dsm.opt`:

```
domain      /File system 1/to/be/backed/up
domain      /File system 2/to/be/backed/up
...
domain      /File system N/to/be/backed/up
```

5.1.1.3 *Include/Exclude* Configuration

The last thing to do is to create the *Include/Exclude* configuration, which defines which files or directories are backed up and which are not. As already explained in chapter 3.1.2, the backup of some files does not make sense; these include system and open as well as temporary files. When trying to do so, the backup process may also fail with an error (e.g. when backing up the `sysfs` under Linux). To exclude such files, you must create the file that you specified as the value for the `incl excl` parameter in the `dsm.sys` configuration file. Also, if you want to exclude files from backup, it is useful to have the following in the first line of `dsm.sys`:

```
include      *
```

To exclude files from the backup, use the `exclude` statement. To exclude entire directories from the backup, use the `exclude.dir` statement. For Linux-based SP clients, we recommend that you exclude at least the directories `/dev`, `/proc` and `/sys` (`/sys` as of kernel 2.6). Then your *Include/Exclude* file will look something like this:

```
include      *
exclude.dir  /dev
exclude.dir  /proc
exclude.dir  /sys
```

The entries of the *Include/Exclude* file are evaluated in their order. If several entries fit on one file, the last, i.e. lowest entry is used. For the correct configuration the following command can help:

```
dsmc query inclexcl
```

These are only the basics of the *Include/Exclude* configuration. If you need more than the presented minimal configuration, please read the corresponding chapter in the official installation and user manual from IBM that matches your operating system. To test whether your *Include/Exclude* configuration will have the desired effect, the SP-Client offers the `preview-`command. You can find more details about this in the official manual in the chapter about the *Include/Exclude* configuration and in section 6.1.

5.1.1.4 Changing the initial password

To change your SP client password, please run the following command as `root` if necessary:

```
dsmc set password <old password> <new password>
```

5.1.1.5 Starting the SP Scheduler

For SP to automatically back up your system, a service must be started, ideally at boot time, called the SP scheduler.

```
/pfad/zu/dsmc sched > /dev/null 2>&1
```

E.g.

```
/opt/tivoli/tsm/client/ba/bin/dsmc sched >/dev/null 2>&1
```

How you invoke this command at system startup depends on your Linux distribution. The most common ways are:

- Creating an rc script
- Adding the entry
TSM::once:/path/to/dsmc sched > /dev/null 2>&1
in the file `/etc/inittab`

5.1.1.6 Starting the SP Scheduler under Mac OS

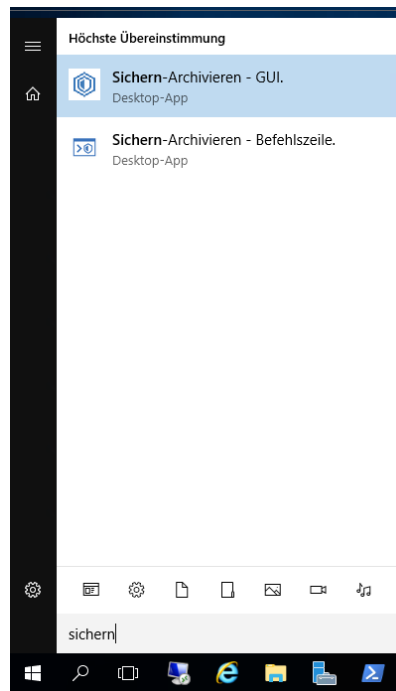
- Open the *IBM Spectrum Protect* folder
- Start the *SP Tools for Administrators*
- Then select *Start Client Acceptor Daemon*
After you have selected `OK`, your local administrative password will be requested. If you have authenticated yourself correctly, the scheduler will be started and you will receive a corresponding confirmation.
- The SP scheduler will create two log files in the `/Library/Logs/tivoli/tsm/` folder: `dsmsched.log` (`stdout`) and `dsmerror.log` (`stderr`)

5.1.2 Configuration under Windows

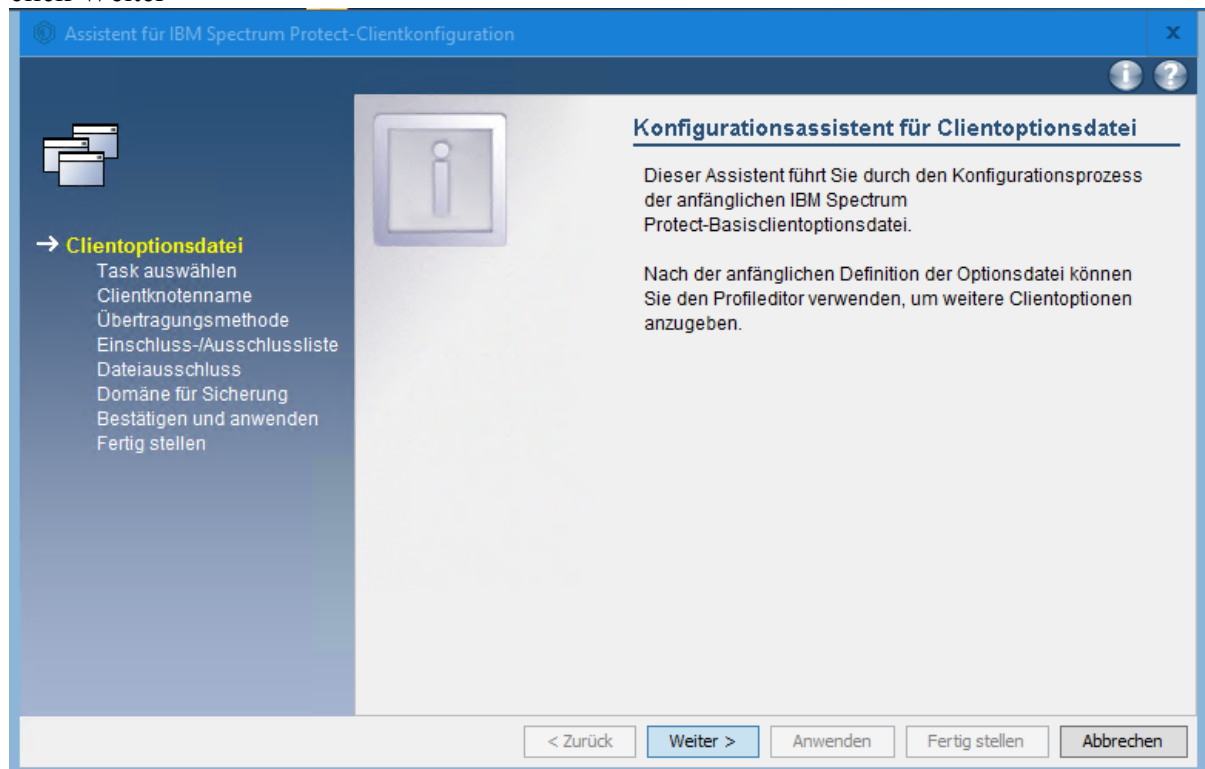
5.1.2.1 Initial configuration of the SP client

Call the SP Client for the first time as administrator. It will then guide you through a dialog that allows you to create the basic configuration of your SP Client. In the following, we present the basic configuration recommended by the LRZ.

Now start the graphical user interface (GUI):

