Spectrum Protect (SP)

Best Practice Guide

Version 1.05

Dr. Alexander Dunaevskiy, Stephan Peinkofer

1 Einführung

1.1 Wichtigste Neuerungen zur vorherigen Verson 1.03

TSM (= *Tivoli Storage Manager*) wurde ab Version 7.1.3 in ISP (= IBM Spectrum Protect) oder einfach in SP (= Spectrum Protect) umbenannt. Diese Umbenennung ist Marketing-Überlegungen von IBM geschuldet und nicht einer grundlegenden Änderung der Funktionsweise der Software. In einigen Beispielen mit älteren Versionen wird TSM ansonsten SP verwendet.

Security Layer von SP Server und Client wurde parallel in der 8.X (ab 8.1.2) und 7.X (ab 7.1.8) Version komplett neugestaltet. Das hat deutliche Auswirkungen auf Kompatibilität der veralteten TSM/SP Clients zu den neuen Server-Versionen, vor allem auf die Kommunikation zwischen Server und Client und auf die Sicherung durch die nicht administrativen User.

1.2 Ihre Meinung ist uns wichtig

Wenn Sie Fragen, Anregungen, Kritik, Verbesserungsvorschläge oder andere Wünsche zu diesem *Best Practice Guide* haben, würden wir uns sehr darüber freuen, wenn Sie uns Ihr Feedback über den Servicedesk *Service: Datenhaltung – Archiv und Backup* mit dem Betreff *BPG Feedback* zukommen lassen.

1.3 SP-Nutzungsbedingungen des LRZ

Die aktuellen Nutzungsbedingungen des Archiv- und Backup-Systems des LRZ finden Sie unter: https://doku.lrz.de/display/PUBLIC/Benutzungsrichtlinien

1.4 Zweck dieser Anleitung

Wie bei vielen großen IT-Anwendungen führen auch bei SP (= *IBM Spectrum Protect*) viele Wege zum Ziel. Diese Anleitung soll Ihnen zeigen, wie man Backup und Archivierung SP am besten konfiguriert und durchführt. Unsere Empfehlungen basieren auf der langjährigen Erfahrung des LRZ mit SP und entsprechen der Vorgehensweise, wie das LRZ selbst das Backup und die Archivierung seiner Daten bewerkstelligt. Sie können in vielfacher Weise davon profitieren, wenn Sie sich an die LRZ-Empfehlungen halten:

- Sie vermeiden von vornherein die häufigsten Konfigurations- und Bedienungsfehler des SP-Clients.
- Falls es doch zu Problemen kommt, kann Ihnen das LRZ in der Regel schneller helfen, da das Überprüfen der Konfiguration einfacher ist.
- Falls die LRZ-Mitarbeiter ein Problem nicht selbst lösen können und ihre Konfiguration unterstützt ist, kann das Problem an den Tivoli-Software-Support weitergegeben werden.
- Sie ersparen sich selbst und dem LRZ unnötige Arbeit und Probleme.
- Sie erhöhen die Sicherheit Ihrer Daten.

Dem LRZ ist bewusst, dass Ihre IT-Struktur und Anforderungen nicht immer mit unseren Empfehlungen vereinbar sind. In diesem Fall sollten Sie auf jeden Fall Rücksprache mit dem LRZ halten, damit wir gemeinsam eine Lösung für Sie finden können. Bei groben, nicht mit dem LRZ abgesprochenen Abweichungen von unseren Empfehlungen kann es vorkommen, dass Ihre Konfiguration von IBM/Tivoli nicht unterstützt wird. In diesem Fall kann Ihnen

gegebenenfalls auch das LRZ nicht helfen. Im schlimmsten Fall kann dies Datenverlust für Sie bedeuten.

Diese Anleitung beschreibt die wichtigsten Eigenschaften und Funktionen für Windows- und Unix-Betriebssysteme, wobei Linux u.a. Unix-ähnliche, POSIX folgende Betriebssysteme viele Gemeinsamkeiten aufweisen. Die Erläuterungen beziehen sich auf SuSE Linux, wenn nichts anderes angegeben ist

1.5 Wichtige Verhaltensregeln

Dos

- Beachten Sie die Nutzungsbedingungen des LRZ.
- Testen Sie die SP-Konfiguration (siehe Kapitel 6) regelmäßig.
- Teilen Sie signifikante Änderungen des geplanten Datenvolumens (d.h. Speicherplatzbedarf) und der Dateianzahl dem LRZ mittels des Servicedesks *Service: Datenhaltung – Archiv und Backup* mit.
- Und teilen Sie organisatorische Änderungen (Ansprechpartner, etc.) ebenfalls dem LRZ mittels des Servicedesks *Service: Datenhaltung – Archiv und Backup* mit.

Don’ts

- Definieren Sie nicht mehr als 100 Filespaces (siehe Abschnitt 2.1.7).
- Speichern Sie nicht mehr als 10 Millionen Dateien in einem Node.
- Speichern Sie nicht mehr als 20 Terabyte in einem Node.
- Starten Sie nicht viele hundert Wiederherstellungen einzeln.

1.5 SP-Supportmatrix

In unserer SP-Supportmatrix finden Sie die für ihr Betriebssystem empfohlene SP-Client-Version.

Hinweis: Das LRZ kann Ihnen nur Hilfestellung leisten, solange Sie eine von IBM unterstützte Systemkonfiguration nutzen. Dies umfasst die Verwendung einer unterstützten Client-Version in Verbindung mit der Einhaltung der Hardware- und Softwareanforderungen. Falls es für Sie triftige Gründe gibt, eine nicht unterstützte Systemkonfiguration zu verwenden (da z.B. kein unterstützter Client für das Betriebssystem mehr verfügbar ist), setzen Sie sich
bitte mit dem LRZ in Verbindung (siehe Kapitel 8).
Seit der Neugestaltung vom Security-Layer von SP (Server Version ab 8.1.2) sind unsere Möglichkeiten Ihnen bei einer nicht unterstützten Systemkonfiguration zu helfen deutlich eingeschränkt.

2 Grundlegende Konzepte und Verfahren von SP

SP basiert auf einer Client-Server-Architektur. Das LRZ hostet die Server. Sie setzen einen Client ein, um Ihre Daten zu sichern und/oder zu archivieren. Der Server speichert Ihre Daten teils auf Festplatten, teils auf Bandkassetten. Bandlaufwerke haben gegenüber Festplatten im Hinblick auf den Energieverbrauch erhebliche Vorteile. Größere Kapazität bei geringeren Kosten sind weitere Vorteile.

2.1 Begriffsdefinitionen

2.1.1 Backup

Regelmäßiges Kopieren von Dateien auf ein dediziertes Speichersystem (Backup-System), um sich gegen Datenverlust im Falle eines Hardware-, System- oder Bedienfehlers auf dem Primär- bzw. Quellsystem (z.B. Server, Arbeitsplatzrechner, usw.) zu schützen.

2.1.2 Restore

Zurückkopieren der gesicherten Version von Dateien vom Backup-System auf das Primär- bzw. Quellsystem. Restore ist das Gegenstück zu Backup.

2.1.3 Archive

Kopieren ausgewählter Dateien auf ein dediziertes Speichersystem (Archiv-System), um sie für längere Zeit sicher aufzubewahren. Die Originaldateien können nach der Archivierung vom Primär- bzw. Ausgangssystem gelöscht werden, um für freien Speicherplatz zu sorgen.

2.1.4 Retrieve

Zurückkopieren archivierter Dateien auf das Primär- bzw. Quellsystem. Retrieve ist das Gegenstück zur Archivierung.

2.1.5 Unterschied zwischen Backup und Archive

Prinzipieller Unterschied zwischen Backup und Archive besteht in der Versionierung:

Backup nutzt Versionierung.

Archive nutzt keine Versionierung.

D.h. wenn man zwei Sicherungen einer Datei mit demselben Namen und selben Pfad macht, werden im Fall von Archive daraus zwei voneinander unabhängige Objekte, im Fall von Backup zwei Versionen eines Objektes. Die Aufbewahrungsregeln für Archive und Backup sind deshalb unterschiedlich aufgebaut und führen zu den typischen Anwendungsmustern für das jeweilige Sicherungsverfahren:

- **Backup**: Daten werden zur Sicherheit kurzfristig (meist in mehreren Versionen) auf einem weiteren Medium gespeichert. Backup-Daten werden z.B. bei Datenverlust zurückgespielt.
- **Archivierung**: Die Daten sollen langfristig und sicher aufbewahrt werden. Im Normalfall wird auf archivierte Daten wieder zugegriffen werden.

2.1.6 Node

Ein Node stellt eine Verwaltungseinheit von SP dar. Im Regelfall entspricht ein Node genau einem Computersystem, das gesichert oder von dem aus archiviert werden soll. Allerdings können sich auch mehrere Computersysteme einen Node teilen, wenn alle Computersysteme

kompatible Betriebssysteme mit derselben Zeichenkodierung verwenden. Ein Computersystem kann auch mehrere Nodes nutzen. Egal ob das Archiv oder das Backup verwendet wird, ab einer Datenmenge von 20TB oder Dateianzahl von 10 Millionen Dateien müssen die Daten auf mehrere Nodes verteilt werden.

2.1.7 Filespace

Ein Filespace ist eine untergeordnete Verwaltungseinheit eines Node. Hier werden Gruppen von Dateien zusammengefasst. Diese Gruppen sind wie folgt definiert:

- **Windows:** Alle Dateien, die gemeinsam auf einer Partition liegen, gehören zu einem Filespace. Die Filespaces werden anhand der sogenannten *Universal Naming Convention* bei fest eingebauten Medien und anhand des Datenträger-/ Volume-Namens bei Wechselmedien unterschieden.
- **Linux:** Alle Dateien, die gemeinsam auf einem Dateisystem liegen, gehören im Normalfall zu einem Filespace. Zusätzlich hat man die Möglichkeit, ein Dateisystem durch Angabe von sogenannten v*irtuellen Mountpoints* in mehreren Filespaces zu organisieren.

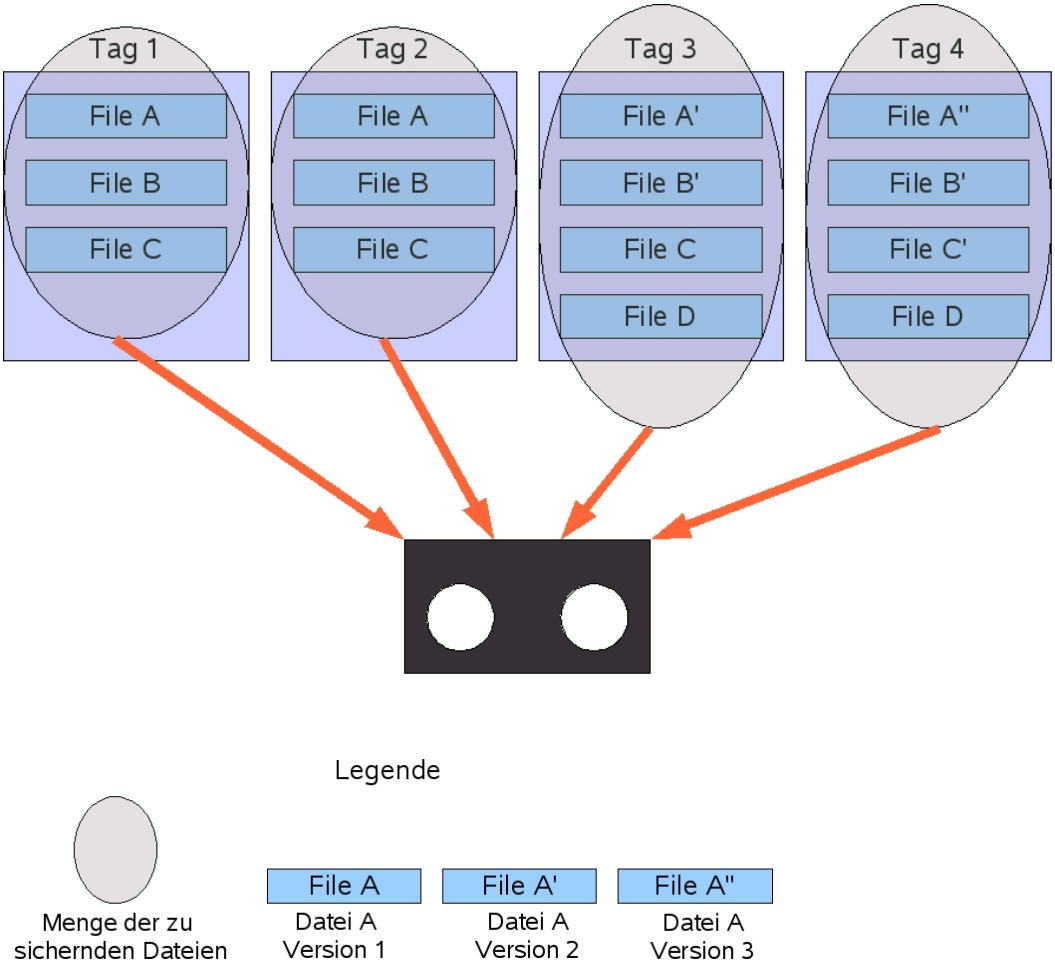
2.2 Backup mit SP

2.2.1 Backup-Strategien im Überblick

Im Folgenden werden die drei grundlegenden Strategien für Backup vorgestellt.

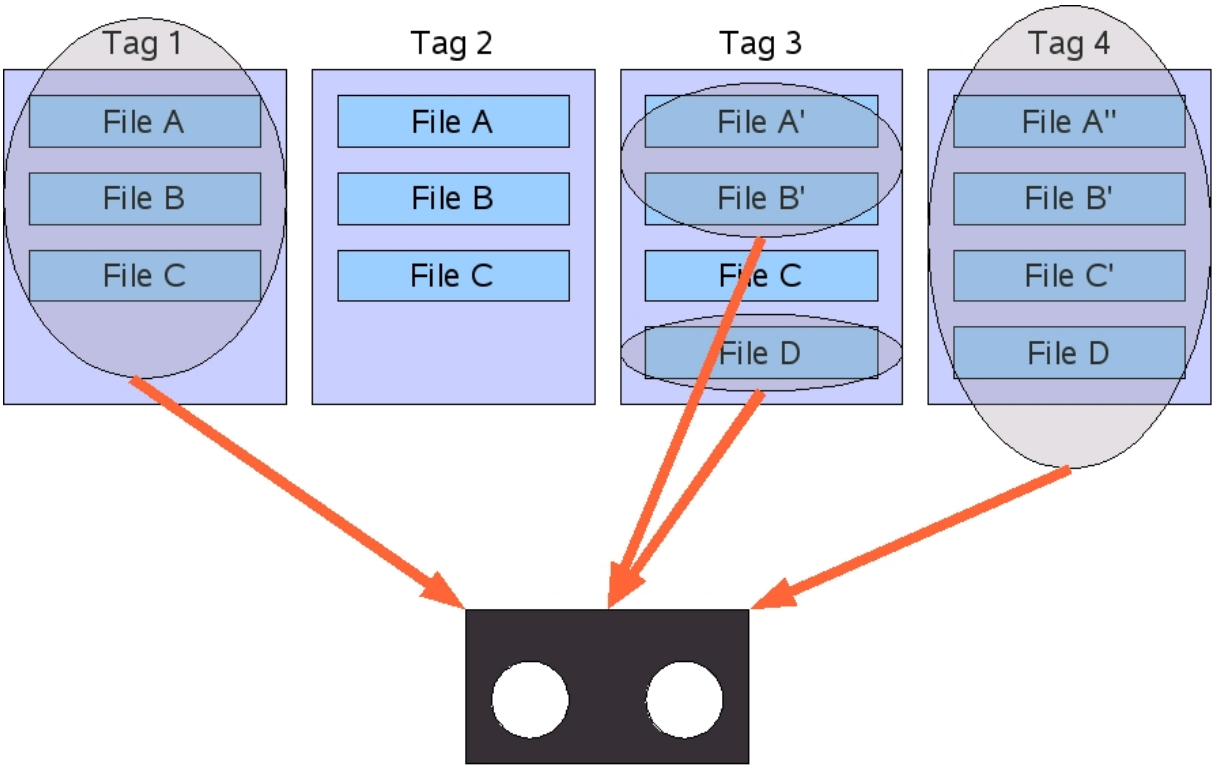
2.2.1.1 Vollständiges Backup

Beim vollständigen Backup werden bei jedem Backup-Vorgang immer alle Dateien (ausgenommen Dateien in einer *Exclude*-Liste) gesichert. Das hat den Vorteil, dass bei einem Datenverlust immer nur das letzte Backup zurückgespielt werden muss. Der Nachteil dieser Strategie ist, dass immer alle Dateien übertragen und gespeichert werden müssen, auch wenn sie sich seit dem letzten Backup-Vorgang nicht verändert haben und somit schon in der aktuellsten Version auf dem Backup-System vorhanden sind. Daraus resultieren lange Backup-Zeiten, hoher Speicherplatzverbrauch durch Redundanzen und eine hohe Netzlast.