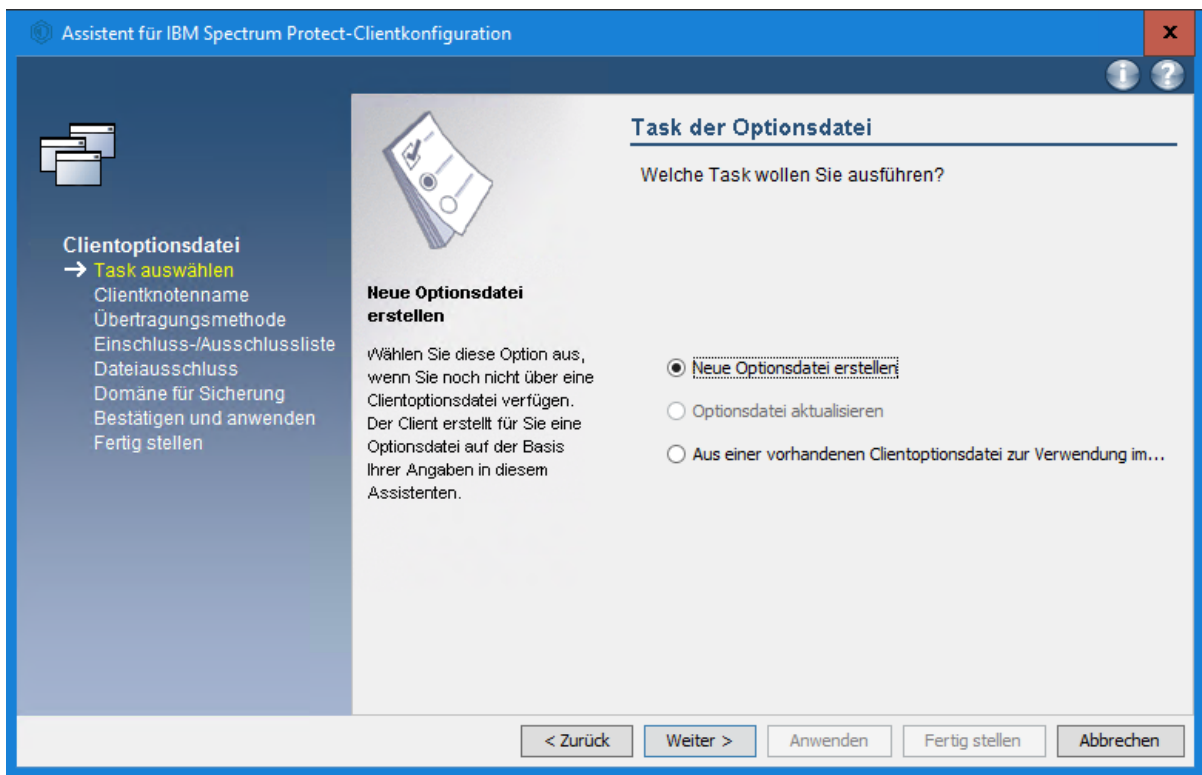


click Weiter >

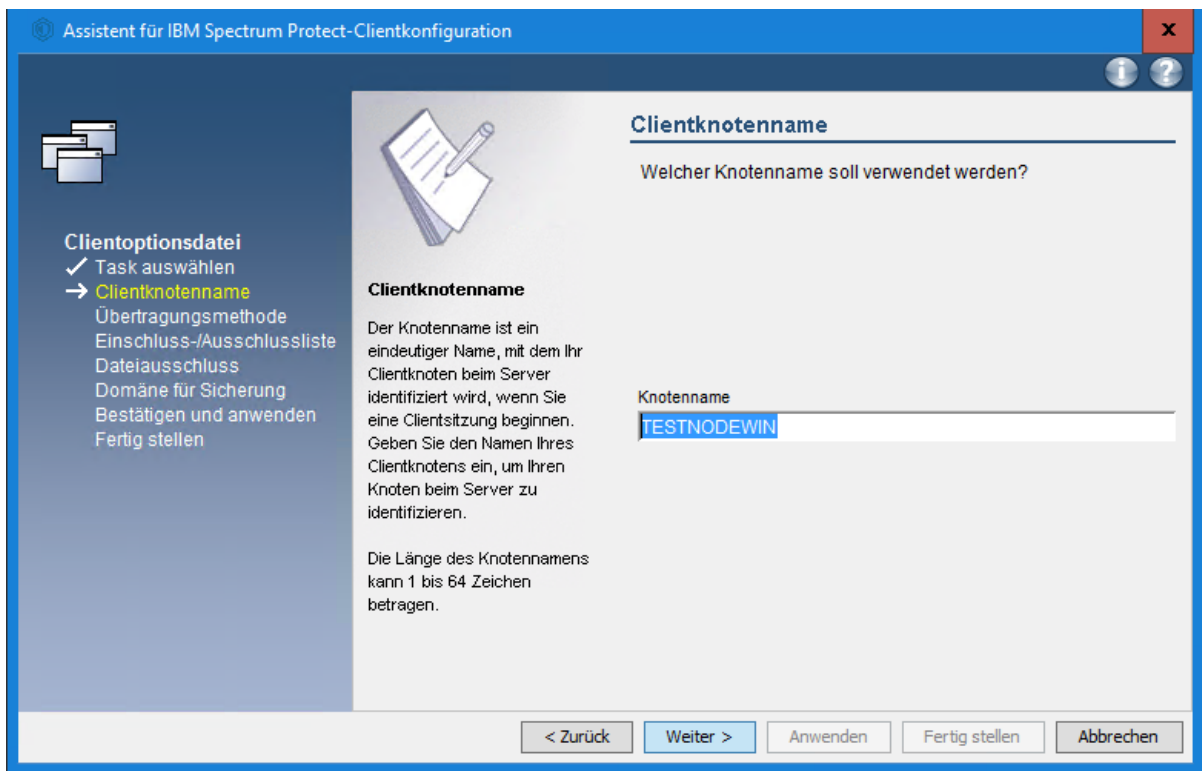


5. Configuration and examples

Create a new SP client configuration:

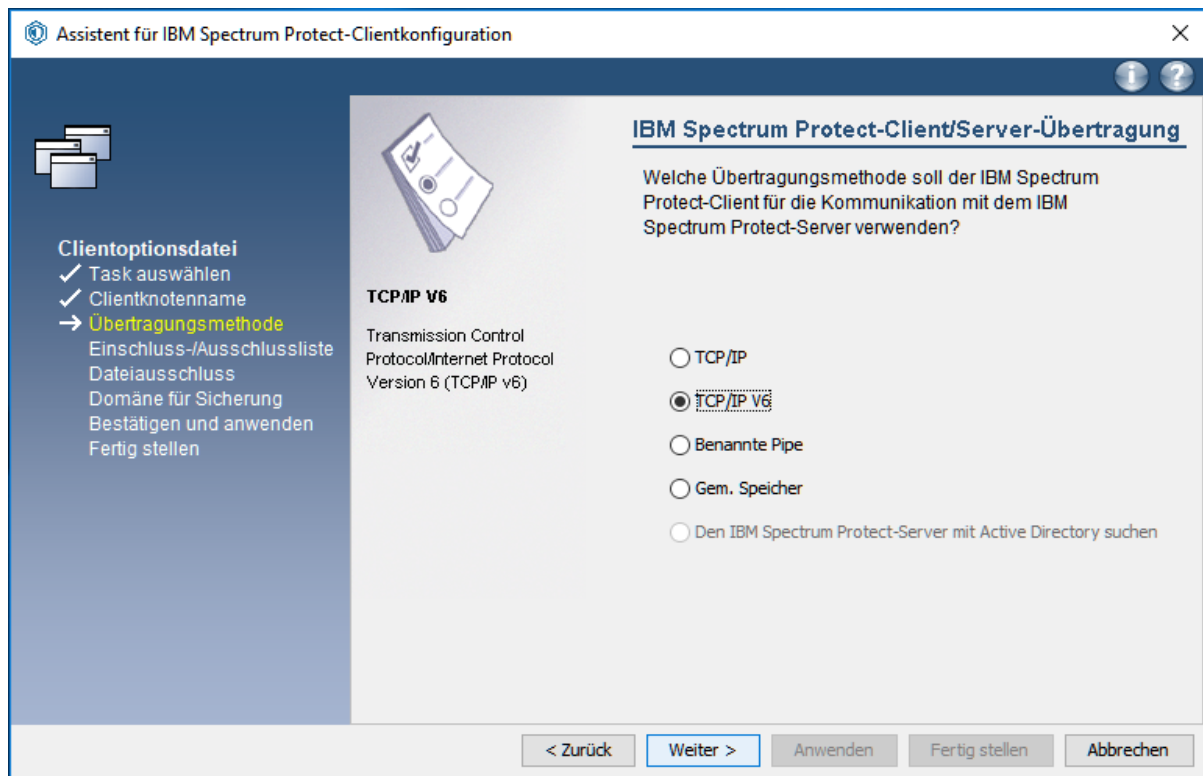


In the next step, you must specify the name of your SP node as it was given to you by the LRZ:

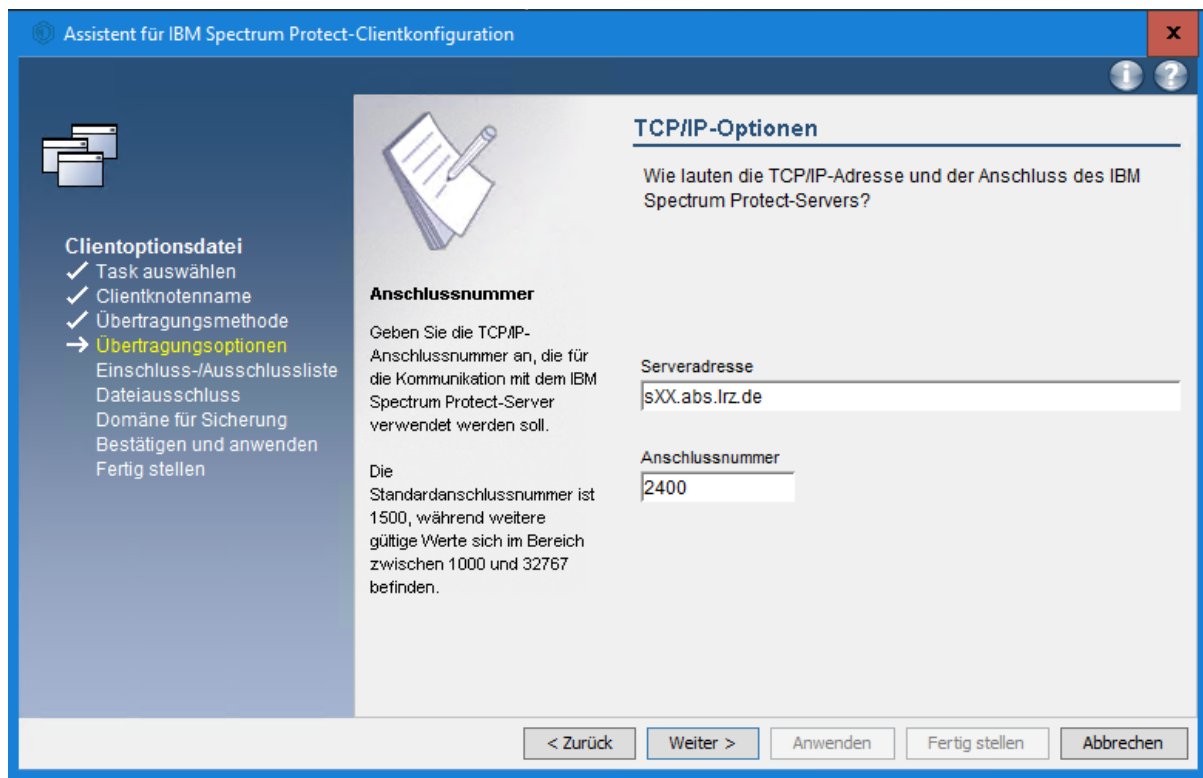


5. Configuration and examples

Then specify how the client should communicate with the LRZ SP server over the network.

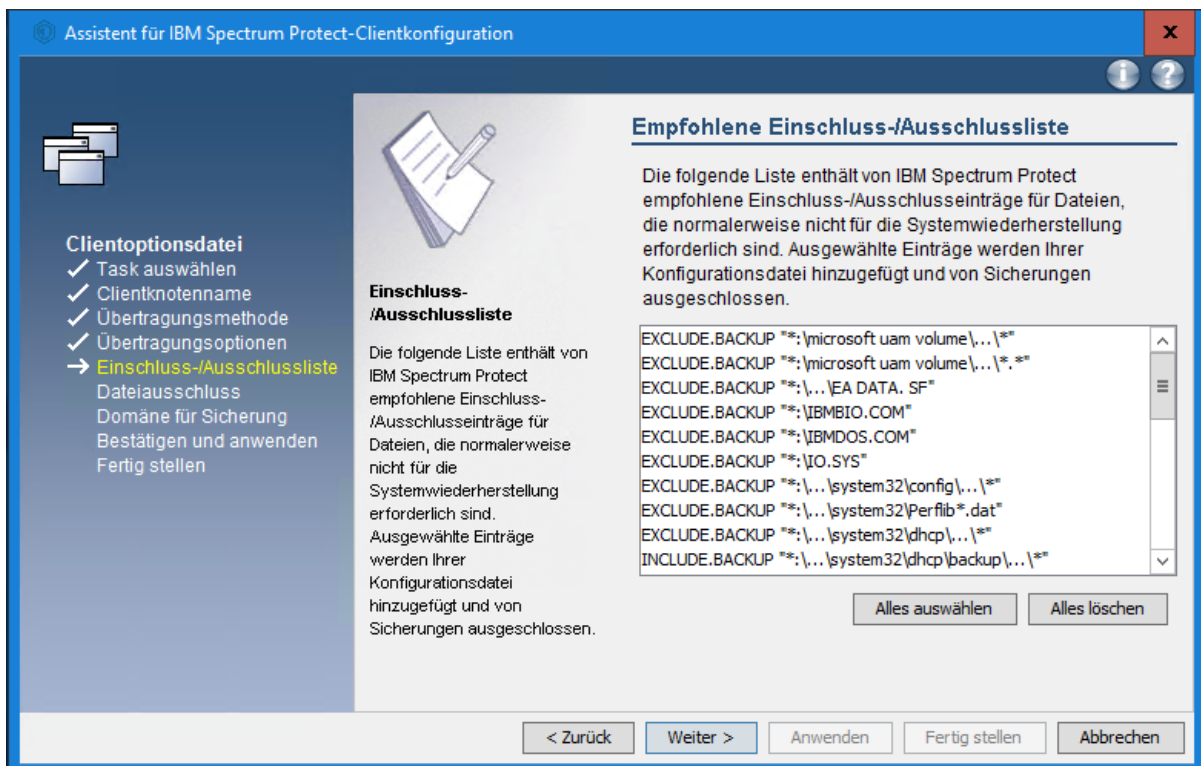


In the next step, you must specify the name and port of the SP server as it has been communicated to you by the LRZ. This port must be enabled in the firewall.

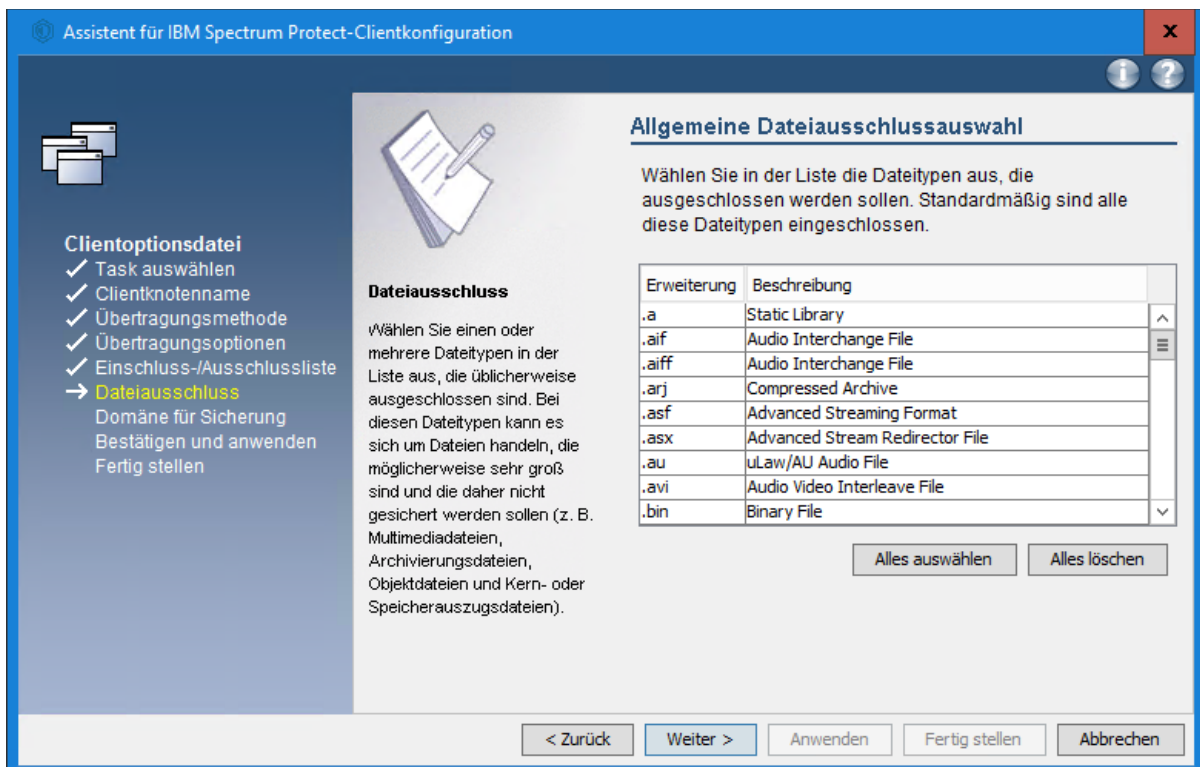


5. Configuration and examples

Next, the dialog shows you a proposal for an *Include/Exclude* list. This list determines which files should be saved and which should not. Press Delete all here and click Weiter >

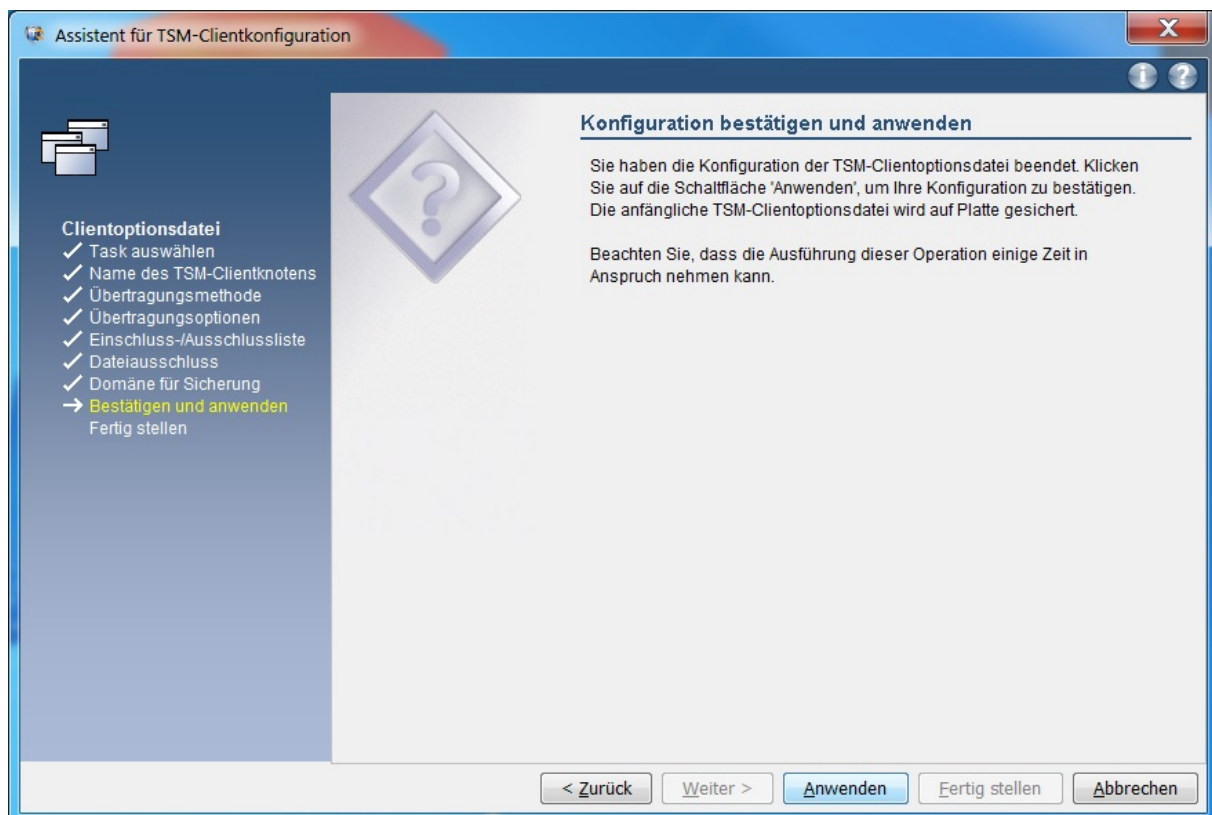
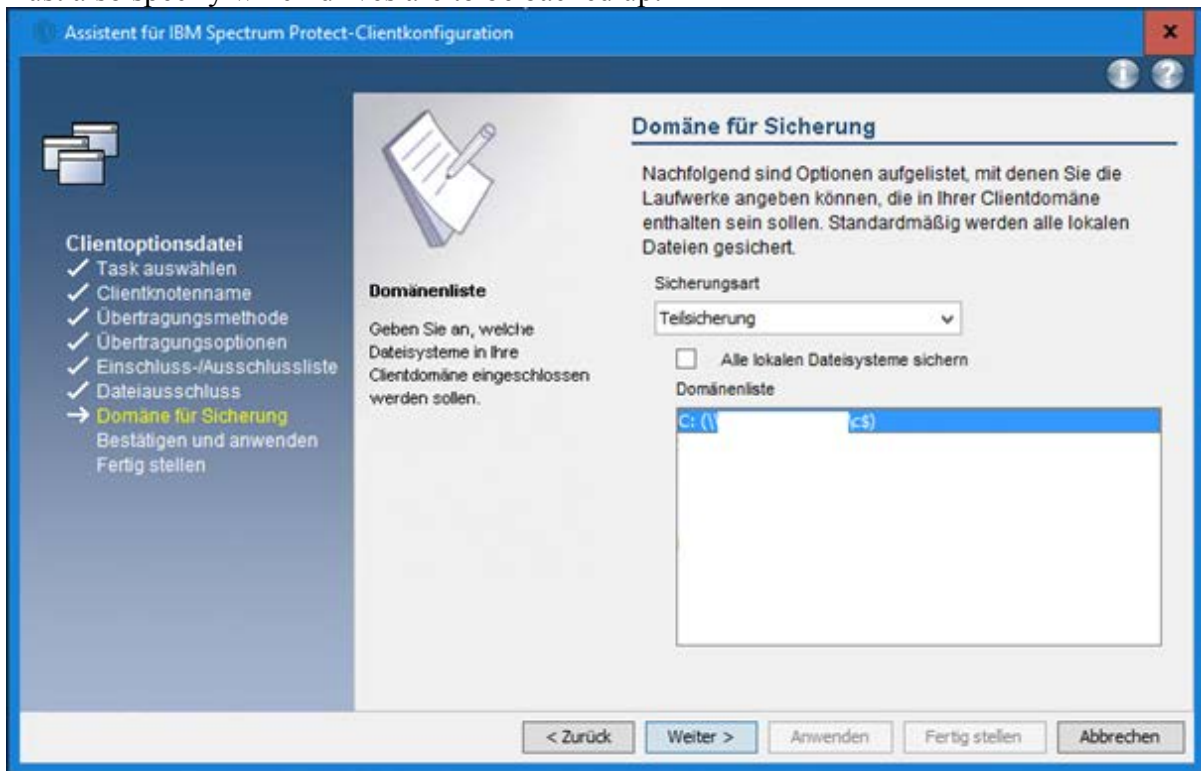


You can also specify which file types should not be backed up by SP (E.g. .mp3, .avi, .mpg, etc.).