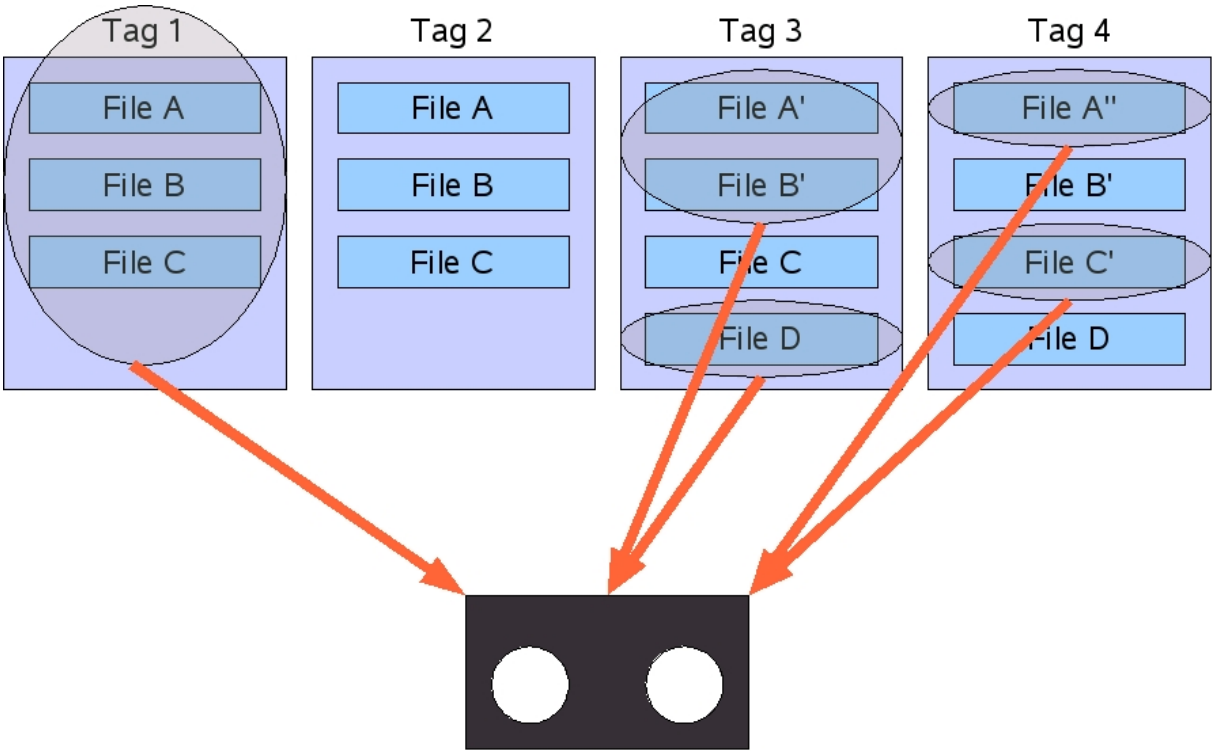
2.2.1.2 Differenzielles Backup

Beim differenziellen Backup werden bei jedem Backup-Vorgang nur die Dateien gesichert, die seit dem letzten vollständigen Backup verändert oder neu erstellt wurden. Der Vorteil dieser Strategie ist, dass nicht jedes Mal alle Dateien übertragen und gespeichert werden müssen. Bei einem Datenverlust wird das letzte vollständige Backup zurückgespielt und danach das letzte differenzielle Backup. Betrachtet man die benötigte Backup-Zeit und den Speicherplatzverbrauch, ist diese Methode noch nicht optimal, da eine einmal geänderte Datei bei jedem differenziellen Backup solange immer wieder mit übertragen und gespeichert wird, bis das nächste vollständige Backup erfolgt.



2.2.1.3 Inkrementelles Backup

Beim inkrementellen Backup werden mit jedem Backup-Vorgang nur die Dateien gesichert, die seit dem letzten Backup-Vorgang (egal ob vollständig oder inkrementell) verändert oder neu erstellt wurden. Der Vorteil dieser Strategie ist, dass sie optimal im Hinblick auf Backup-Zeit und Speicherplatzverbrauch ist. Der Nachteil dieser Strategie ist die längere Dauer eines Restores, da alle inkrementellen Backups in der Reihenfolge ihrer Entstehung zurückgespielt werden müssen.



Im Folgenden sind die Vor- und Nachteile der drei Backup-Methoden zusammengefasst:

	Speicherplatzbedarf	Netzlast	Backup-Zeit	Restore-Zeit
Vollständiges Backup	-	-	-	+
Differentielles Backup	o	o	o	o
Inkrementelles Backup	+	+	+	-

2.2.2 Arbeitsweise von Backup-Software

Im Prinzip arbeitet jede Backup-Anwendung nach einer Strategie oder einer Kombination von Strategien, wie im vorangegangenen Abschnitt dargestellt. Betriebliche Backup-Systeme verwenden meist eine Kombination aus vollständigem und differentiellem oder aus vollständigem und inkrementellem Backup.
Die Restore-Prozedur von differenziellen und inkrementellen Backups ist sehr aufwendig, da mehrere Backups nacheinander zurückgespielt werden müssen. Um dieses Problem zu lösen, nutzen höher entwickelte Backup-Anwendungen eine Datenbank, in der sie unter anderem speichern, wo sich eine bestimmte Version einer Datei befindet (d.h. auf welchem Magnetband

und an welcher Position auf dem Band). Dadurch muss die Backup-Anwendung nicht den gesamten Restore-Zyklus durchlaufen, sondern kann direkt auf die gewünschte Version der Datei zugreifen. Dieses Vorgehen bringt natürlich eine enorme Zeitersparnis mit sich.

2.2.3 Das Backup-Verfahren von SP

Wie bereits erwähnt, arbeiten viele Backup-Anwendungen nach der *Full & Differential*- oder *Full & Incremental*-Strategie. Nicht so SP: SP führt ausschließlich inkrementelle Backups durch. Das bedeutet, dass SP nur ein einziges Mal eine Vollsicherung durchführt, nämlich beim ersten Backup-Vorgang. Bei allen weiteren Sicherungsläufen wird immer nur die Änderung zum vorhergehenden Sicherungslauf gesichert. Diese Backup-Methode wird auch als progressiv oder *Incremental Forever* bezeichnet. Um eine zu hohe Fragmentierung der Daten im Backup-System zu verhindern, stellt SP diverse Mechanismen bereit, die sicherstellen, dass die Daten eines Nodes auf möglichst wenige Bänder verteilt werden.

2.2.4 Die Versionsverwaltung von SP

Auch beim inkrementellen Backup von SP werden alle neuen Versionen von geänderten Dateien gespeichert. Diese verschiedenen Versionen derselben Datei werden aus Kostengründen im Allgemeinen nicht für immer, sondern nur für einen gewissen Zeitraum aufbewahrt; im Falle eines Datenverlusts möchte man schließlich in der Regel nur die aktuellste Version einer Datei zurückholen. Natürlich kann es vorkommen, dass z.B. eine Datei versehentlich überschrieben wurde und dass dies erst nach einigen Tagen bemerkt wird, wenn es ist auch unwahrscheinlich ist, dass so etwas erst nach einem längeren Zeitraum auffällt.
Anders als bei einigen anderen Backup-Anwendungen kann man bei SP nicht nur einstellen, wie lange eine bestimmte Version einer Datei aufbewahrt werden soll, sondern auch, wie viele Versionen einer Datei überhaupt aufbewahrt werden. Hinzu kommt, dass SP die auf dem Quellrechner gelöschten Dateien bei der Versionierung anders behandelt als die auf dem Quellrechner noch vorhandenen Dateien.
Bevor wir uns genauer mit der Arbeitsweise der SP-Versionierung beschäftigen, sind noch zwei SP-spezifische Begriffe zu klären, die der aktiven und der inaktiven Version einer Datei:

- In SP wird die aktuellste Version einer Datei, die auf dem Quellrechner noch existiert, als *aktive Version* bezeichnet.
- Alle alten Versionen einer Datei und auch die aktuellste Version einer Datei, die auf dem Quellrechner gelöscht wurde, werden als *inaktive Version* bezeichnet.

Das Verhalten der SP-Versionierung wird durch die folgenden vier Parameter gesteuert:

- `Versions Data Exists` gibt an, wie viele Versionen einer auf dem Quellrechner noch vorhandenen Datei gespeichert werden.
- `Versions Data Deleted` gibt an, wie viele Versionen einer auf dem Quellrechner gelöschten Datei gespeichert werden. Dieser Parameter ist immer kleiner oder gleich dem Wert von `Versions Data Exists`.
- `Retain Extra Versions` gibt an, wie lange eine inaktive Version einer Datei im Backup-System gespeichert wird, bevor sie gelöscht wird. Dieser Parameter gilt nicht für die letzte auf dem Backup-System verbliebene inaktive Version einer Datei.

- `Retain Only Version` gibt an, wie lange die letzte auf dem Backup-System verbliebene inaktive Version einer Datei gespeichert wird, bevor sie endgültig gelöscht wird.

Hinweise:

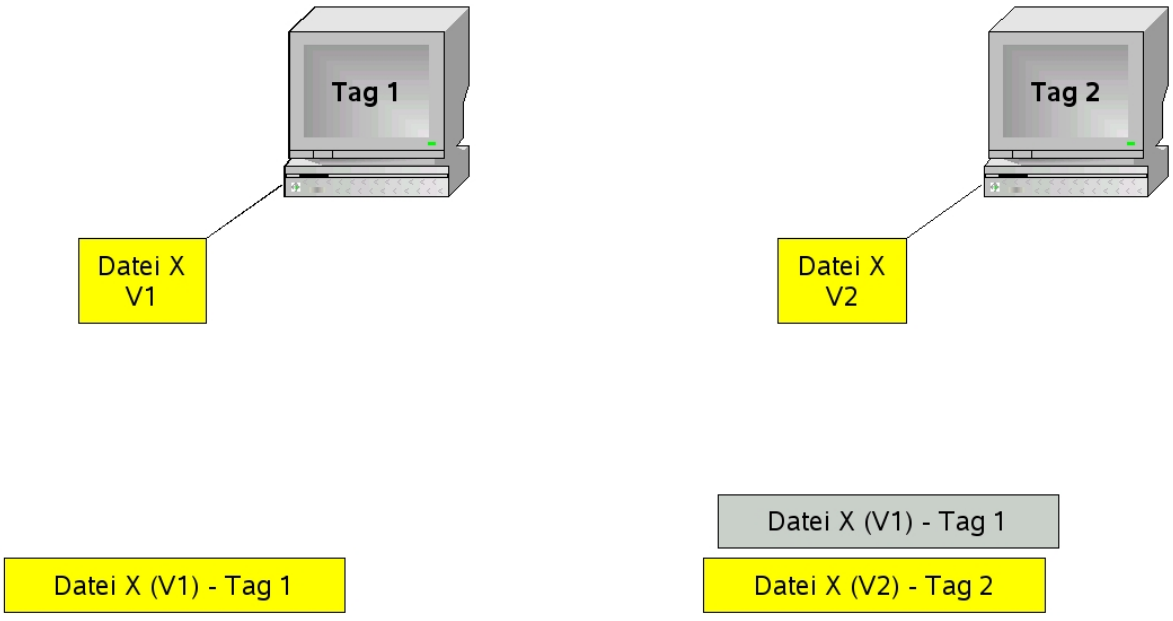
- Die aktive Version einer Datei wird nie vom Backup-System gelöscht.
- Die oben genannten Parameter können nicht vom Benutzer verändert werden, sondern sind vom LRZ vorgegeben.

Folgendes Beispiel soll helfen, die Wirkungsweise der Parameter besser zu verdeutlichen. Nehmen wir an, ein Benutzer sichere jeden Tag einmal die Datei X. Es seien folgende (fiktive) Einstellungen gegeben:

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

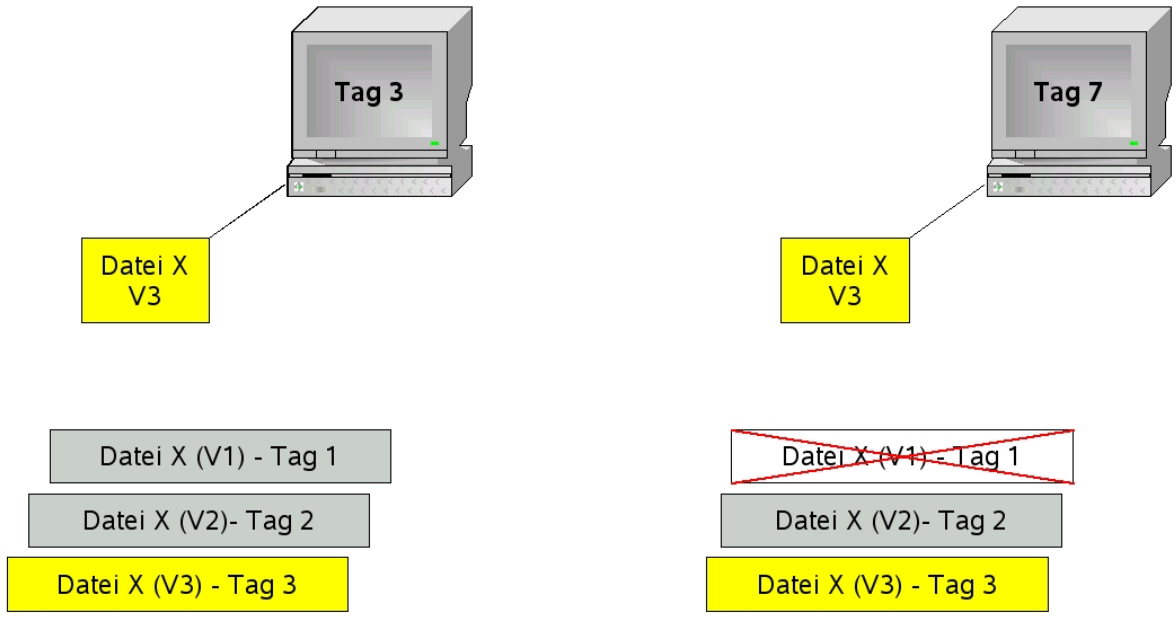
Die tatsächlichen Werte Ihres Systems können Sie mit dem folgenden Kommando herausfinden:

```
dsmc query mgmt -detail
```



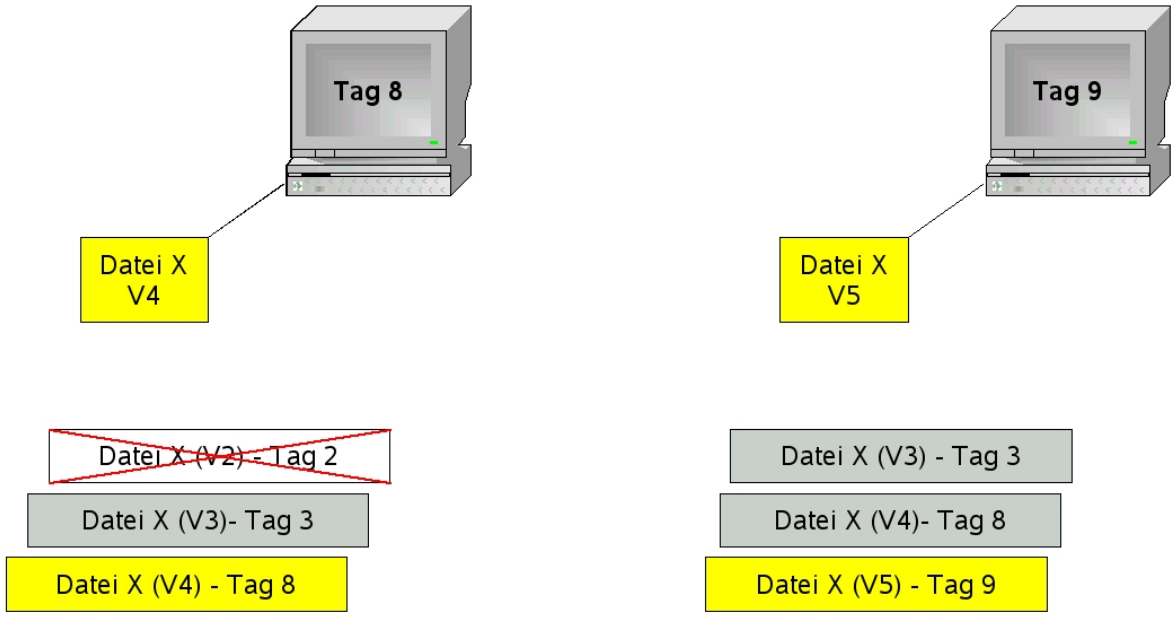
1. Tag: Eine Kopie der Datei X wird im Backup-System als aktive Kopie in Version V1 angelegt.

2. Tag: Durch Ändern der Datei X wird im Backup-System eine neue Kopie der Datei angelegt, wobei die alte Version V1 auf inaktiv und die neue Version V2 auf aktiv gesetzt wird.