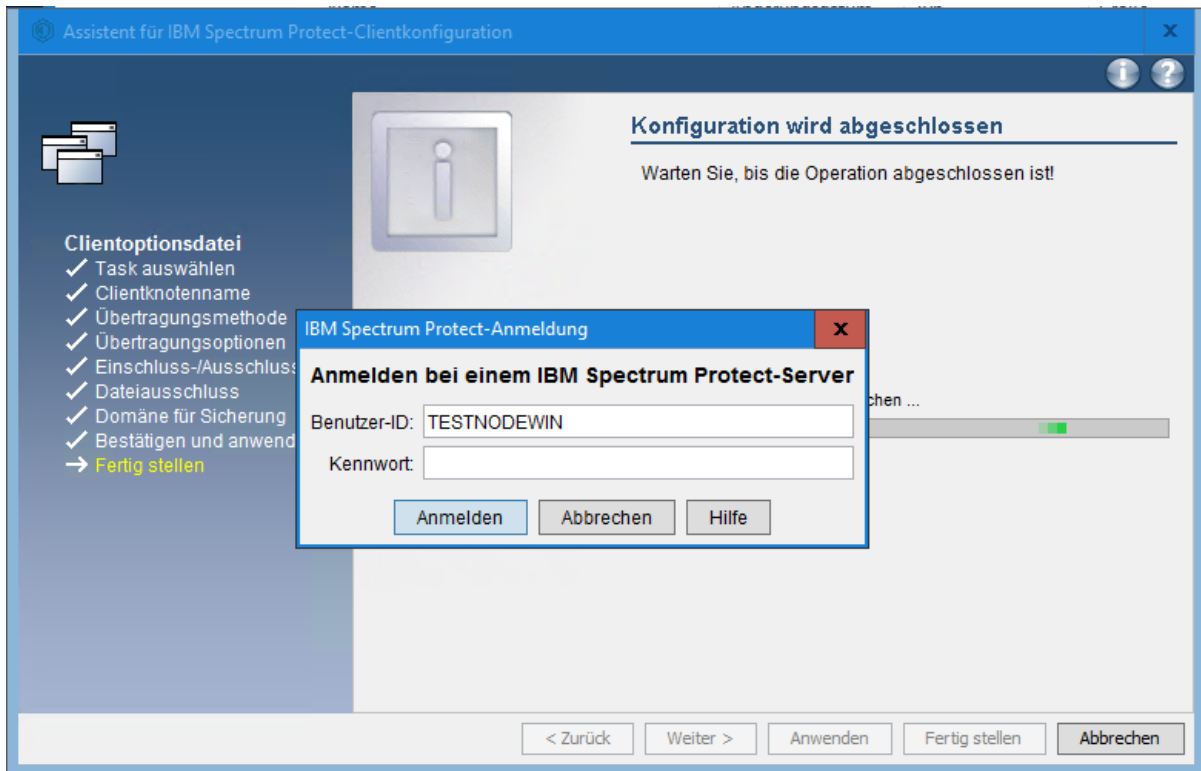
5. Configuration and examples

Finally, you must specify that the SP Client should perform the backup incrementally. You must also specify which drives are to be backed up:

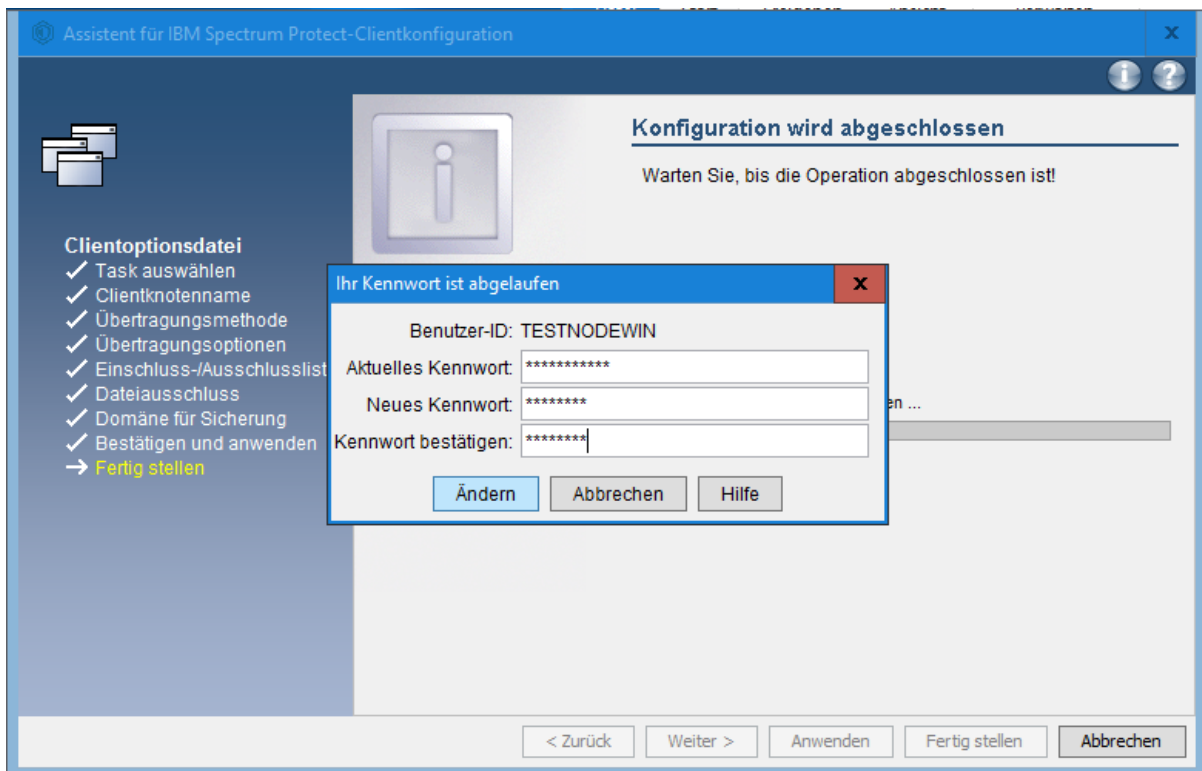


5. Configuration and examples

Then you have to log in to the SP server. To do this, use the node name as the user ID and the corresponding password provided to you by the LRZ.



Now enter the current node password and then the new password twice and press Ändern:



5. Configuration and examples

Now the SP-Client is configured so that it basically works. However, the configuration is not yet optimal, so please follow the advanced configuration.

5.1.2.2 Advanced configuration

The configuration file `dsm.opt` is located in the installation directory → `C:\Program Files\Tivoli\TSM\baclient`

Your `dsm.opt` configuration file looks something like this after the basic configuration:

```
NODENAME          TESTNODEWIN
TCPSEVERADDRESS  sXX.abs.lrz.de
TCPPOINT         2400
DOMAIN           \\XXXXXXXXXX\c$
```

Please now extend your configuration file with the entries that are missing. The comments with `*` in front of them can also be used for an overview.

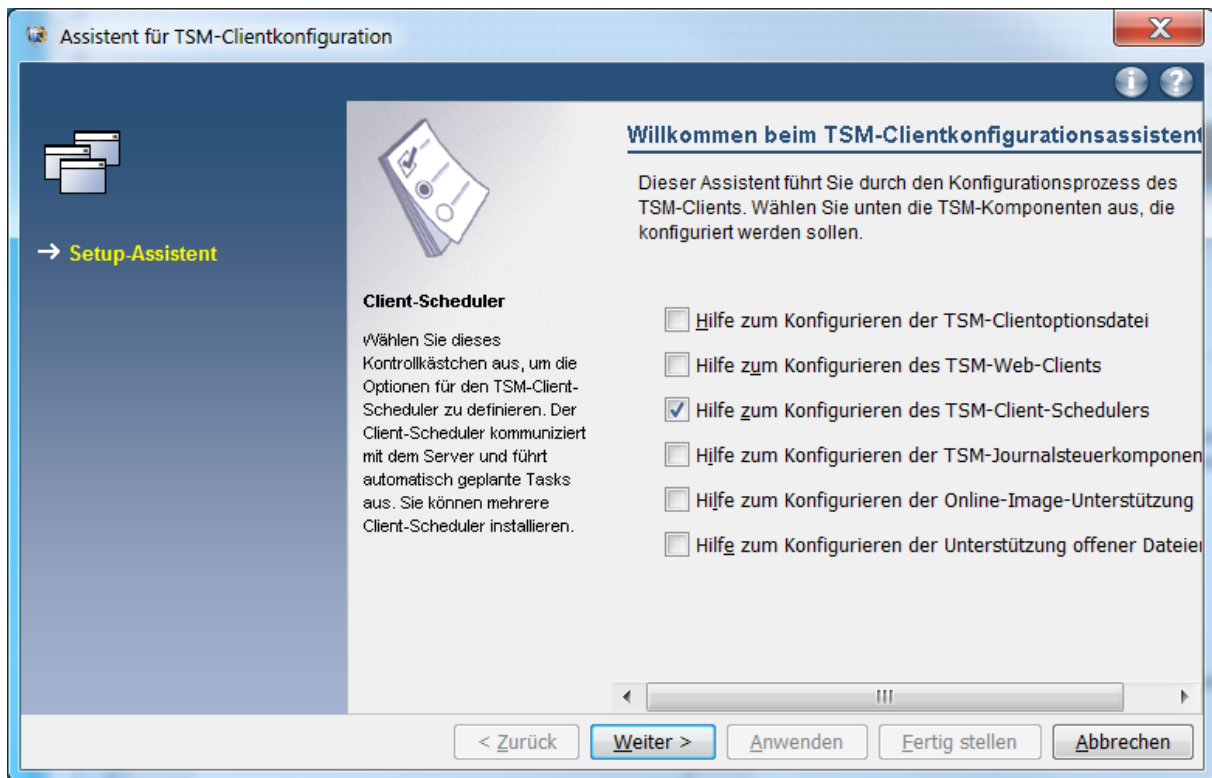
```
NODENAME          TESTNODEWIN
TCPSEVERADDRESS  sXX.abs.lrz.de
TCPPOINT         2400
COMMMETHOD     V6TCPIP
*### define your domains (partitions) that should be backuped
DOMAIN "\\testpc\c$"
*### Please uncomment pwgen (with *) before the first login, only necessary
if the Node password has not been changed yet.
PASSWORDACCESS  GENERATE
*### Logpruning after 7 Days
ERRORLOGRETENTION 7 D
SCHEDLOGRETENTION 7 D
*### Setting for the automatic Backup service
QUERYSCHEDPERIOD 1
*### Exclude Windows and Program directory's
EXCLUDE.DIR "C:\temp"
EXCLUDE.DIR "C:\Windows\Temp"
EXCLUDE.DIR "C:\Windows\System32"
EXCLUDE.DIR "C:\Users\...\AppData"
EXCLUDE.DIR "C:\ProgramData\Microsoft\Windows Defender"
EXCLUDE.DIR "C:\ProgramData\Sophos"
EXCLUDE.DIR "C:\System Volume Information"
EXCLUDE.DIR "C:\Windows\ServiceProfiles"
*### Use VSS to increase the chance that the files could be backuped while
they are opened in any program
SNAPSHOTPROVIDERFS VSS
SNAPSHOTPROVIDERIMAGE VSS
*### Avoid problems with Permissions of data
SKIPNTPERMISSIONS YES
SKIPNTSECURITYCRC YES
```

Currently the service for automatic backup is not running yet, it has to be configured separately.

5.1.2.3 Configuration of the SP scheduler

To enable the automated backup service, do the following. Select in the SP Client main window *Utilities/Dienstprogramme*, then *Setup Wizard/Setup-Assistent*.

5. Configuration and examples



Now select that you want to create a new schedule (*Neuen oder zusätzlichen Scheduler installieren*).

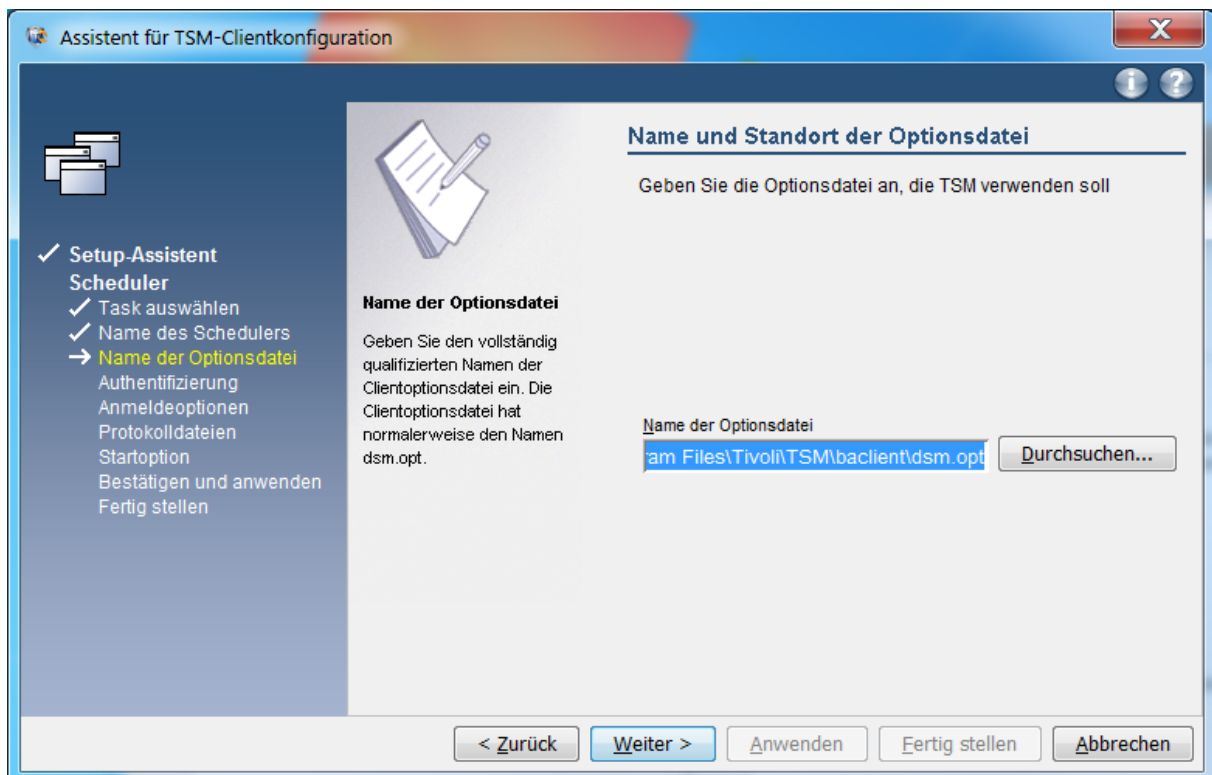


If desired, you can assign any name for the service.

5. Configuration and examples

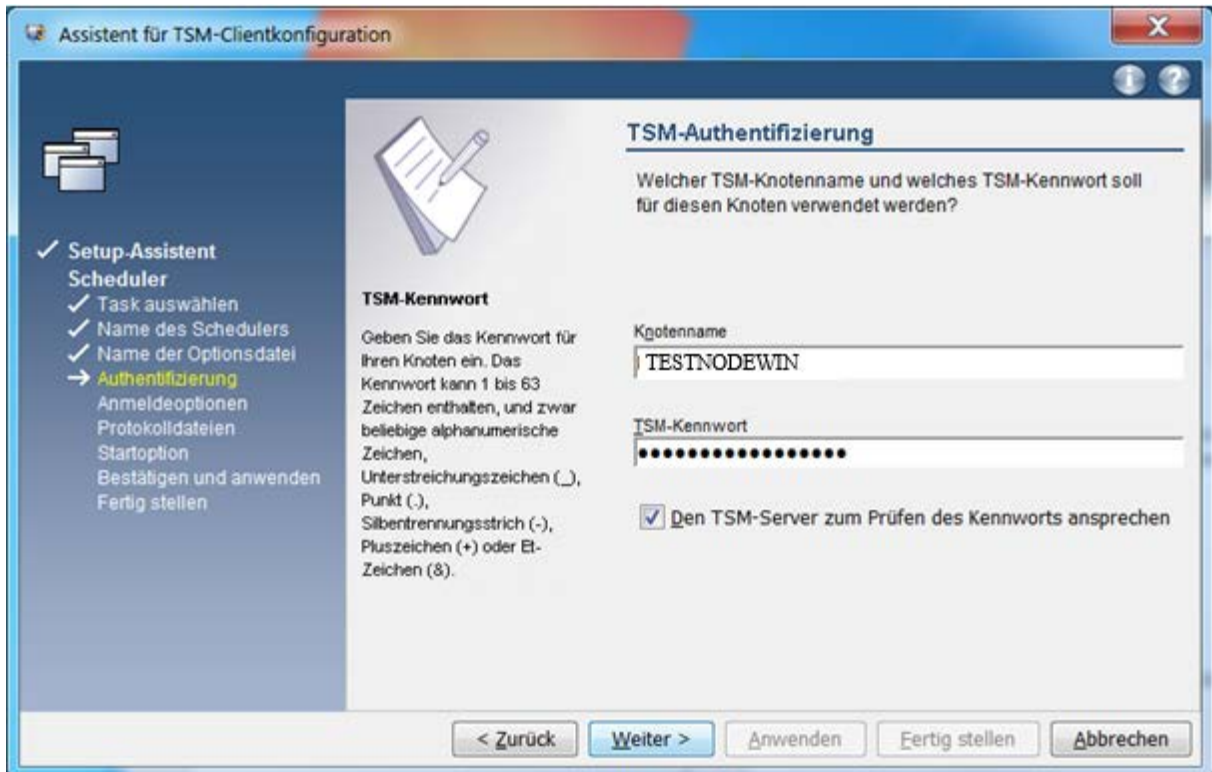


Use SP's default suggestion for the `dsm.opt` file.