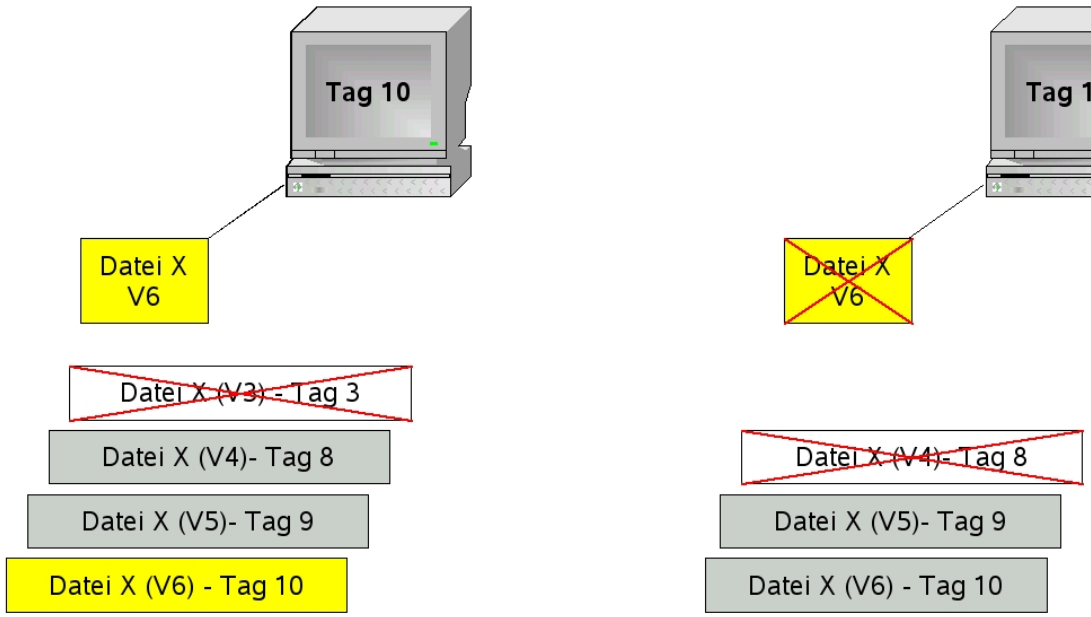
3. Tag: Durch weiteres Ändern der Datei X wird im Backup-System eine weitere Kopie der Datei angelegt, wobei die vorherige, aktive Version V2 auf inaktiv und die neue Version V3 auf aktiv gesetzt wird.

7. Tag: Da die Version V1 der Datei X bereits 5 Tage (Tag 2 bis Tag 6) im inaktiven Zustand war, wird sie aufgrund des eingestellten Parameters `Retain Extra Versions` (inaktive Dateien werden 5 Tage aufbewahrt) gelöscht.



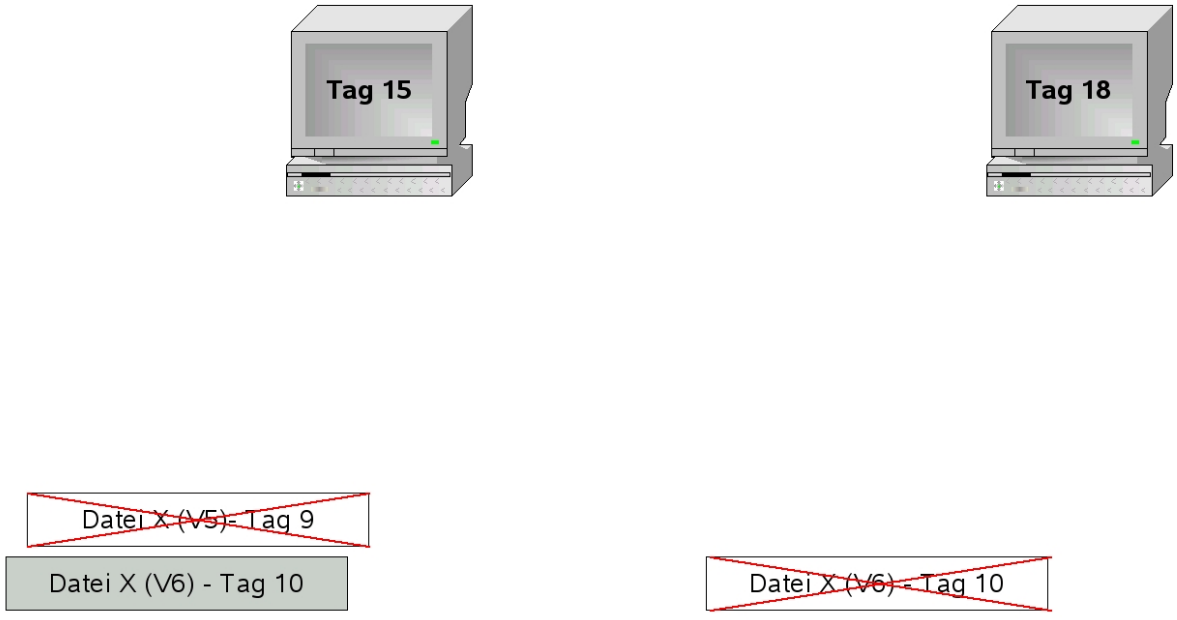
8. Tag: Datei X wird erneut verändert (V3 wird inaktiv, V4 aktiv gesetzt). Da Version V2 der Datei X bereits 5 Tage (Tag 3 bis Tag 7) im inaktiven Zustand war, wird sie aufgrund des eingestellten Parameters `Retain Extra Versions` (inaktive Dateien werden 5 Tage aufbewahrt) gelöscht.

9. Tag: Durch Ändern der Datei X wird im Backup-System eine erneute Kopie der Datei angelegt, wobei die alte aktive Version V4 auf inaktiv und die neue Version V5 auf aktiv gesetzt wird.



10. Tag: Durch Ändern der Datei X wird im Backup-System eine erneute Kopie der Datei angelegt, wobei die vorherige aktive Version V5 auf inaktiv und die neue Version V6 auf aktiv gesetzt wird. Da die Version V3 der Datei die älteste inaktive Kopie ist und durch den Parameter `Versions Data Exists` vorgegeben ist, dass maximal 3 Versionen einer Datei aufbewahrt werden, wird diese Version gelöscht.

11. Tag: Durch Löschen der Datei X auf dem Quellrechner wird die aktive Version V6 der Datei auf inaktiv gesetzt und die Version 4 der Datei auf dem Backup-System gelöscht, da durch den Parameter `Versions Data Deleted` vorgegeben ist, dass maximal die 2 aktuellsten Versionen einer gelöschten Datei aufbewahrt werden.



15. Tag: Da die Version V5 der Datei X bereits 5 Tage im inaktiven Zustand war, wird sie aufgrund des Parameters `Retain Extra Versions` vom Backup-System gelöscht.

18. Tag: Da die Version 6 der Datei X bereits 7 Tage im inaktiven Zustand war, wird sie aufgrund des Parameters `Retain Only Versions` vom Backup-System gelöscht.

2.2.5 Regelmäßige automatische Backups mit SP

Um mit SP regelmäßig automatische Backups durchzuführen, gibt es im Prinzip zwei Verfahren:

1. Verwenden des SP-Scheduler-Programms
2. Aufruf des SP-Backup-Kommandos mit einem anderen z.B. betriebssystemeigenen Scheduler also `cron` unter Linux oder den „geplanten Tasks“ unter Windows.

Das LRZ empfiehlt die erste Variante: Verwendung des SP-Scheduler-Programms:

> Das SP-Scheduler-Programm basiert auf einem Zeitfensterverfahren. Das bedeutet, dass die Sicherung nicht zu einem genauen Zeitpunkt startet, sondern in einem gewissen Zeitfenster. Dieses Verfahren ist in der Regel zuverlässiger, da, falls beim ersten Startversuch Fehler auftreten, SP versuchen wird, das Backup zu einem späteren Zeitpunkt innerhalb des Fensters erneut zu starten. Die Startzeit des Backups wird der aktuellen Lastsituation des Backup-Systems angepasst. Daraus resultiert für die Applikation eine optimierte Backup-Zeit.

2.3 Vergleich: Archivierung und Backup bei SP

Die SP-Archive-Funktion dient im Gegensatz zur Backup-Funktion der längerfristigen Speicherung von Daten. Der Hauptzweck der Archive-Funktion ist, dem Benutzer die Möglichkeit zu geben, Dateien, die nicht ständig benötigt werden, auszulagern und sie sicher aufzubewahren. Die Arbeitsweise der Archivierung unterscheidet sich dabei deutlich von der Arbeitsweise des Backups. Diese Unterschiede sind in der folgenden Tabelle zusammengefasst:

	Backup	**Archivierung**
Varianten	vollständig, differenziell oder inkrementell oder eine Kombination der drei Basisarten	immer vollständig
Beschränkung der Versionsanzahl einer Datei	ja `Versions Data Exists`	nein
Versionsverwaltung	festgelegt durch `Retain Only Version` für die letzte inaktive Version einer Datei, durch `Retain Extra Versions` für alle übrigen inaktiven Versionen	festgelegt für alle inaktiven Versionen einer Datei durch `Retain Version`
Verhalten bei gelöschten Dateien	letzte gespeicherte Dateiversion wird als inaktiv markiert	keine Auswirkung

Da Archivdateien vom Quellsystem gelöscht werden können, bis diese wieder benötigt werden, trifft das LRZ für diese Daten besondere Vorkehrungen, um die Wahrscheinlichkeit eines Datenverlusts so gering wie möglich zu halten. Aus Sicherheitsgründen werden alle Archivdateien nicht nur im Archivsystem des LRZ, sondern auch im Archivsystem eines anderen Rechenzentrums gespeichert. Jedoch dauert es je nach Datenaufkommen bis zu 4 Wochen, bis die Zweitkopie angelegt wird. Daher empfehlen wir Ihnen, archivierte Daten frühestens nach 4 Wochen vom Quellsystem zu löschen.

Der Archivierungsdienst des LRZ dient der längerfristigen Aufbewahrung von Daten aus dem Bereich der Forschung und Lehre. Eine Verwendung zur Speicherung von Daten anderer Art, insbesondere von Systemdateien von Rechnern, wird vom LRZ nicht unterstützt, da für die Sicherung dieser Daten die Verwendung der Backup-Funktion viel sinnvoller ist.

3 Planung der SP-Konfiguration

Bevor Sie Daten beim LRZ sichern oder archivieren, sollten Sie sich Gedanken über die Konfiguration Ihres Backup- und Archiv-Clients machen. Das folgende Kapitel zeigt Ihnen, welche Fragen Sie sich selbst auf jeden Fall beantworten sollten, bevor Sie mit dem Backup bzw. der Archivierung beginnen.

3.1 Grundlegende Überlegungen

3.1.1 Backup oder Archivierung oder beides?

Die erste Frage, die Sie sich stellen sollten, ist, ob Sie das SP-System für Backup oder Archivierung benutzen wollen. Obwohl Sie in der Regel mit jedem SP-Node sowohl Backup als auch Archivierungen durchführen können, ist es unter bestimmten Bedingungen (siehe 3.1.3) sinnvoll oder sogar nötig, dedizierte Nodes für Backups und für Archivierungen zu verwenden. Der Unterschied zwischen Backup und Archivierung wurde bereits im Abschnitt 2.1.5 erläutert.

3.1.2 Was soll gesichert werden?

Eine der wichtigsten Fragen, die Sie sich stellen sollten, ist, was Sie nicht sichern müssen. Dem LRZ ist bewusst, dass es für Sie am komfortabelsten ist, sämtliche Dateien auf Ihrem System zu sichern, und es ist Ihnen auch freigestellt, dies zu tun. „Sicherungsunwürdige“ Dateien von der Sicherung auszuschließen, hat jedoch auch einige Vorteile:

- Sie können die Backup-Zeit drastisch verkürzen.
- Sie können die Restore-Zeit drastisch verkürzen.
- Sie entlasten sowohl Ihre Systeme als auch die des LRZ.
- Sollte der SP-Dienst eines Tages aufgrund von Änderungen der Nutzerordnung für Sie kostenpflichtig werden, sparen Sie sich überflüssige Kosten.

3.1.3 Wie viele Daten können gesichert oder archiviert werden?

Die Information, wie viele Daten Sie sichern oder archivieren werden, ist für die Planung des LRZ sehr wichtig. Nur so können wir Ihnen die bestmögliche Performance und Unterstützung bieten, da wir aufgrund des zu erwartenden Datenwachstums die Nodes auf unserer Serverfarm verteilen.
Das „wie viel“ bezieht sich dabei nicht nur auf das Gesamtvolumen, sondern auch auf die Anzahl der Dateien. Uns ist klar, dass dies oft die am schwierigsten zu beantwortende Frage

ist, da man das Datenwachstum sehr schwer voraussagen kann. Falls Sie mehr als 20 TB oder mehr als 10 Millionen Dateien sichern oder archivieren wollen, sollten Sie folgendes beachten:

Eine Aufteilung in mehrere Nodes oder wenigstens mehrere Filespaces ist ratsam, wenn mehr als 20 TB oder mehr als 10 Millionen Dateien gesichert oder archiviert werden.

Wenden Sie sich bitte rechtzeitig an unseren Servicedesk *Service: Datenhaltung – Archiv und Backup.*

Das hat die folgenden Gründe:

- Je mehr Dateien unter einem Node verwaltet werden, desto langsamer werden die Suchzugriffe auf die SP-Datenbank für diesen Node. Das kann dazu führen, dass SP im schlimmsten Fall für einen kompletten Restore mehrere Tage benötigt.
- Je mehr Datenvolumen unter einem Node verwaltet wird, desto länger dauert eine Node-Verlagerung. Von Zeit zu Zeit muss das LRZ die Daten aller Nodes auf ein neueres System migrieren. Während dieses Migrationsvorgangs sind keine Zugriffe auf den Node möglich und, da eine Migration eines großen Nodes mehrere Tage (bis Wochen) in Anspruch nehmen kann, ist es unter Umständen sinnvoller, mehrere kleinere Nodes nacheinander zu migrieren anstatt eines großen.

3.1.4 Wie oft soll gesichert werden?

Im Normalfall sollten Sie Ihr System jeden Tag einmal sichern. Bei manchen Systemen ist aber eine mehrmalige Sicherung pro Tag nicht zu vermeiden. In diesem Fall sollten Sie wirklich nur „sicherungswürdige“ Dateien sichern, um die Backup-Zeiten möglichst kurz zu halten. Teilweise mag aber auch eine wöchentliche Sicherung Ihrer Daten ausreichend sein. Die Entscheidung der Sicherungshäufigkeit können nur Sie selbst am besten treffen.

3.1.5 Wer darf Sichern und Wiederherstellen?

In der Regel dürfen administrative User, wie root unter UNIX oder Administrator unter WINDOWS, die Sicherung und Wiederherstellung durchführen. Es ist allerdings möglich durch spezifische Konfigurationsanpassung auch den anderen User diese Möglichkeit zu geben. Die Hinweise zur Konfigurationsanpassung finden Sie weiter im Kapitel 5.

3.1.6 Wie vertraulich sind meine Daten?

Eine weitere sehr wichtige Frage, die Sie sich stellen sollten, ist, inwieweit Sie Ihre Daten vor dem Zugriff Dritter schützen müssen. SP bietet Zugriffsschutzmechanismen, die verhindern sollen, dass Dritte auf Ihre Daten zugreifen können. Sie sollten jedoch folgende Punkte beachten:

1. Jeder, der den Node-Namen Ihres Rechners und das dazugehörige Passwort kennt, kann auf die gespeicherten Daten zugreifen. Geben Sie diese Information nicht weiter!
2. Sämtliche Daten, die zwischen älteren Versionen von SP-Client und -Server ausgetauscht werden, gehen in der Standardeinstellung unverschlüsselt über das Netzwerk.

   Die neueren Client und Server Versionen mit der neu gestalteten Security-Layer (der 7. Versionen ab 7.1.8 und der 8. ab Version 8.1.2) kommunizieren hingegen mittels TLS/SSL Verschlüsselung auf der Basis des sehr sicheren AES-Verfahrens.

3. Sämtliche Daten werden standardmäßig unverschlüsselt beim LRZ gespeichert. Allerdings haben im Rechenzentrum nur befugte Mitarbeiter Zugang. Die Datenträger nach Ablauf Ihrer Lebenszeit werden vernichtet.

Der ersten Schwachstelle können Sie entgegenwirken, indem Sie das Anfangspasswort für Ihren Node, das Ihnen vom LRZ mitgeteilt wurde, beim ersten Systemkontakt ändern und dies auch in regelmäßigen Abständen wiederholen. Natürlich ist das Passwort geheim zu halten.

Die zweite Schwachstelle können Sie durch Verwendung neuerer Clients schließen.