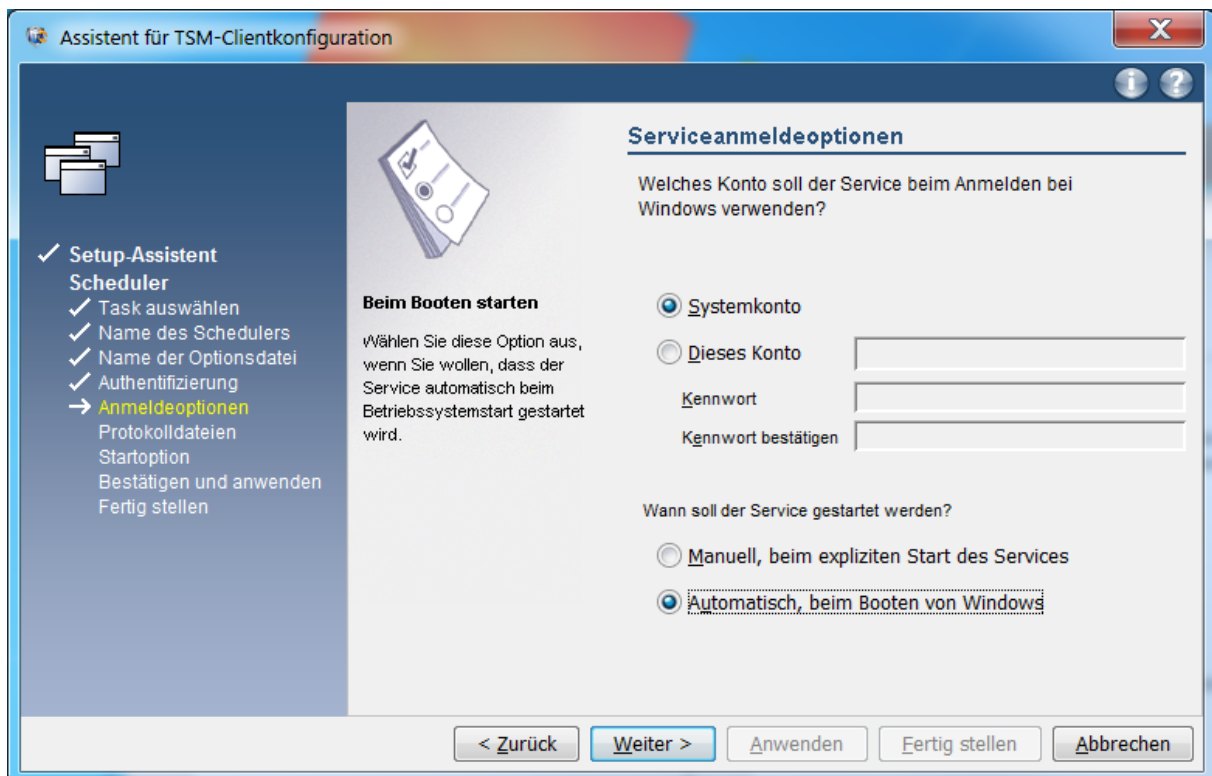


5. Configuration and examples

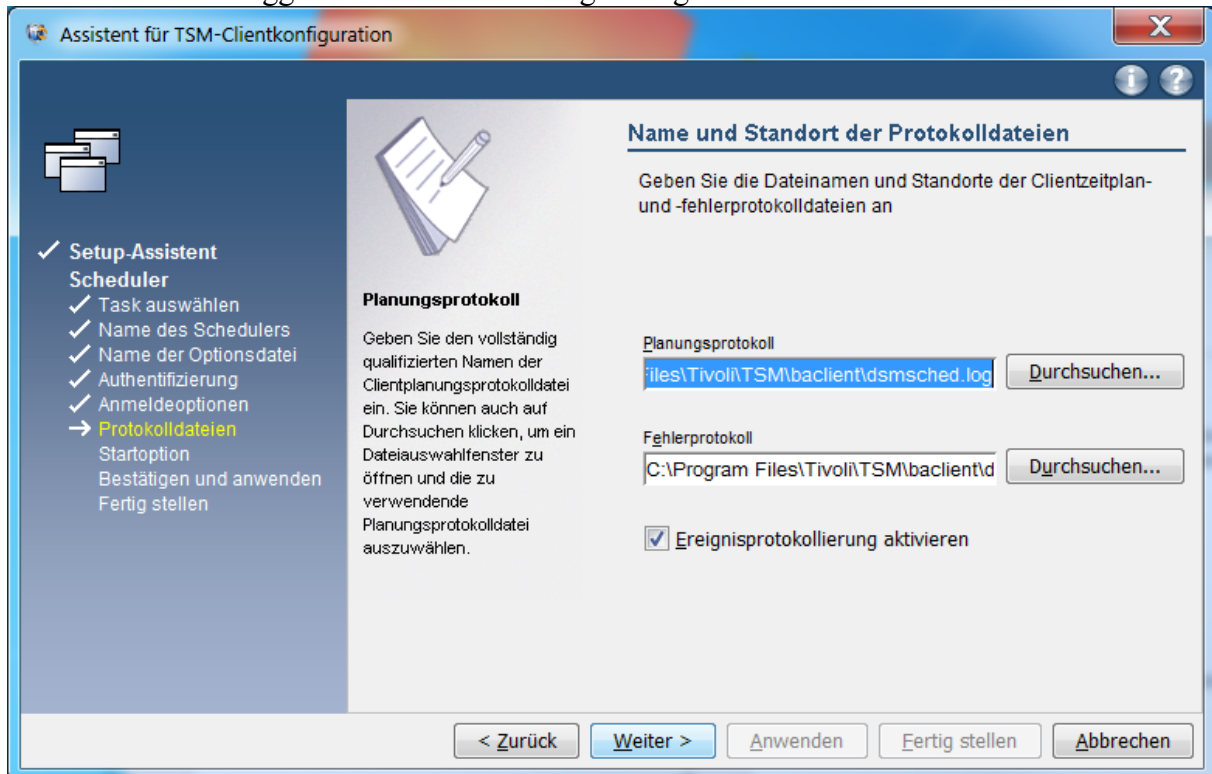
Enter the node name and the corresponding password and enable the option to verify the password.



Specify that the system account should be used and that the service should be started automatically when Windows boots.



Use the SP client suggestion for the following settings.



Now, as soon as you start the SP scheduler manually or reboot your system, SP will automatically back up your system.

5.2 Splitting of data into multiple nodes Archive & Backup

As already mentioned in Section 3.1.3, it is advisable to use multiple nodes or at least define multiple virtual filesystems when a certain data volume or file count is reached. In the following, we will explain how you can manage a split into several nodes or several virtual filesystems. Note, however, that it is assumed that you make these configurations before you archive files. If you have already backed up or archived data and plan to convert to multiple nodes or filesystems, please contact the LRZ, as there may be some additional things to consider in order to access the already archived data as usual. The following illustration is based on the implementation under Linux.

5.2.1 Splitting into multiple nodes under Linux, Unix and Mac

To address multiple nodes on a client machine, the server definition in the `dsm.sys` configuration file looks something like this:

```
servername <nodename1>
tcpserveraddress <n33>.abs.lrz.de
tcpport <1216>
nodename <nodename1>
passwordaccess generate
inclexcl /opt/tivoli/tsm/client/ba/bin/<nodename1>.excl.local
ERRORLOGRETENTION 7 D
SCHEDLOGRETENTION 7 D
errorlogname /var/log/messages/dsm/<nodename1>error.log
schedlogname /var/log/messages/dsm/<nodename1>sched.log
...
*#####
servername <nodename2>
tcpserveraddress <n34>.abs.lrz.de
tcpport <1317>
nodename <nodename2>
passwordaccess generate
inclexcl /opt/tivoli/tsm/client/ba/bin/<nodename2>.excl.local
ERRORLOGRETENTION 7 D
SCHEDLOGRETENTION 7 D
errorlogname /var/log/messages/dsm/<nodename2>error.log
schedlogname /var/log/messages/dsm/<nodename2>sched.log
...
*#####
...
servername <nodenameN>
tcpserveraddress <n99>.abs.lrz.de
tcpport <1919>
nodename <nodenameN>
...
```

and the `dsm.opt` so:

```
servername <nodename1>
SUBdir yes
...
servername <nodename2>
SUBdir yes
...
servername <nodename2>
...
```

Now, to access a specific node with the SP client, you can call the `dsmc` or `dsmj` command with the parameter `-se=<nodenameX>`.

5.2.2 Splitting into multiple filespaces on Linux, Unix and Mac

The so-called *virtual filespaces* are defined in the configuration file `dsm.sys` as follows:

```
VirtualMountPoint /Path/to/Virtual/Filespace1
VirtualMountPoint /Path/to/Virtual/Filespace2
...
VirtualMountPoint /Path/to/Virtual/FilespaceN
```

5.2.3 Splitting the data into several nodes under Windows

If you currently have only one node configured, then the configuration of the node is stored in the `dsm.opt` file under `C:\Program Files\Tivoli\TSM\baclient`. To access two or more nodes you have to create a new `.opt` file in the path `C:\Program Files\Tivoli\TSM\baclient` for the new node. This would then optimally be named `<nodename>.opt`. Example:
Nodename TESTWIN2 -> name of the nth `.opt` file `testwin2.opt`

The configuration of the TESTWIN2 node is done as described in chapter 5.1.2.2. Open cmd as administrator and change with `cd C:\Program Files\Tivoli\TSM\baclient` to the path of the SP client. Now you can open the ISP GUI (graphical user interface) of the new node with the command `dsm -optfile=testwin2.opt` and start the ISP commandline with `dsmc -optfile=testwin2.opt`.

6 Test the configuration

To ensure that your SP client configuration works as you planned, you should test it. In the following, we will present all the steps to check the SP client configuration. You should perform this test not only after the initial configuration of SP, but ideally at regular intervals, or at least every time you change the SP client configuration or language settings such as the character encoding of your operating system. Files that have not been backed up or archived cannot be restored. Check your configuration.

6.1 Evaluating the preview function

The SP client provides a preview. Preview creates a file `dsmprev.txt`, which records for each file whether it will be saved or not. To do this, call the following command for each file system on your computer:

```
dsmc preview backup <Mountpoint> (Linux)
respectively
dsmc preview backup <Laufwerksbuchstabe> (Windows)
```

You should check the `dsmprev.txt` file that is now created for anything unusual. Make sure that all files to be backed up are really specified as being backed up.

6.2 Testing the backup function

To test the backup function, you can create a test directory. Now create a few files in this directory. For the test it is best to create some special cases like umlauts or spaces in the file name. Then back up the directory by executing the following command:

```
dsmc incremental -subdir=yes /Path/to/Testdirectory/
```

In the output of the command, you can check whether all files have been backed up. In addition, you can use the following command to display which files from the test directory are now present on the SP server:

```
dsmc query backup -subdir=yes /Path/to/Testdirectory/
```

7. Retrieve archive data

In the last step, try to restore the backed up files. To do this, execute the following command:

```
dsmc restore -subdir=yes /Path/to/Testdirectory/  
/Path/to/Output/of/Testdirectory/
```

Check the output of the restore command to see if all files could be restored. In addition, you should compare the contents of the restored files with those of the original files.

6.3 Testing the Archive Function

To test the archive function, proceed in the same way as in the previous section, but use the commands:

```
dsmc archive -subdir=yes /Path/to/Testdirectory/  
dsmc query archive -subdir=yes /Path/to/Testdirectory/  
dsmc retrieve -subdir=yes /Path/to/Testdirectory/  
/Path/to/Output/of/Testdirectory/
```

6.4 Checking the scheduler log file

After the previous steps have convinced you that your SP configuration is operational, you should definitely check whether a backup run could also be performed without problems. To do this, you must evaluate the scheduler log file, whose location you can specify on a Linux system as the value of the variable `schedlogname` in the `dsm.sys` configuration file.

On Windows you can usually find the file under
`C:\Programme\Tivoli\TSM\baclient\dsm Sched`

During the evaluation, you should pay particular attention to files that have not been backed up and aborts of the backup process.

7 Retrieve archive data

If you want to retrieve archive data from the SP archive to your local computer, you should retrieve all the required data at once if possible, i.e. by a single `Retrieve` request.

There are two reasons for this procedure:

1. With each retrieve request, the tape with the archive data is rewound and it must be repositioned. Individual retrievals therefore take longer than in a bulk.
2. Frequent insertion puts a lot of stress on the tape media, which in the worst case can destroy the tape and lead to data loss.

If it is not possible to retrieve the required archive files all at once for space reasons, you should in any case retrieve as large a volume of data as possible with each retrieve. Should the LRZ observe an excessive number of mounts, we reserve the right to stop this in order to protect our hardware and the data stored on it from defects.

8 Tasks of a SP supervisor

Even after the SP Client has been installed and configured, a minimum of maintenance is still essential. Even though the SP Client software is usually low-maintenance, we would like to point out a few tasks that, if performed regularly and conscientiously, can save you time in the long run:

- Regularly check the log data to see if and, if so, what errors occur. Especially if you do not use the SP scheduler.
- Paying attention to the LRZ's notice and statistics messages and checking the information to be read in them for potential inconsistencies such as unusually high memory consumption.
- Regular version updates of the SP client (see Chapter 4).
- Regular testing of the SP configuration (see Chapter 7), especially in the case of updates or configuration changes.
- Organizational changes (contact persons, etc.) must be communicated to the LRZ in a timely manner. Please note that security-critical operations such as resetting a node password can only be performed by the contact person registered at the LRZ for the node.
- The LRZ must be notified as soon as possible of any serious changes to the data volume to be backed up.
- Exclusion of open files or under Windows use of OFS. For more information, please refer to the official SP client manual from IBM.

9 What to do when something does not work

Consult the following sources of information:

- [SP FAQs](#)
- *SP Best Practice Guide* of the LRZ, i.e. this document, which we regularly update and improve.
- Official [SP-Client-Manual fom IBM](#)
- Search for solutions in the [SP-Forum](#)

If you cannot solve your problem with the above mentioned help, you can contact us via the [Servicedesk](#) *Service: Datenhaltung – Archiv und Backup*. For problem handling we need at least the following information from you:

- Operating system of the SP client computer
- with Linux please also:
 - Used distribution and version
 - Kernel version, that means the output of `uname -a`
 - Version of `glibc`, `libstdc++`, `rpm`
- Used computer architecture
- SP-Client Version
- the file created by calling `dsmsc query systeminfo`,
- detailed problem description

We ask you to submit all support requests exclusively via the [Servicedesk](#). This is the only way we can ensure that your requests are processed as quickly as possible and transparently as well as qualified. Direct requests to our staff are not considered official requests and are therefore only processed with the lowest priority.

In addition, staff vacations and other absences may cause delays in processing.

10 General tips

In this section we present some selected frequently asked questions, answers and tips. First of all, it should be noted that we have explicitly given the respective `dsmc` commands in the long form above. However, you can often use almost any short forms can be used as long as they can be interpreted unambiguously by SP:

```
dsmc incremental -subdir=yes /tmp/test
dsmc incremen -subdir=yes /tmp/test
dsmc increm -subdir=yes /tmp/test
dsmc inc -subdir=yes /tmp/test
dsmc i -subdir=yes /tmp/test
```

Accordingly, the commands `q` for query, `ba` for backup, `ar` for archive, `rest` for restore and `ret` for retrieve.

10.1 How to upgrade my Linux SP client to a newer version?

Please read carefully chapter 4. and the `README` file of the SP version you want to upgrade your SP client to.

Basically the cleanest procedure consists of 4 steps:

- Creating the copies of configuration files (see remarks of 4.2.2)
- Uninstalling your old SP client software (see 4.3)
- Reinstalling the new version from the SP client software (see 4.1)
- Restoration of configuration files from the copies made at the beginning at the place of SP client reconfiguration.

10.2 I want to access the backed up data of a Linux server from my Windows notebook.

Depending on the SP, Windows, and Linux versions installed, the attempt can lead to very malicious problems, so data loss may be expected. Windows uses a different character encoding and communicates some Windows-specific information to the SP server. The node is then locked for access from Linux. Unlocking the node then requires manual intervention in the server's internal database. The resulting side effects cannot be estimated.

10.3 I want to replace a Linux machine and want to access the data of another Linux machine I manage from the command line. How can I do this?

10. General tips

The `dsmc` option `-virtualnodename=<Other Node_Name>` allows you to access the data of the node named `Other Node_Name` from your node. However, you must know the password to do this, use the same SP client version, and use the same character encoding.

Example: Access to node `N1` with the data on SP server instance `S12` from host `N2` with the data on SP server instance `S22`:

```
dsmc -se=S12 -virtualnodename=N1
```

Write access by a newer SP client may cause an older SP client to be unable to access the data or to access it correctly.

10.4 On Scientific Linux, your instructions for setting up the SP scheduler do not work. How can I get the scheduler to work?

Scientific Linux is not fully supported by SP, so our *Best Practice Guide* is based on SuSE Linux. The Linux distributions differ in many details, e.g. in how the scripts are controlled when starting the computer. E.g. under Scientific Linux adding the entry as described in Section 5.1.1.6

```
TSM::once:/pfad/zu/dsmc sched > /dev/null 2>&1
```

entry in the `/etc/inittab` file has no effect if it also says to read:

```
ADDING OTHER CONFIGURATION HERE WILL HAVE NO EFFECT ON YOUR SYSTEM.
```

The following example of a `dsmsched-init` script may be helpful to start the SP scheduler:

```
-----
#!/bin/sh

### BEGIN INIT INFO
# Provides: dsmcsched
# Required-Start: $network $remote_fs
# Required-Stop: $network
# Default-Start: 3 5
# Default-Stop: 3 5
# Description: Start ADSM/SP scheduler.
### END INIT INFO

PATH=/bin:/usr/bin:/usr/local/bin:/usr/local/adsm:$PATH
DSM_LOG=/tmp
export DSM_LOG
export LANG=de_DE

return=$rc_done

OPTS="--schedlog=/tmp/dsmsched.log --errorlog=/tmp/dsmsched.err"

case "$1" in
    stop )
        echo -n "Stopping ADSM scheduler now! ..."

```

10. General tips

```
rc.dsmc stop -server=local 1>/dev/null 2>>/tmp/dsmcsched.err
echo -e "$return"
;;
start )
echo -n "Starting ADSM in 5 sec"
for i in 1 2 3 4 5; do
    echo -n "."
    sleep 1
done
echo -n " Please wait ..."
rc.dsmc start $OPTS -server=local 1>/dev/null \
2>>/tmp/dsmcsched.err &
echo -e "$return"
;;
* )
echo $0: unknown command: $1 >&2
;;
esac
-----
```

This script should be placed in the `/etc/init.d` `platziert` folder and made executable. On SuSE Linux, you can then execute the `insserv dsmsched` commando. This commando will include `dsmsched` in the `Init` procedure.

For RedHat offshoots, which include Scientific Linux, the entry for `dsmsched` should be made in the `/etc/rc.local` or the soft links in the `/etc/init.d/rc3.d` and `/etc/init.d/rc5.d` folders should be created manually, pointing to the `/etc/init.d/dsmsched` script.

The script shown above is an example. The values set for the `PATH`, `DSM_LOG` and `LANG` variables should be set differently on your system.

10.5 SP Client and NAS Backup on Windows 7, 8 and 10

How to back up a NAS partition on a Windows 7, 8 or 10 or Windows Server 2008/R2, 2012/R2 and 2016 that is not a domain machine?

1. Local user must be administrator and backup operator.
2. The user with whom is logged on the computer must be added to the Backup operators and Administrators group (local administrator) -> settings are applied only after restarting the computer.
3. The following must be added to the `dsm.opt` file:

```
INCLUDE "<NAS SHARE>" STANDARD
DOMAIN "<NAS SHARE>"
SKIPNTPERMISSIONS YES
SKIPNTSECURITYCRC YES
```

E.g.

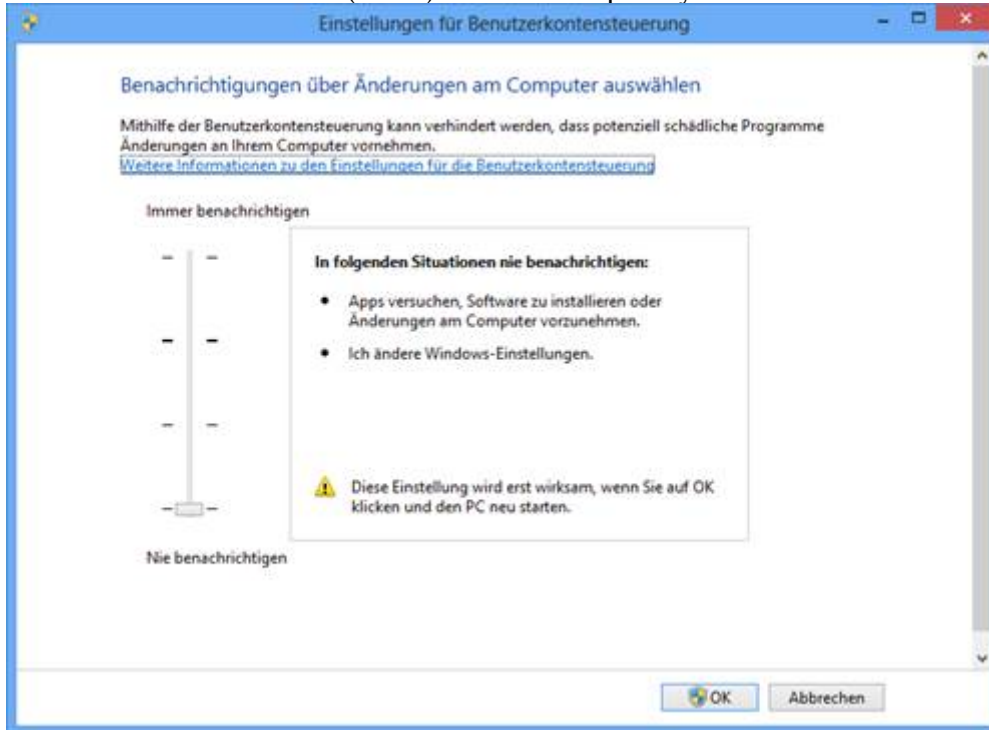
```
INCLUDE "\\nas.ads.mwn.de\al23456" STANDARD
```