Um der dritten Schwachstelle und ggf. der Zweiten bei Verwendung der älteren Clients entgegenzuwirken, bietet der SP-Client die Möglichkeit, sämtliche Daten zu verschlüsseln und erst dann an den SP-Server zu schicken. Damit ist sichergestellt, dass einerseits keine unverschlüsselten Daten über das Netz gehen und andererseits, dass die Daten nicht unverschlüsselt beim LRZ gespeichert werden. Der SP-Client verwendet dabei wahlweise die Verschlüsselungsalgorithmen `56-bit DES`, `128-bit AES` und `256-bit AES`. Das LRZ empfiehlt Ihnen, immer den stärksten Verschlüsselungsalgorithmus, den Ihre SP-Version anbietet, zu verwenden. Falls Sie Verschlüsselung verwenden, sind Sie für den Schlüssel zum Ver- und Entschlüsseln der Dateien verantwortlich. Sollten Sie ihn verlieren oder vergessen, können weder Sie noch das LRZ noch die Herstellerfirma IBM Ihre Daten wiederherstellen. Anzumerken ist außerdem, dass der rechenintensive Verschlüsselungsvorgang den Client belastet. Es sollte nicht ohne Grund verschlüsselt werden, da verschlüsselte Daten auf den Magnetbändern nicht mehr so gut wie unverschlüsselte Originaldaten komprimiert werden können. Somit steigt der notwendige Speicherplatzbedarf. Um den Backup- und Archivierungsdienst auch in Zukunft kostenlos anbieten zu können, bitten wir um einen nachhaltigen Umgang mit den Ressourcen des LRZ.
Weitere Informationen über die Verschlüsselungsfunktion des SP-Clients finden Sie im offiziellen Installations- und Benutzerhandbuch von IBM für Ihre SP-Version; wo Sie dies finden, steht in Abschnitt 9. Bei weiteren Fragen wenden Sie sich bitte an das LRZ.

3.2 Grundlegende Konfigurationsrichtlinien

Im Folgenden stellen wir die grundlegenden Konfigurationsrichtlinien des LRZ vor. Wir bitten Sie eindringlich, diese einzuhalten, da es dann für uns erheblich leichter ist, Sie im Problemfall zu unterstützen.

3.2.1 Speicherort der Programmdateien

Bitte installieren Sie die Programmdateien immer in das von der SP-Installationsroutine empfohlene Verzeichnis.

3.2.2 Speicherort der Konfigurationsdateien

Bitte legen Sie sämtliche Konfigurationsdateien immer an die Stelle, an der sie der SP-Client für Ihr System standardmäßig erwartet:

System	Konfigurationsverzeichnis
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 Planung des System-Backups

Für ein Backup des Betriebssystems ist SP nicht besonders geeignet, da zum Restore ein bereits lauffähiges Betriebssystem mit SP-Client benötigt wird. In der Regel ist es einfacher, schneller und oft besser, das Betriebssystem neu zu installieren, als das System mit SP wiederherzustellen.
Falls Sie auf eine *Bare-Metal-Restore*-Funktion, also ein Backup Ihres Betriebssystems, das auf einen „leeren“ Rechner zurückgespielt werden kann, nicht verzichten können, empfehlen wir Ihnen, eine sogenannte Image-Software zu verwenden. Damit können Sie nach erfolgreicher Installation und Konfiguration des Betriebssystems ein lokales Backup erzeugen, dass Sie im Katastrophenfall auf einen neuen Rechner einspielen können. Anschließend können Sie die seit der Erstellung des eingespielten Images gemachten Änderungen an Ihrer Betriebssysteminstallation über SP zurückholen. Eine Möglichkeit, die Restore-Zeit dann weiter zu verkürzen, ist, in regelmäßigen Abständen ein Image Ihrer Betriebssystemplatte zu erzeugen.

3.4 Planung des Backup-Zeitfensters

Bei der Registrierung Ihres Nodes über das LRZ DATWEB-Interface müssen Sie ein Zeitfenster auswählen. Es definiert, wann in etwa Ihr Node gesichert werden soll. Zurzeit bietet das LRZ folgende Zeitfenster standardmäßig an:

- morgens (täglich, werktags oder wöchentlich)
- abends (täglich, werktags oder wöchentlich)
- nachts (täglich, werktags oder wöchentlich)

Sie sollten sich überlegen, wann Ihr System am wenigsten belastet ist, und das Backup-Fenster in diesen Zeitraum legen. Sollten Sie andere Anforderungen haben, fragen Sie bitte beim Servicedesk *Service: Datenhaltung – Archiv und Backup* des LRZ nach.

3.5 Planung der Dateiarchivierung

3.5.1 Aufteilung in mehrere Filespaces

Wie bereits in Kapitel 3.1.1 erwähnt, ist es bei größeren Archiven sinnvoll, die archivierten Dateien auf mehrere Filespaces zu verteilen. So können Retrieve-Operationen und Node-Verlagerungen deutlich schneller durchgeführt werden. Um mehrere Filespaces zu nutzen, müssen Sie für jeden Filespace ein eigenes Verzeichnis anlegen und die Daten in geeigneter Weise auf die Verzeichnisse verteilen. Nach welchen Regeln Sie dies tun, müssen Sie selbst entscheiden, da es in der Hauptsache von Ihrer Anwendung und/oder Ihren Daten abhängt. Am LRZ gibt es zum Beispiel Archive, in denen für jedes Jahr oder für verschiedene Datenkategorien ein Verzeichnis angelegt wird. Die technische Umsetzung der Aufteilung in Filespaces erfolgt dann über virtuelle Mountpoints, die in Kapitel 5.2.2 beschrieben werden.

Bitte beachten Sie, dass eine Aufteilung eines physikalischen Filespaces in mehrere virtuelle Filespaces durchgeführt werden muss, bevor Daten dort archiviert wurden. Beachten Sie außerdem, dass diese Option nur unter Linux verfügbar ist. Falls Sie beabsichtigen, ein großes Archiv mit einem Windows-Client aufzubauen, oder falls Sie Probleme haben, ein geeignetes Verteilungsschema zu finden, setzen Sie sich bitte mit dem LRZ in Verbindung, damit wir gemeinsam eine Lösung erarbeiten können.

3.5.2 Aufteilung in mehrere Nodes

Bei sehr großen Archiven reicht unter Umständen eine Verteilung auf mehrere Filespaces nicht aus, da zu viele Filespaces pro Node wiederum zu Performance-Problemen führen. In diesem Falle muss man die Archivdaten auf mehrere Nodes aufteilen. Falls Sie planen, solch ein großes Archiv zu erstellen, setzen Sie sich bitte mit dem LRZ in Verbindung damit wir gemeinsam ein Konzept erarbeiten können.

3.5.3 Langzeitarchivierung

Im Normalfall werden Archivdateien von SP nach einer gewissen Zeit, die Sie in den aktuellen Benutzungsrichtlinien nachlesen können, vom Archivsystem gelöscht; aktuell sind das zehn Jahre. Wenn Ihnen für Ihre Daten dieser Zeitraum zu gering erscheint, können Sie beim LRZ einen formlosen Antrag auf Langzeitarchivierung stellen. Insbesondere sollen Sie in Ihrem Antrag darlegen, warum die Notwendigkeit besteht, Ihre Daten über einen noch längeren Zeitraum zu archivieren. Beachten Sie hier insbesondere den Abschnitt über Langzeitarchivierung in den Benutzungsrichtlinien.

3.5.4 Zeichenkodierung festlegen

Der SP-Client unterstützt Umlaute in Verzeichnis- und Dateinamen nur in bestimmten Zeichenkodierungen (*Character Encodings*). Wenn Sie Umlaute in Verzeichnis- und Dateinamen einsetzen möchten, müssen Sie gegebenenfalls einige Konfigurationseinstellungen Ihres Betriebssystems verändern. Sie müssen sicherstellen, dass die Verzeichnis- und Dateinamen in der Zeichenkodierung `ISO-8859-15` oder `UTF-8` angelegt werden. Dazu sind mindestens die Umgebungsvariablen `LANG` und `LC_CTYPE` auf den Wert `de_DE@euro` für `ISO-8859-15` und auf den Wert `de_DE.UTF-8` für `UTF8` zu setzen. Falls Sie *File Sharing* über Samba oder ähnliches einsetzen, müssen Sie auch dort über entsprechende Konfigurationsmechanismen die Zeichenkodierung auf `ISO-8859-15` bzw. `UTF-8` einschränken. Bitte beachten Sie, dass diese beiden Zeichenkodierungen nicht miteinander kompatibel sind und somit die Konfiguration aller Linux-Installationen auf eine Zeichenkodierung wie oben beschrieben angepasst werden muss, falls Sie Umlaute in Datei- und Verzeichnisnamen verwenden wollen.

Falls Sie Verzeichnis- und Dateinamen mit Umlauten in einer anderen Zeichenkodierung als `ISO-8859-15` bzw. `UTF-8` anlegen, kann es passieren, dass:

- die entsprechenden Dateien oder Verzeichnisse nicht gesichert werden,
- das gesamte Backup mit einer Fehlermeldung abbricht.

Im schlimmsten Fall kann das bedeuten, dass Sie kein Backup von Ihrem System haben.

3.6 Planung eines Betriebssystemwechsels/-updates

Wenn Sie Ihren SP-Node zum Backup eingesetzt haben und Ihr Betriebssystem wechseln oder die Major-Version (vgl. Abschnitt 4.2) aktualisieren wollen, sollten Sie beachten, dass die Weiterverwendung Ihres alten Nodes mit einem neuen Betriebssystem nicht unterstützt wird. Der Grund liegt darin, dass es in der Vergangenheit immer wieder zu unvorhergesehenen Nebeneffekten gekommen ist. Um diese zu vermeiden, unterstützt das LRZ Sie im Falle eines Betriebssystemwechsels oder Updates der Major-Version mittels zwei Vorgehensweisen:

1. Sie beantragen einen neuen Node.
2. Sie wenden sich an den Servicedesk *Service: Datenhaltung – Archiv und Backup* und teilen uns mit, dass Sie Ihr Betriebssystem wechseln wollen. Das LRZ benennt Ihren bisherigen Node in `<NODENAME>.OLD` um und reinitialisiert einen neuen Node `<NODENAME>`.

Sollten Sie in Ihrem alten Node neben Backup-Daten auch Archivdaten gespeichert haben, so sind Sie selbst dafür verantwortlich, die Daten von dem alten Node auf den neuen Node zu migrieren. Bei einem großen Archiv halten Sie bitte vorher Rücksprache mit dem LRZ.

Sollten Sie in Ihrem Node ausschließlich Archivdaten gespeichert haben, unterstützt das LRZ den Wechsel von einer Major-Version auf die nächsthöhere Major-Version des gleichen Betriebssystems. Wechsel des Betriebssystems sind aber auch für Archive nicht unterstützt. Es liegt in Ihrer Verantwortung, herauszufinden, ob IBM den angestrebten Wechsel der Betriebssystemversion unterstützt. Falls Sie dazu Hilfe von IBM benötigen, wenden Sie sich bitte an den Servicedesk *Service: Datenhaltung – Archiv und Backup.*

Worauf wir in diesem Zusammenhang noch hinweisen wollen, sind die von der jeweiligen Betriebssystemversion verwendeten Zeichenkodierungen (*Character Encodings*, vgl. Abschnitt 3.5.4). Falls Sie einen Node über mehrere Betriebssystemgenerationen hinweg benutzen wollen, ist es unbedingt erforderlich, die ursprüngliche Zeichenkodierung der ersten Betriebssystemversion, die Archivdaten darin abgelegt hat, beizubehalten. Andernfalls sind im besten Fall die Dateinamen nicht mehr lesbar, im schlimmsten Fall können Sie auf Ihre archivierten Daten nicht mehr zugreifen. Da in letzter Zeit immer mehr Betriebssysteme standardmäßig eine Zeichenkodierung in Unicode UTF-8 verwenden, ist es wichtig, dass Sie sich über diese Einschränkung im Klaren sind.

4 Installation/Update/Deinstallation des SP-Clients

4.1 Installation

Um SP nutzen zu können, müssen Sie als erstes die passende SP-Client-Software für Ihr Betriebssystem herunterladen und installieren. Folgende URL führt zu den Download-Seiten des SP-Clients: https://doku.lrz.de/display/PUBLIC/Download
Nachdem die passende Datei heruntergeladen wurde, müssen Sie diese eventuell noch entpacken. Das entpackte Verzeichnis des Linux-Clients der Architektur AA (x86_64, ppc64, s390x usw.) enthält folgende Dateien:

Pakete	Inhalt	Installationsverzeichnis

`gskcrypt64-8.x.x.x.linux.AA.rpm`
 	
`gskssl64-8.x.x.x.linux.AA.rpm`
	Verschlüsselung	`/usr/local/ibm/gsk8_64`

`TIVsm-API64.AA.rpm`	Anwendungsprogrammierschnittstelle (API), die die gemeinsam genutzten Bibliotheken und Beispiele für die SP-API enthält.	`/opt/tivoli/tsm/client/api/bin64`
`TIVsm-BA.AA.rpm`	SP-Client für Sichern und Archivieren, Kommandozeile (`dsmc`), administrativer Client	`/opt/tivoli/tsm/client/ba/bin`

	(`dsmadmc`), Web-Client und die Dokumentation	

`TIVsm-APIcit.AA.rpm`
 	
`TIVsm-BAcit.AA.rpm`
	Optional. Diese Dateien stellen die Komponenten *von IBM Tivoli Common Inventory Technology* bereit, mit denen Sie Informationen zur Anzahl der Client- und Servereinheiten, die mit dem System verbunden sind, sowie zur Auslastung der Prozessor-Value-Units (PVUs) durch Servereinheiten abrufen können. Weitere Informationen enthält der Abschnitt über das Abschätzen von Prozessor-Value-Units im *IBM Spectrum Protect for Linux*-Administratorhandbuch.	`APIcit` wird im Verzeichnis
		
		`/opt/tivoli/tsm/client/api/bin64/cit/`
		
		installiert.
		
		`BAcit` wird im Verzeichnis
		
		`/opt/tivoli/tsm/client/ba/bin/cit/`
		
		installiert.

`TIVsm-filepath-Distribution.AA.rpm`
 	
`TIVsm-JBB.AA.rpm`
	Dateien, die für die Unterstützung von journalgestützten Sicherungen benötigt werden.	`/opt/filepath`
		`/opt/tivoli/tsm/client/ba/bin`

`TIVsm_BAhdw.AA.rpm`	Stellt die Unterstützung von Snapshot-Sicherungen für NetAPP- und N-Series-NAS-Server bereit.	`/opt/tivoli/tsm/client/ba/bin/plugins`
`TIVsm-msg.xx_xx.AA.rpm`	Zusätzliche Sprachen inklusive Client-Messages; `xx_xx` definiert die installierte Sprache.	`/opt/tivoli/tsm/client/lang/xx_xx`

Die entpackten Verzeichnisse enthalten bei Windows und Mac OS folgende Dateien:

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

Die Installation der Clientsoftware wird wie folgt gestartet:

OS	**Start der 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`

	Am Beispiel der gängigsten PC Architektur (AA=x86_64, x.x.x entnehmen Sie bitte aus Ihrem entpackten Verzeichnis:
	
	`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`
	
	Bei einigen SP-Versionen kann es notwendig sein, die `rpm`-Option `--nodeps` mit anzugeben, falls obige Kommandos den Fehler melden, dass das `ksh`-Paket benötigt wird, doch das `ksh`-Paket sicher bereits installiert ist.

Windows	Rechtsklick auf *setup.exe* und Linksklick auf *Ausführen als Administrator*
Mac OS	• Öffnen des *Icons*, um den *Wizard* zu starten und • Backup-/Archiv-Client-Komponente zu installieren. • Sie werden während der Installation aufgefordert werden, ein Konto mit *Superuser*-Rechten anzugeben. Die Konfiguration des Mac OS SP-Client ist wie bei Linux durchzuführen.

Ausführlichere Installationsanleitungen finden Sie in den IBM/Tivoli-Dokumentationen, auf die in den `README`-Dateien (vgl. Abschnitt 1.7) verwiesen wird.

Für den Windows-SP-Client empfiehlt das LRZ die Installation des Merkmals *Open File Support*, das es SP ermöglicht, auch geöffnete Dateien zu sichern. Dazu müssen Sie im Installationsdialog die Option *Custom Installation* auswählen und im nächsten Dialogfenster *Open File Support* mit auswählen.

4.2 Updates

Im Zuge der Produktpflege und Produktentwicklung veröffentlicht IBM in bestimmten Zeitabständen neue Versionen der SP-Produktlinie. Die SP-Versionsnummer besteht aus vier Ziffern, die jeweils durch einen Punkt getrennt sind. Die erste Zahl repräsentiert die SP-Version, die zweite Zahl das Release und die beiden letzten Zahlen den sogenannten Level. 8.1.2.100 bedeutet also Version 8, Release 1, Level 2.100. Dabei muss man zwischen Haupt- (*major*) und Neben-Updates (*minor*) unterscheiden. Die ersten zwei Ziffern repräsentieren die Hauptversionsnummer, die letzten zwei die Nebenversionsnummer. Während Neben-Updates in der Regel der Beseitigung von Fehlern dienen, werden mit den Hauptversionen meist neue oder verbesserte Programmfunktionen ausgeliefert.

Natürlich ist es am bequemsten, eine einmal installierte und für gut befundene Client-Version über die gesamte Laufzeit eines Systems hinweg einzusetzen. Leider kann das LRZ Ihnen diese Vorgehensweise nicht empfehlen. Warum Updates notwendig sind und wie Sie am einfachsten und sichersten ein Versionsupdate durchführen, wird in den nächsten beiden Unterkapiteln erläutert.

4.2.1 Warum Updates?

Für das Durchführen von regelmäßigen Updates Ihres SP-Clients sprechen 4 Hauptgründe:

1. Programmfehler aus der älteren Version werden ausgebessert. Im Falle der Korrektur von sicherheitsrelevanten Fehlern ist ein Update besonders wichtig.