10. General tips

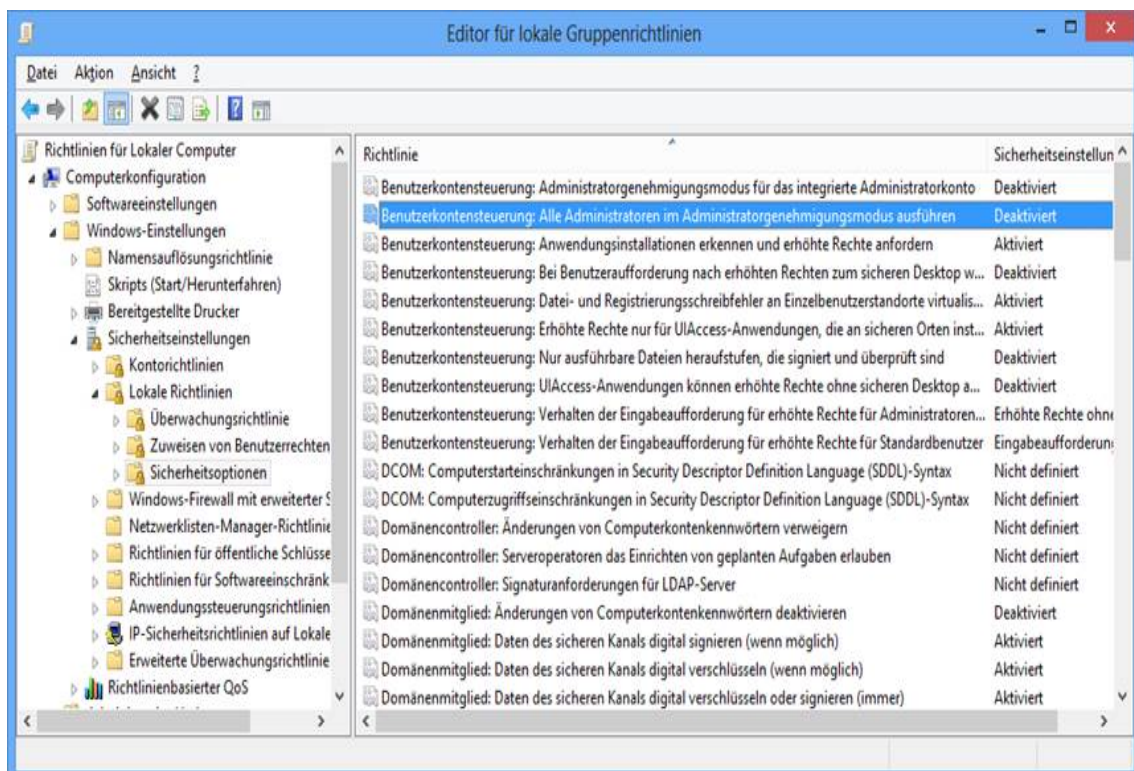
```
DOMAIN "\\nas.ads.mwn.de\a123456"  
SKIPNTPERMISSIONS YES  
SKIPNTSECURITYCRC
```

YES

4. Connect network drive and save identifier and password.
5. user account control (UAC) must be completely disabled:



6. In the local group policies in the security options: *Benutzerkontensteuerung: Alle Administratoren im Administratormodus ausführen* set to *deaktiviert*.



Now the network drive should be listed in the TSM settings in the Domain List (Edit -> Client Preferences -> Backup).

Despite these settings it can happen (especially under Windows 10) that the network drive is not shown during a manual backup/archive via the GUI (under Network).

If it is not displayed, the network drive can only be backed up manually via the ISP commandline or via the Action -> Backup Domain function (note here the backup is started with the dsm.opt config and corresponds to the scope of the automatic backup).

Otherwise you can use the TSM Preview function to check if the network drive is backed up (Utilities -> Preview Include-Exclude).

10.6 How can you use a non "Default Management Class", e.g. B10V or B7V7D?

The control of management classes (MGM) is controlled in SP by the include/exclude list using "include" statement.

The explicit specification of the management class is done according to the file specification. Without explicit specification the so called "Default Management Class" is used.

At the LRZ this is called STANDARD

Example of a line from inclexcl file:

```
include /home/.../*          # <- is saved to the default MGM
                             "STANDARD", i.e. 3 versions 180 days.
```

```
include /home/.../* STANDARD # <- the same as the line above only explicitly
                             written out = will be saved to the default MGM
                             "STANDARD", i.e. 3 versions 180 days.
```

```
include /home/.../* B10V    # <- saved to the "B10V" MGM,
                             i.e. 10 versions 180 days.
```

```
include /home/.../* B7V7D   # <- saved to the "B7V7D" MGM,
                             i.e. 7 versions 7 days.
```

You can check your inclexclude list with the following command:

```
Q INCLEXCLUDE
```

You can find out how the files are saved with the help of PREVIEW command:

```
PREVIEW BA <Dateispezifikation>
```

E.g.

PREVIEW BA "/tmp/My_File"

You can find out how the files have already been backed up with the following command:

Q BA <Dateispezifikation> (-SUBDIR=YES) -DETAIL

E.g.

Q BA "/tmp/MEINE_DATEI" -DETAIL

or

Q BA "/tmp/MEINE_DIR/" -SUBDIR=YES -DETAIL*

The following command can be used to list the available management classes:

Q MGM -DETAIL

10.7 Encryption

I have partly very sensitive data and would like to backup this data encrypted automatically via SP-Schedule. How do I configure this and how can I verify that the data is actually backed up encrypted?

Setting up encryption

Setting up SP encryption consists of three steps:

1. Allow *Encryption* in client option file `dsm.opt` (Windows) and in client system option `dsm.sys` (Linux). Two lines must be inserted for this:

```
encryptkey <Keytype>  
ENCRYPTIONTYPE <Type>
```

`Keytype` has one of the `prompt`, `save` or `generate` values.

`Type` has one of the `AES256`, `AES128` or `DES56` values

`Keytype=save` is only valid, when

```
passwordaccess generate
```

is set and the encrypted backup is necessary for the SP-Scheduler.

E.g.

```
passwordaccess generate  
encryptkey save  
ENCRYPTIONTYPE AES128
```

2. In the `incl excl` file, insert the specification for the objects to be encrypted.

10. General tips

```
include.encrypt <Specification>
```

E.g.

```
include.encrypt /tmp/Encrypt/*
```

3. Encryption password must be entered.

Start the SP client and back up a file from one of your directories that should be backed up encrypted. At the first encrypted backup SP will request the encryption password and store it encrypted in the file `TSM.PWD`.

Important note: In case of loss of the encryption password there is no possibility to recover the data. For this reason, keep the encryption password safe.

Verify encryption

1. In the command line

```
dsmc query backup <File specification> -subdir=yes -detail
```

E.g.

```
dsmc query backup /tmp/Encrypt/d -detail
```

outputs the detailed information about the file (including encryption type).

The output then looks like this:

Größe	Sicher.-Datum	Verw.klasse	A/I	Datei
----	-----	-----	---	-----
72 B	25.02.2013 13:44:56	DEFAULT	A	/tmp/Encrypt/d

Geändert: 25.02.2013 13:35:17 Zugriffen: 25.02.2013 13:35:17

Komprimiert: NEIN Verschlüsselungstyp: 128-Bit-AES

Vom Client dedupliziert: NEIN

or for a non-encrypted file:

Größe	Sicher.-Datum	Verw.klasse	A/I	Datei
----	-----	-----	---	-----
72 B	18.02.2013 13:51:34	DEFAULT	A	/tmp/Encrypt/d

Geändert: 18.02.2013 13:51:28 Zugriffen: 18.02.2013 13:49:39

Komprimiert: NEIN Verschlüsselungstyp: Keine

2. Graphical client

Select a file that you have backed up encrypted. Right-click to get "File information" from the menu. Among other things, the encryption type is displayed:

10. General tips

Encryption type: 128-Bit-AES

for the upper example, if everything has been configured correctly.

Encryption type: NONE

if no encryption has been done on the SP side.

10.8 Restore of data to a specific point in time

I want to restore the versions of my backup data so that they correspond to the state from a certain point in time. How can I do this?

For this type of recovery, the graphical client is advantageous. Under Windows it is used by default. On Linux, this client is started with the `dsmj` command.

Select *Zurückschreiben*. The corresponding *Zurückschreiben* program is then started. Next to the *Optionen* there is a button *Nach Zeitpunkt*. Click on it, then the *Zurückschreiben nach Datum* menu appears, where you can then specify the time and then select and restore the data to be restored in the *Zurückschreiben* menu.

10.9 My computer has broken (been stolen). What is the best way to restore the backed up data to a new computer?

Please proceed as follows:

1. Install the SP client on your new computer. Note the following points when doing so:
 1. The SP client version should be the same as on your old machine. If this is not possible, the SP version on the new computer must in no case be older than on the old one. You can ask the SP version from your old computer at the LRZ if you do not remember it.
 2. The operating system on your new computer should remain the same. If this is not possible, a newer version of the operating system should be used. Failure to do so may result in data loss. Especially the exchange between Linux and Windows is very problematic (see above).
 3. The character encoding on the new and old computer should be the same. Otherwise the correct representation of the special characters is not guaranteed.
2. Configure the SP client on your new machine so that the node name and server settings match those on the old machine, as well as the *Include/Exclude* settings (`incl excl` file (Linux), corresponding section of the `dsm.opt` (Windows)). If you don't remember the *Include/Exclude* settings, please first enter only `include *`

10. General tips

If you used the SP client encryption on your old computer, you need to know the encryption password and the specification of the encrypted objects to restore the data. Please then enter your

```
include.encrypt <Specification>
```

in the *Include/Exclude*-settings (see above).

3. Enable the *aktive/inaktive Dateien anzeigen* option. When the SP Client is started on the new machine, it performs the comparison between the data that is on the machine and the data that has been backed up to SP. Since you have replaced the machine, most of the backed up data will not be present on the new machine and will then be considered deleted by the SP client. This data is thus marked as inactive. However, since this matching takes a while, confusingly, one part will be visible as active and one part as inactive. For this reason you have to activate the option *aktive/inaktive Dateien anzeigen*, otherwise you may see your saved data incomplete. To do this, please click on *Zurückschreiben* in the graphical client and then in the menu item *Ansicht* on *aktive/inaktive Dateien anzeigen* or use the `-ina` option in the command line. Only after this activation you can select the older versions and deleted files.

4. Now start restoring your data.

10.10 Related links

[Servicedesk](#)

[Terms of use of the archive and backup system](#)

[SP Client Manual from IBM](#)

[SP FAQs](#)

[SP-Forum](#)

[SP-Supportmatrix](#)