2. Neue Versionen besitzen unter Umständen neue nützliche Programmfeatures.
3. Wenn Sie immer die aktuellste Major-Version eines Clients einsetzen, können Sie sich sicher sein, dass Sie eine von IBM unterstützte Version benutzen.
4. Wenn Sie immer die aktuellste Nebenversion einer noch unterstützten Hauptversion eines Clients einsetzen, ersparen Sie sich im Problemfall, auf die aktuellste Nebenversion aktualisieren zu müssen (*Nota bene:* Aus unserer langjährigen Erfahrung mit dem IBM-Support wissen wir, dass IBM die Kunden in der Regel als Erstes auffordert, auf die aktuellste Nebenversion der eingesetzten und noch unterstützten Hauptversion zu aktualisieren und zu überprüfen, ob das Problem in dieser Version immer noch besteht).

Sie können sich natürlich dazu entschließen, keine regelmäßigen Updates Ihres SP-Clients durchzuführen. Allerdings kann das LRZ Ihnen bei Problemen nur helfen, wenn Ihre SP-Client-Version von IBM unterstützt wird. Da IBM eine SP-Version im Durchschnitt nur 2 Jahre lang unterstützt, sollten Sie in regelmäßigen Abständen überprüfen, ob dies für Ihre Version noch zutrifft.

4.2.2 Planung und Durchführung des Updates

Das „Updaten“ eines SP-Clients besteht darin, dass der alte Client komplett deinstalliert und der neue Client installiert wird.
Sie sollten Updates auf eine neue Major-Version erst durchführen, wenn diese Version auch auf der LRZ-Downloadmatrix verlinkt ist. Das LRZ garantiert nämlich nur dann, dass diese Client-Version auch mit der aktuell am LRZ eingesetzten Serverversion kompatibel ist.
Nachdem Sie Ihren SP-Client aktualisiert haben, sollten Sie die Schritte aus Kapitel 6 durchführen, um zu verifizieren, dass Ihr Client einwandfrei funktioniert.

Vor Durchführung eines Updates fertigen Sie bitte Kopien von Ihren wichtigsten SP-Client-Konfigurationsdateien (`dsm.opt`, `dsm.sys` und `inclexcl`-Datei) an. In der Regel spielt bei Windows nur die `dsm.opt` eine Rolle. Bei Linux-SP-Clients können Sie den Namen und Pfad zu der `inclexcl`-Datei mit Hilfe des Kommandos

```
cat dsm.sys | grep –i inclexcl
```

feststellen. Die Ausgabe von diesem Befehl sieht dann etwa wie folgt aus und gibt den vollständigen Pfad zu der *Include/Exclude*-Datei an:

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

Wenn Sie unter Linux nicht genau wissen, wo sich die SP-Client-Konfigurationsdateien befinden, so schauen Sie zuerst im Verzeichnis

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

nach. Finden Sie dort die Dateien nicht, kann der Linux-Befehl

```
locate dsm.sys
```

zum Auffinden von `dsm.sys` nützlich sein.

4.3 Deinstallation des SP-Clients

Die Deinstallation des SP-Clients unter Windows und Mac-Os kann durch die Software-Verwaltung durchgeführt werden.

Unter Linux gehen Sie wie folgt vor. Stellen Sie durch

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

fest, welche Pakete installiert sind und entnehmen Sie daraus, welche SP-Paketgruppen und welche Spracherweiterungen (Wert von xx_xx, z.B. DE_DE) installiert sind und deinstallieren Sie sie mit `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
```

Die Deinstallation von älteren Client-Versionen als 6.3 kann sich von der oben beschriebenen Prozedur unterscheiden. Die TSM-Version 6.2 enthält zusätzlich zu 64Bit Versionen noch 32Bit Pakete und Kompatibilitätspakete, nämlich `gskssl32`, `gsk7bas64` und `gskcrypt32`. Bitte suchen Sie gegebenenfalls nach den installierten Paketen.

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

Die Versionen vor 6.2 hatten keine Unterstützung für SSL-Verschlüsselung und keine Pakete vom Typ `gsk*.rpm`, d.h. der Befehl

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

sollte dann keine Antwort liefern.

Ein Minor-Upgrade des SP-Client kann unter Umständen auf der Basis eines Major-Releases funktionieren, so dass die Versionen von Client und API sich geringfügig unterscheiden können.

Ein Beispiel für 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 Konfiguration und Beispiele

5.1 Archiv und Backup

5.1.1 Konfiguration unter Linux und Mac OS

5.1.1.1 Erstellen der `dsm.sys`-Konfigurationsdatei

Die Datei `dsm.sys` ist die wichtigste Konfigurationsdatei Ihres SP-Clients. Sie sollte mindestens den folgenden Inhalt haben:

```
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            <Pfad zum Error-Logfile>
schedlogname            <Pfad zum Scheduler-Logfile>
passwordaccess          generate
passworddir             < Path >
```

Die Angaben in spitzen Klammern (`<. . .>`) sind als Platzhalter zu verstehen und müssen durch passende Werte ergänzt werden.

- `defaultserver` legt fest, welcher SP-Server per Default angesprochen wird.
- `Nodename legt fest welcher ISP-Knoten (Node) angesprochen werden soll`
- `servername`, `tcpserveraddress` und `tcpport` gehören zusammen und definieren einen SP-Server. Der Name für `servername` ist frei wählbar. Die Werte von `tcpserveraddress` und `tcpport` werden durch die Informationen bestimmt, die Ihnen vom LRZ bei der Registrierung Ihres Nodes mitgeteilt wurden. Bitte beachten Sie, dass Ihre Firewall entsprechend freigeschaltet für `tcpport` ist. Fragen Sie gegebenenfalls Ihren lokalen Administrator.
- `inclexcl` legt den Pfad zur Konfigurationsdatei für nicht zu sichernde Dateien fest.
- `schedlogretention` und `errorlogretention` geben an, wie viele Tage die Log-Meldungen des Scheduler bzw. die Errorlog-Dateien aufgehoben werden sollen.
- `schedlogname` gibt an, wo im Verzeichnisbaum die Log-Datei des Scheduler angelegt werden soll.
- `passwordaccess generate` wird benötigt nur wenn Client ohne direkte Eingabe des Passwortes Sichern/Wiederherstellen soll. Dabei wird Passwort verschlüsselt im File `TSM.PWD` abgelegt, falls Client Version < 8.1.2 bzw. 7.1.8 ist oder Nutzer = root und die Client Version ≥ 8.1.2 bzw. 7.1.8 ist. Dies wird oft bei Sicherung per Scheduler benötigt.
  Bemerkung: Verifizieren Sie, ob `TSM.PWD` angelegt worden ist, z.B. mit locate `TSM.PWD`

- `passworddir < Pfad zur Directory >` wird nur im Falle Client Version ≥ 8.1.2 bzw. 7.1.8 für einen nicht administrativen User (≠ root) welcher `passwordaccess generate` benutzen möchte. In der angegebenen Directory werden dann drei Files `TSM.IDX, TSM.KDB, TSM.sth` angelegt. Diese Files beinhalten verschlüsseltes Passwort ähnlich zu TSM.PWD und die notwendigen Einstellungen für den non-root User.

Achtung: Der User muss für die angegebene Directory Lese-/Schreibrechte besitzen, sonst werden die o.g. TSM.* Files nicht angelegt und `passwordaccess generate` wird nicht funktionieren.
Bemerkung: Nach dem ersten Client Zugriff verifizieren Sie, ob die Files tatsächlich angelegt worden sind:

cd `< Pfad zur Directory >` ;ls `TSM.IDX, TSM.KDB, TSM.sth`

5.1.1.2 Erstellen der `dsm.opt`-Konfigurationsdatei

Anders als bei Windows gibt es beim Linux-SP-Client nicht nur eine `dsm.opt`-Konfigurationsdatei, sondern auch eine `dsm.sys`-Konfigurationsdatei. Unter Linux sind die Einstellungen verteilt: In der `dsm.sys`-Datei wird die systemweite Konfiguration vorgenommen. Die `dsm.opt`-Datei kann als Ergänzung zur `dsm.sys`-Datei gesehen werden. Mit ihr können die Benutzer des Systems eigene Einstellungen vornehmen. Auch, wenn man dies nicht möchte, muss bei der Konfiguration des Clients eine `dsm.opt`-Datei unter `/opt/tivoli/tsm/client/ba/bin/dsm.opt` angelegt werden. Dann lassen Sie diese Datei einfach leer. Tragen Sie die nur Dateisysteme, die gesichert werden sollen, in der `dsm.opt` ein:

```
domain      /Zu/sicherndes/Filesystem1
domain      /Zu/sicherndes/Filesystem2
...
domain      /Zu/sicherndes/FilesystemN
```

5.1.1.3 *Include/Exclude*-Konfiguration

Als letztes muss noch die *Include/Exclude*-Konfiguration erstellt werden, in der festgelegt wird, welche Dateien bzw. Verzeichnisse gesichert werden und welche nicht. Wie bereits in Kapitel 3.1.2 erläutert, ist die Sicherung mancher Dateien nicht sinnvoll; dazu zählen System- und offene wie temporäre Dateien. Bei dem Versuch kann der Backup-Vorgang auch mit einem Fehler (z.B. bei Sicherung der `sysfs` unter Linux) abbrechen. Um solche Dateien auszuschließen, müssen Sie die Datei, die Sie in der `dsm.sys`-Konfigurationsdatei als Wert für den Parameter `inclexcl` angegeben haben, erstellen. Auch wenn Sie Dateien von der Sicherung ausschließen wollen, ist es sinnvoll, wenn folgendes in der ersten Zeile der `dsm.sys` steht:

```
include     *
```

Um Dateien von der Sicherung auszuschließen, verwenden Sie das `exclude`-Statement. Um ganze Verzeichnisse von der Sicherung auszuschließen, verwenden Sie das `exclude.dir`-Statement. Für linux-basierte SP-Clients empfehlen wir Ihnen, zumindest die Verzeichnisse `/dev`, `/proc` und `/sys` (`/sys` ab Kernel 2.6) auszuschließen. Dann sieht Ihre *Include/Exclude*-Datei in etwa so aus:

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

Die Einträge der *Include/Exclude*-Datei werden in ihrer Reihenfolge ausgewertet. Falls mehrere Einträge auf eine Datei passen, wird der letzte, d.h. unterste Eintrag verwendet. Zur richtigen Konfiguration kann das folgende Kommando helfen:

```
dsmc query inclexcl
```

Dies sind lediglich die Grundlagen der *Include/Exclude*-Konfiguration. Falls Sie mehr als die vorgestellte Minimalkonfiguration benötigen, lesen Sie bitte das entsprechende Kapitel im zu Ihrem Betriebssystem passenden offiziellen Installations- und Benutzerhandbuch von IBM.
Um zu testen, ob Ihre *Include/Exclude*-Konfiguration den gewünschten Effekt erzielen wird, bietet der SP-Client das `preview`-Kommando an. Näheres dazu finden Sie im offiziellen Handbuch im Kapitel über die *Include/Exclude*-Konfiguration und in Abschnitt 6.1.

5.1.1.4 Ändern des Erstpassworts

Um Ihr SP-Clientpasswort zu ändern, führen Sie bitte folgendes Kommando ggf. als `root` aus:

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

5.1.1.5 Starten des SP-Schedulers

Damit SP Ihr System automatisch sichern kann, muss ein Dienst, idealerweise bereits beim Boot-Vorgang gestartet werden, der SP-Scheduler.

```
/pfad/zu/dsmc sched > /dev/null 2>&1
```
z.B.
```
/opt/tivoli/tsm/client/ba/bin/dsmc sched >/dev/null 2>&1
```

Wie Sie dieses Kommando beim Systemstart aufrufen, hängt von Ihrer Linux-Distribution ab. Die gängigsten Wege sind:

- Erstellen eines rc-Scripts
- Hinzufügen des Eintrags
  `TSM::once:/pfad/zu/dsmc sched > /dev/null 2>&1`
  in der Datei `/etc/inittab`

5.1.1.6 Starten des SP-Schedulers unter Mac OS

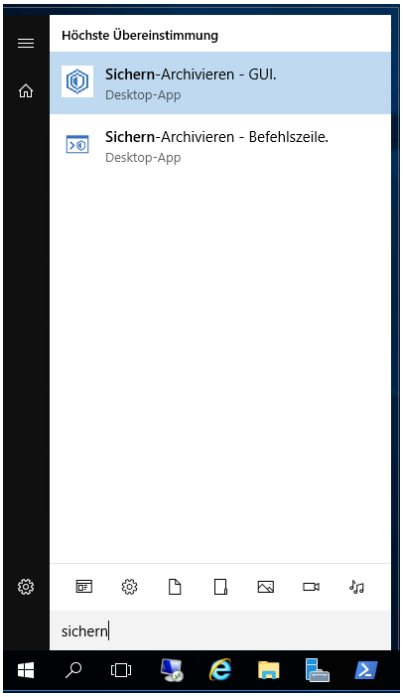
- Öffnen Sie den *IBM Spectrum Protect* Ordner
- Starten Sie *SP Tools for Administrators*
- Wählen Sie dann *Start Client Acceptor Daemon*
  Nachdem Sie `OK` gewählt haben, wird Ihr lokales administratives Passwort abgefragt. Wenn Sie sich richtig authentifiziert haben, wird der Scheduler gestartet und Sie bekommen eine entsprechende Bestätigung.
- Der SP-Scheduler wird im Ordner `/Library/Logs/tivoli/tsm/` zwei Log-Dateien anlegen: `dsmsched.log` (`stdout`) und `dsmerror.log` (`stderr`)

5.1.2 Konfiguration unter Windows

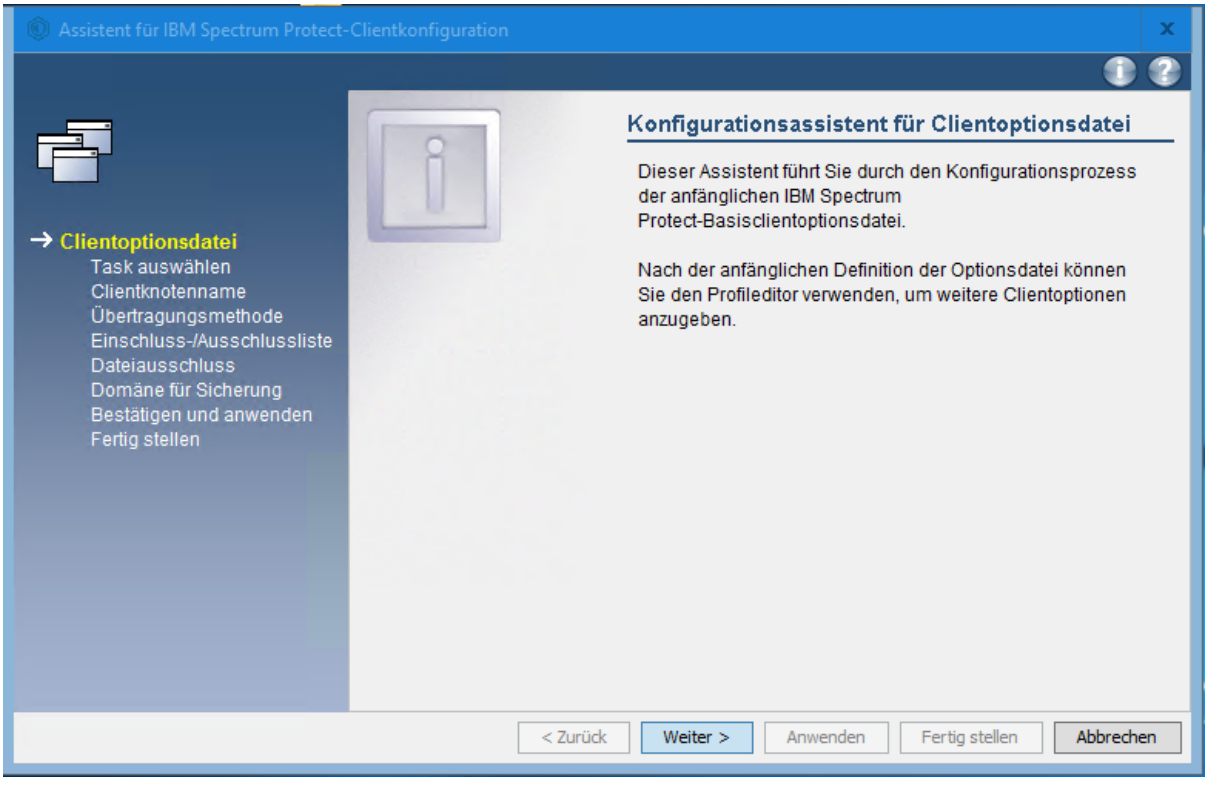
5.1.2.1 Erstkonfiguration des SP-Clients

Rufen Sie den SP-Client das erste Mal als Administrator auf. Er wird Sie dann durch einen Dialog führen, mit dem Sie die Grundkonfiguration Ihres SP-Clients erstellen können. Im Folgenden stellen wir die vom LRZ empfohlene Grundkonfiguration vor.

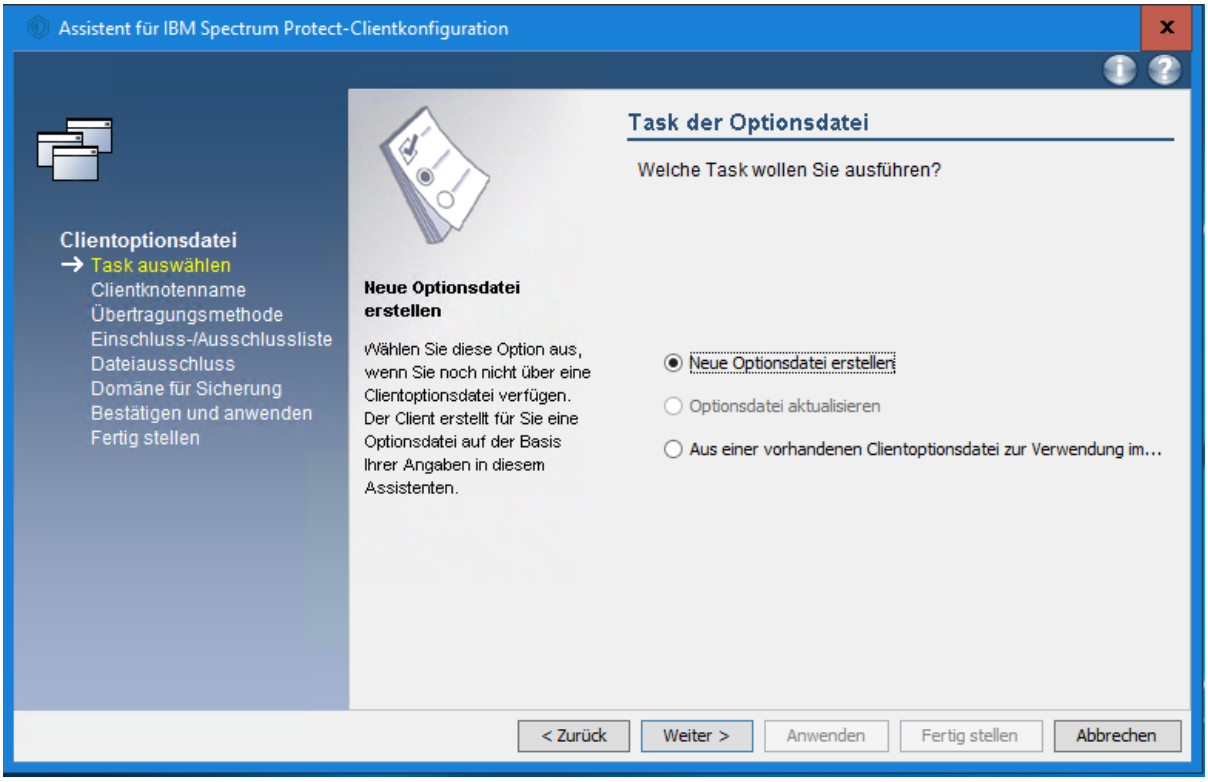
Starten Sie nun die grafische Oberfläche (GUI):



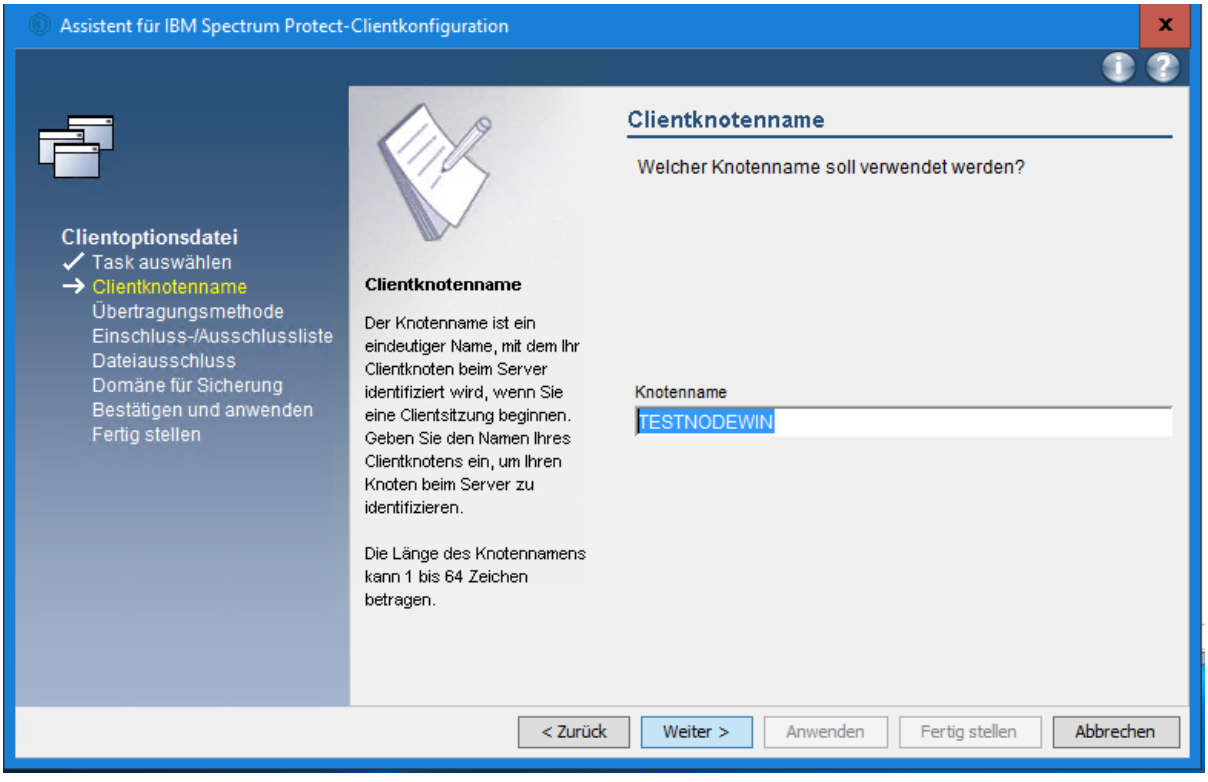
klicken Sie auf Weiter >



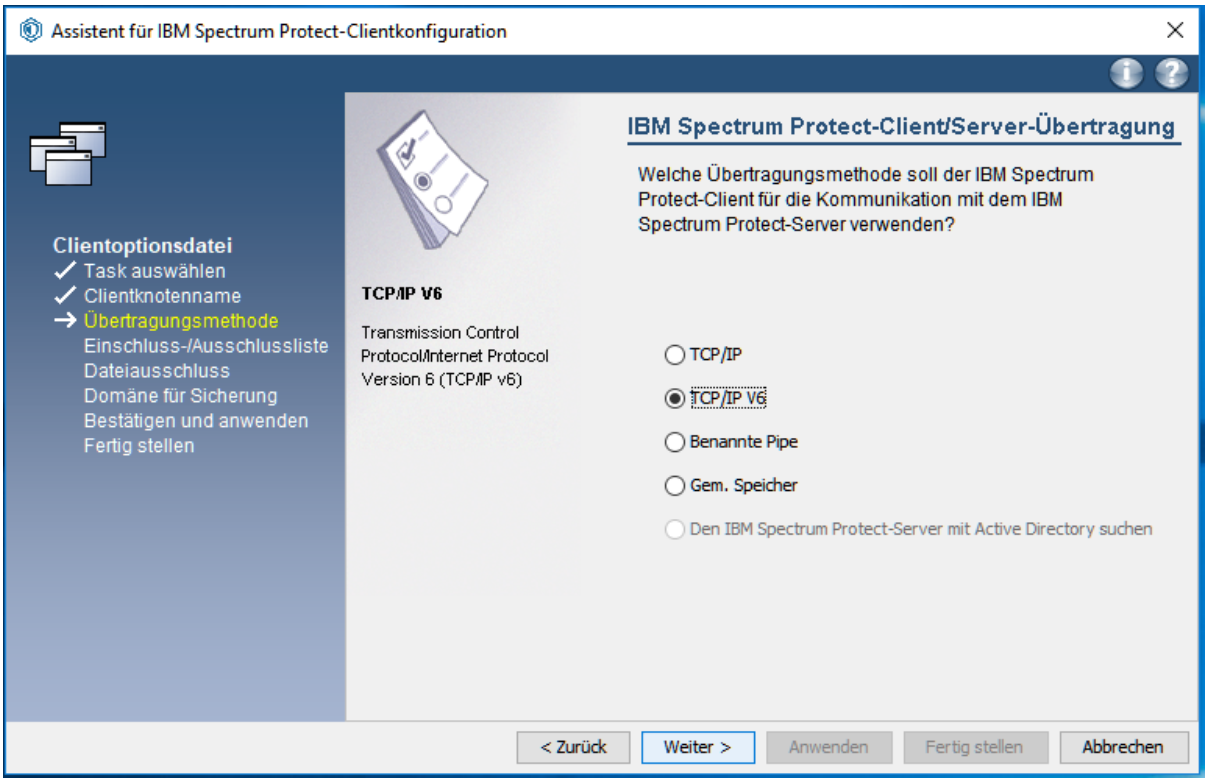
Erstellen einer neuen SP-Client-Konfiguration:



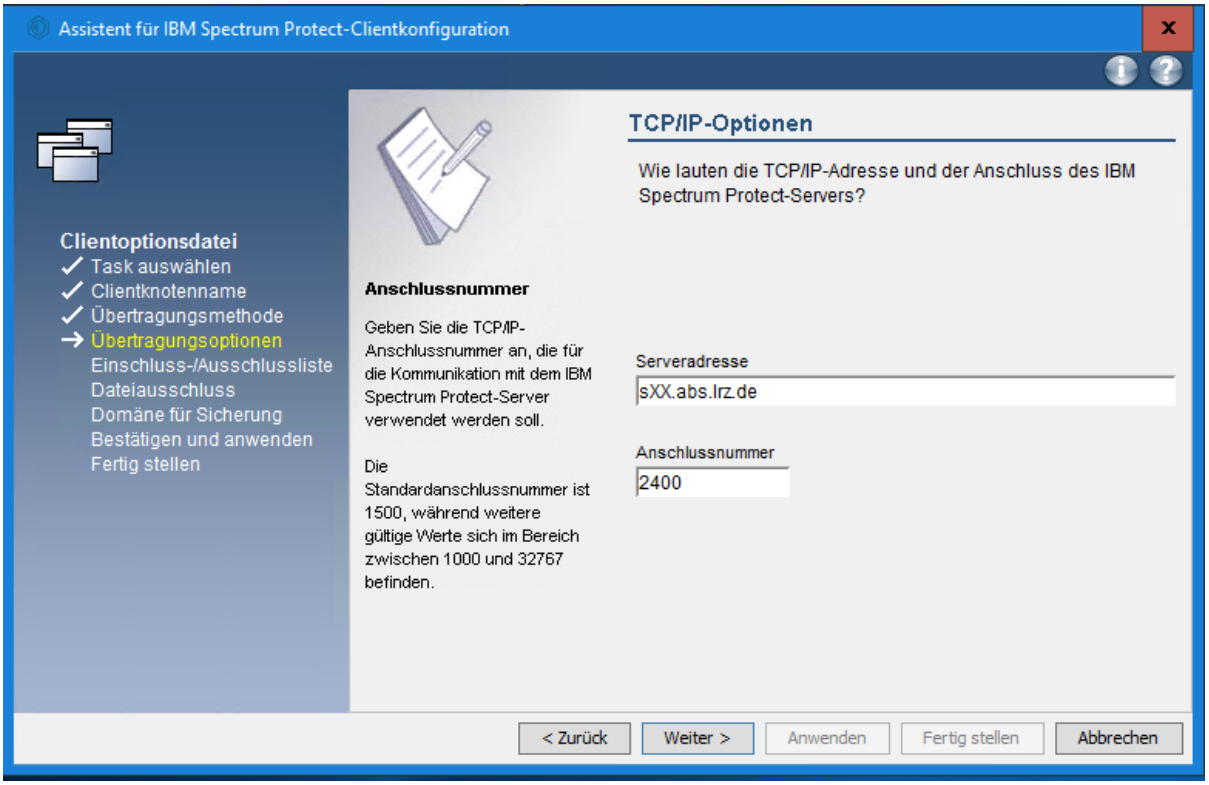
Im nächsten Schritt müssen Sie den Namen Ihres SP-Nodes, so wie er Ihnen vom LRZ mitgeteilt wurde, angeben:



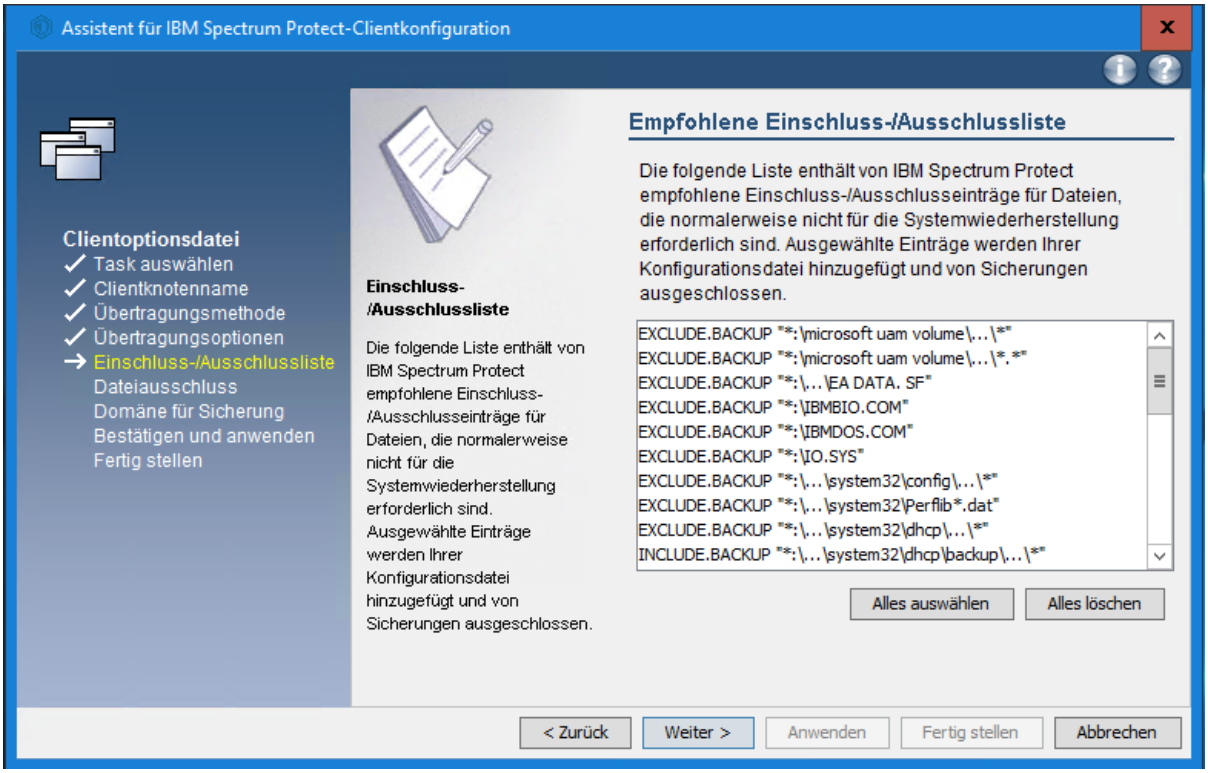
Dann legen Sie fest, wie der Client über das Netzwerk mit dem SP-Server des LRZ kommunizieren soll.



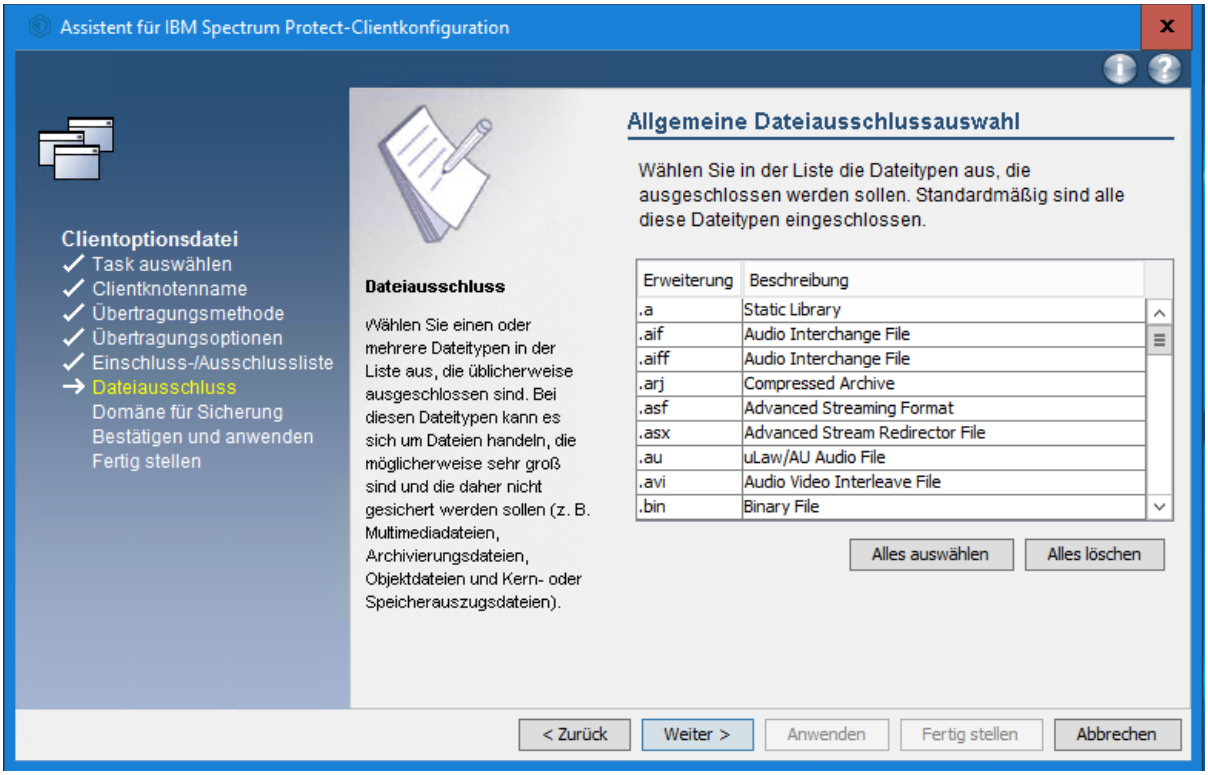
Im nächsten Schritt müssen Sie den Namen und den Port des SP-Servers, so wie er Ihnen vom LRZ mitgeteilt worden ist, angeben. Dieser Port muss in der Firewall freigeschaltet sein.



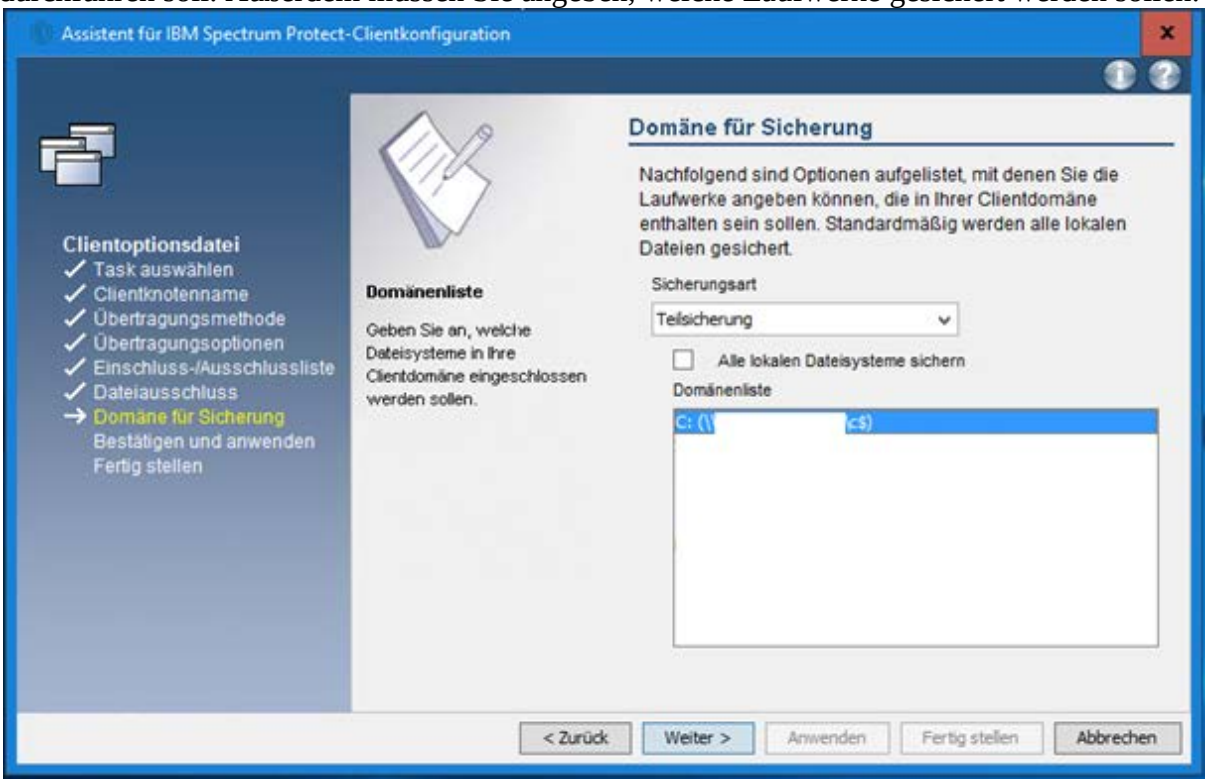
Als nächstes zeigt Ihnen der Dialog einen Vorschlag für eine *Include/Exclude*-Liste. Diese Liste legt fest, welche Dateien gesichert werden sollen und welche nicht. Drücken Sie hier auf alles löschen und klicken Sie auf Weiter >

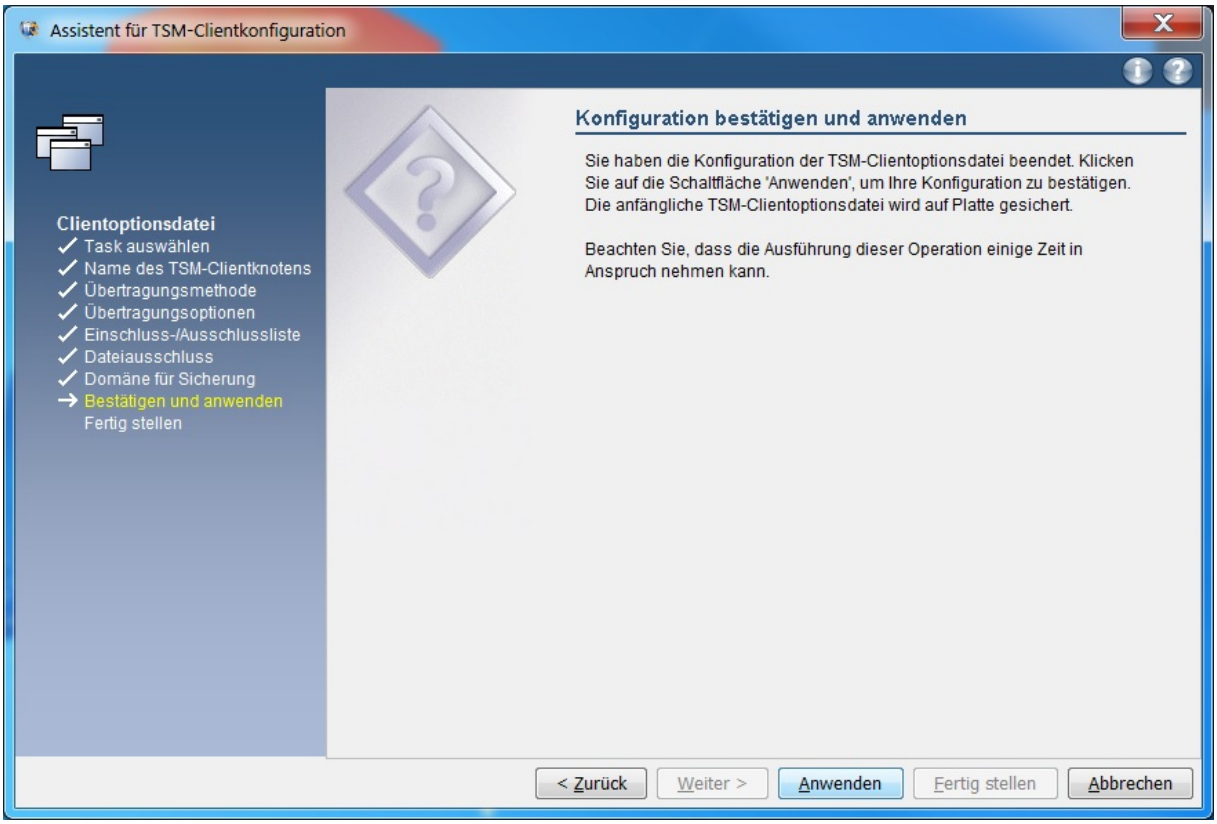


Sie können auch festlegen, welche Dateitypen von SP nicht gesichert werden sollen (z.B. `.mp3`, `.avi`, `.mpg`, etc.).

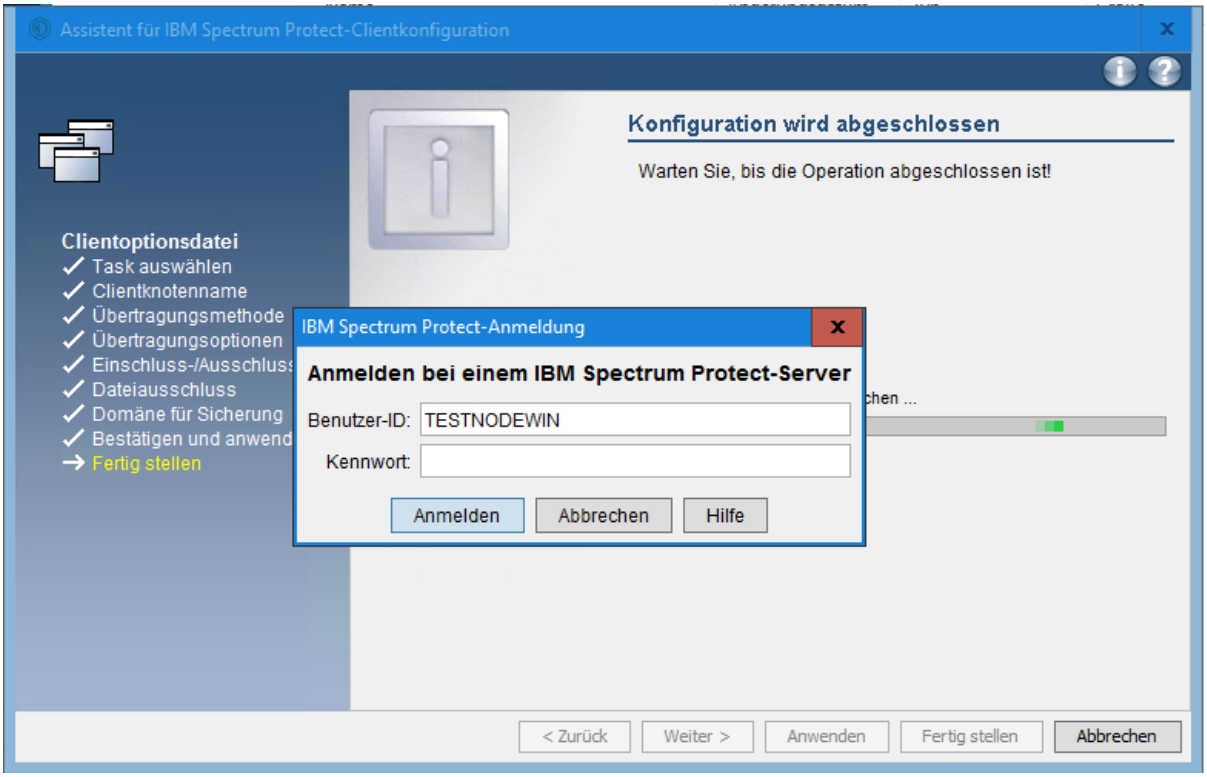


Schließlich müssen Sie noch festlegen, dass der SP-Client das Backup inkrementell durchführen soll. Außerdem müssen Sie angeben, welche Laufwerke gesichert werden sollen:

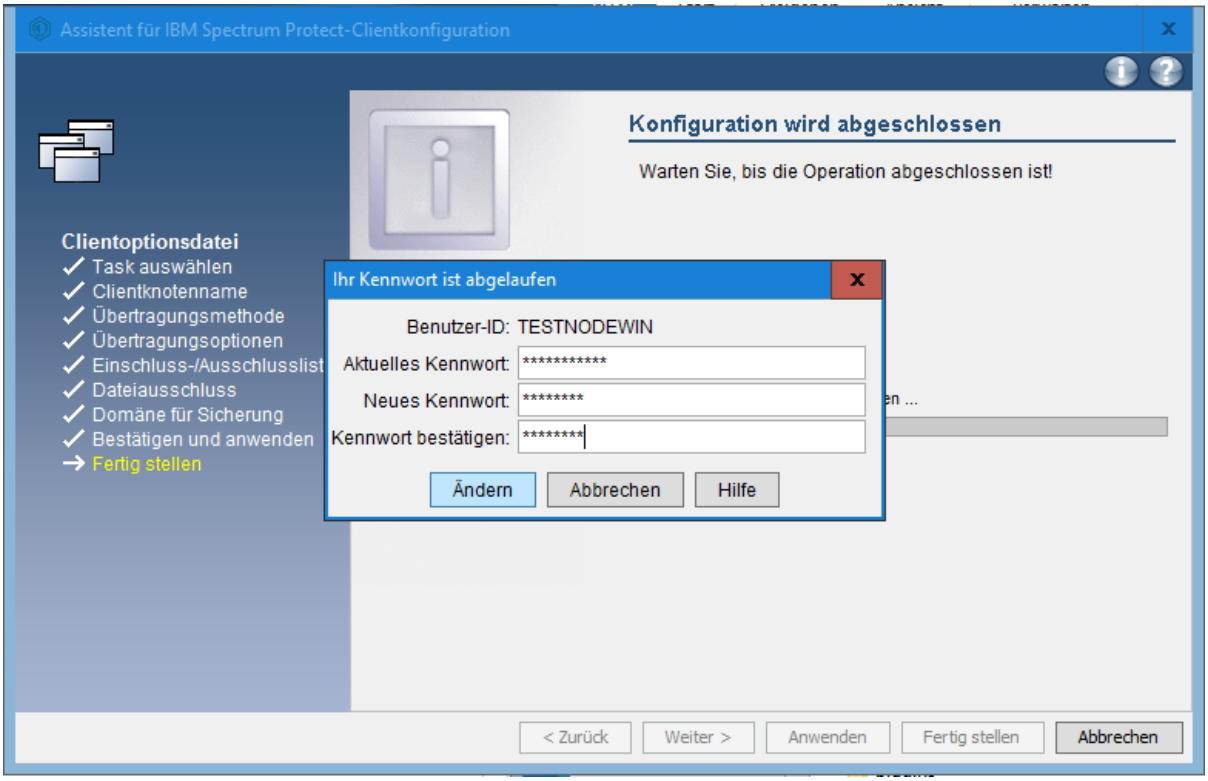




Dann müssen Sie sich am SP-Server anmelden. Verwenden Sie dazu den Node-Namen als Benutzerkennung und das dazugehörige Passwort, die Ihnen vom LRZ mitgeteilt wurden.



Geben Sie nun das aktuelle Node Kennwort und dann zweimal das neue Kennwort ein und drücken Sie auf Ändern:



Nun ist der SP-Client so konfiguriert, dass er Node grundsätzlich funktioniert. Jedoch ist die Konfiguration noch nicht Optimal, deswegen folgen Sie bitte der erweiterten Konfiguration.

5.1.2.2 Erweiterte Konfiguration

Die Konfigurationsdatei dsm.opt liegt im Installationsverzeichnis → C:\Program Files\Tivoli\TSM\baclient
Ihre dsm.opt Konfigurationsdatei sieht nach der Grundkonfiguration in etwa so aus:

```
NODENAME         TESTNODEWIN
TCPSERVERADDRESS sXX.abs.lrz.de
TCPPORT          2400
DOMAIN          \\XXXXXXXXXX\c$
```

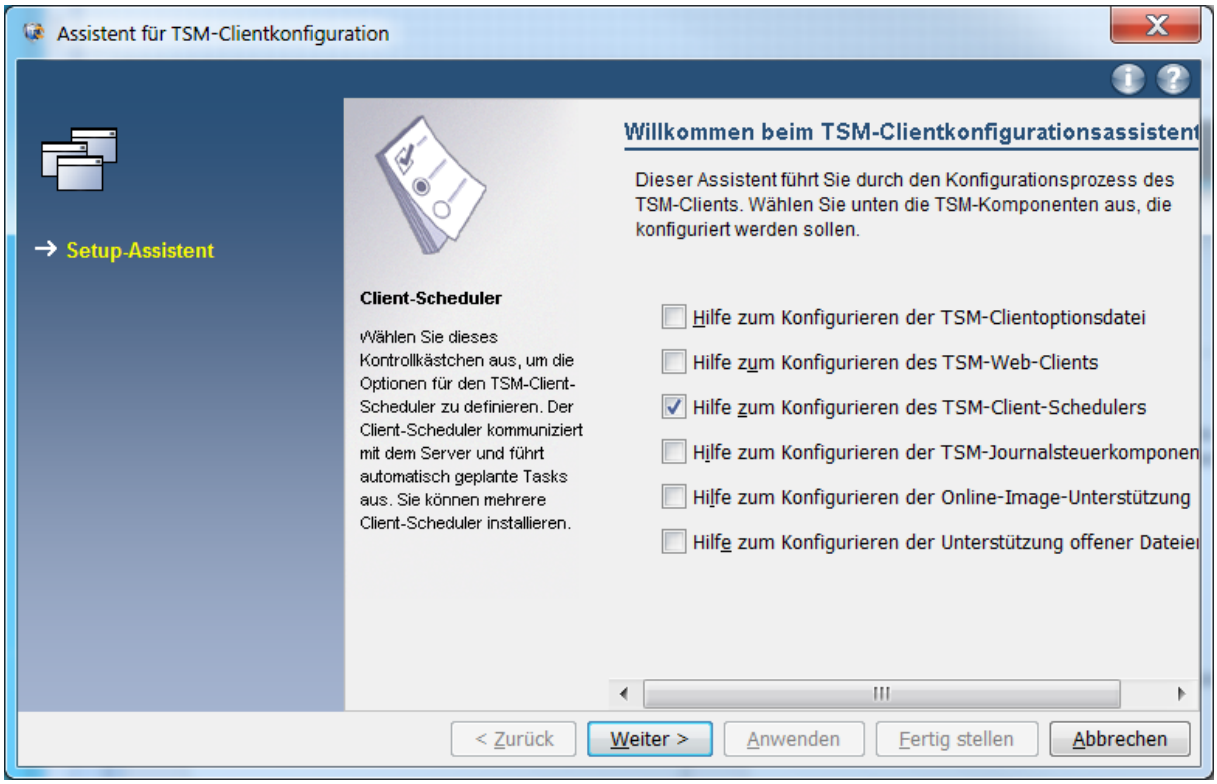
Bitte erweitern Sie nun ihre Konfigurationsdatei um die Einträge, die fehlen. Die Kommentare mit * davor können Sie zum Überblick auch übernehmen.

```
NODENAME         TESTNODEWIN
TCPSERVERADDRESS sXX.abs.lrz.de
TCPPORT          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
```

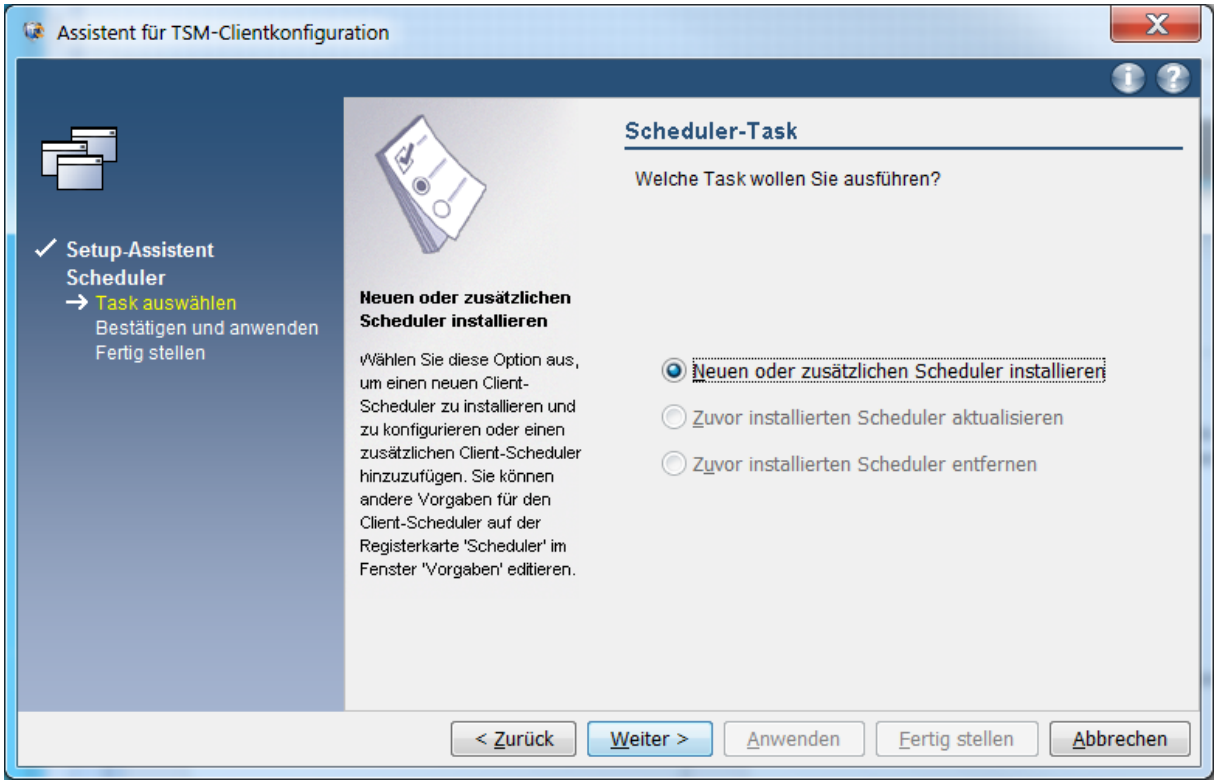
Aktuell läuft der Dienst für die automatische Sicherung noch nicht, er muss separat konfiguriert werden.

5.1.2.3 Konfiguration des SP-Scheduler

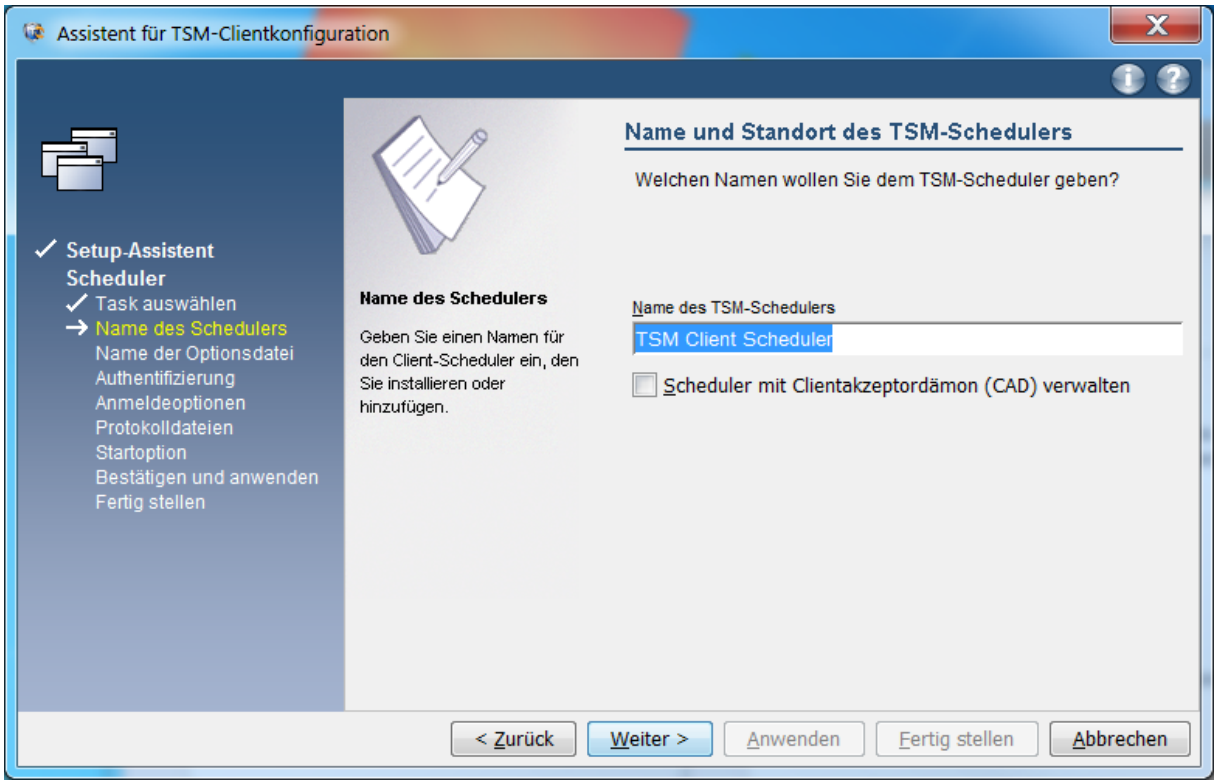
Um den Dienst für automatisiertes Backup zu aktivieren, gehen Sie wie folgt vor. Wählen Sie im Hauptfenster des SP-Clients *Utilities/Dienstprogramme* aus, dann *Setup Wizard/Setup-Assistent*.



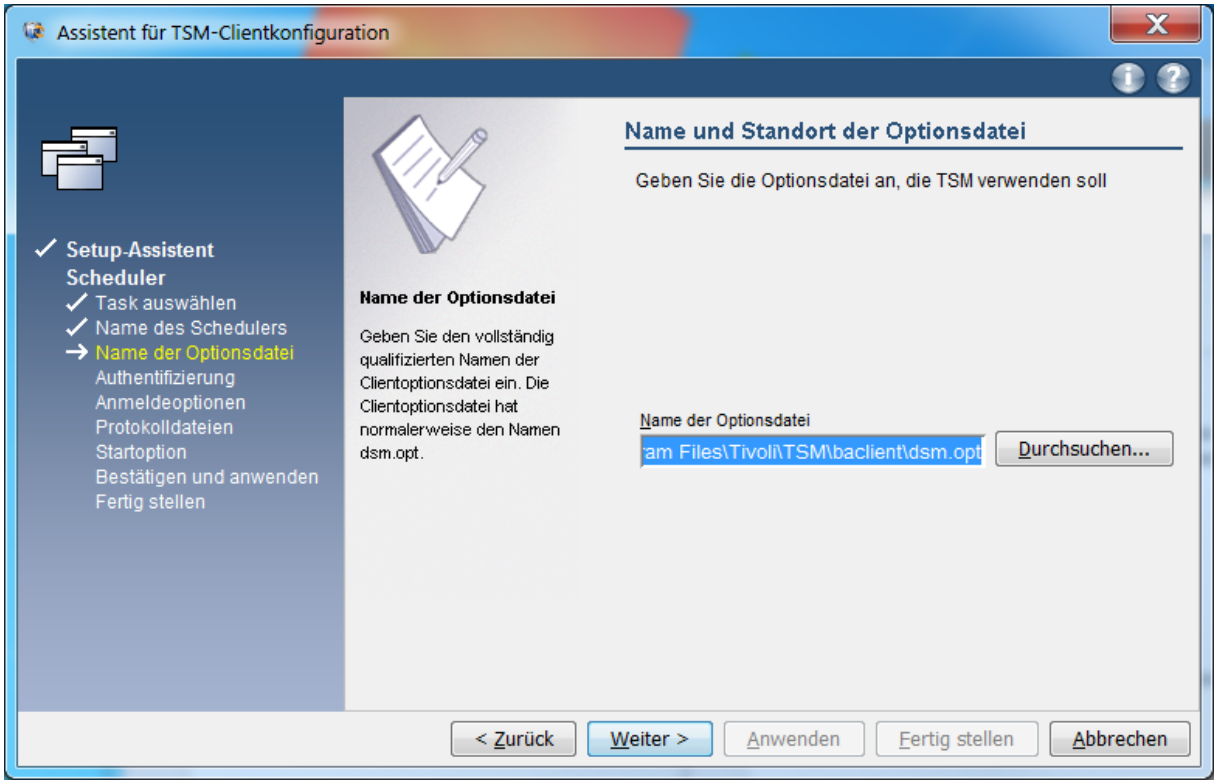
Wählen Sie nun aus, dass Sie einen neuen Ablaufplan (*Scheduler*) erstellen wollen.



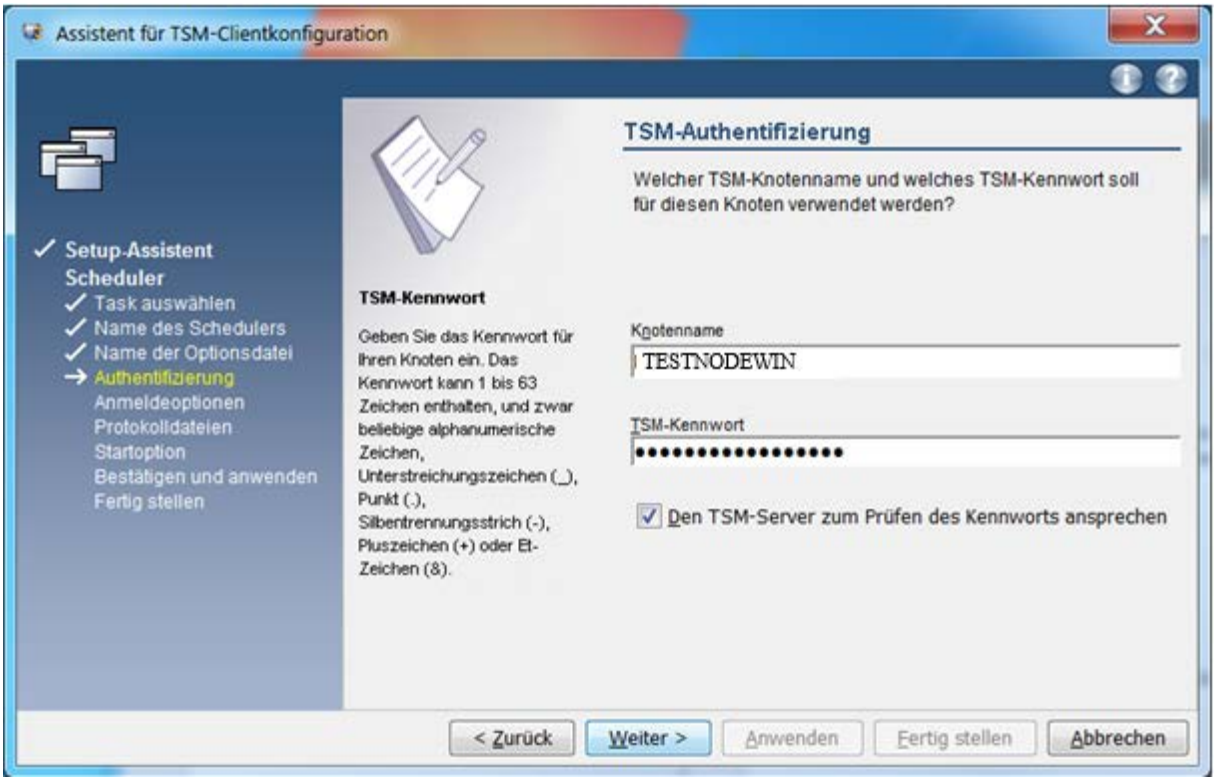
Falls gewünscht, können Sie einen beliebigen Namen für den Service vergeben



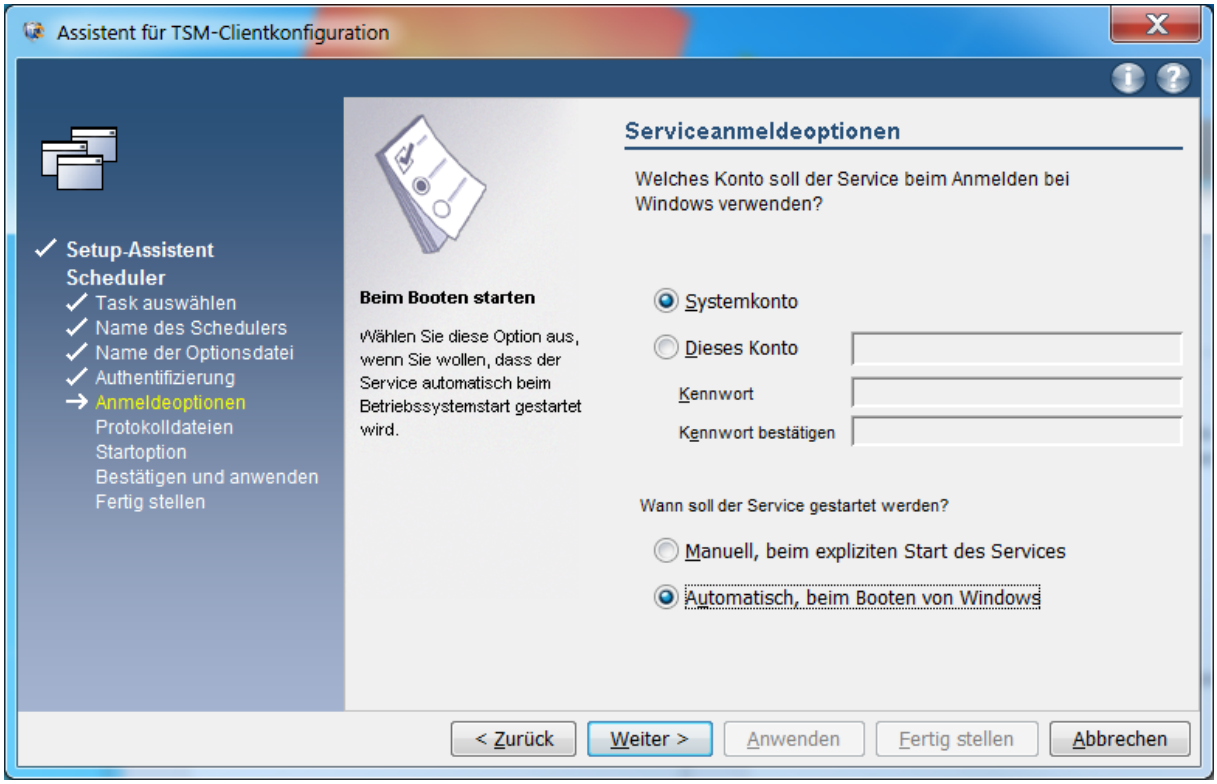
Verwenden Sie den voreingestellten Vorschlag von SP für die `dsm.opt`-Datei.



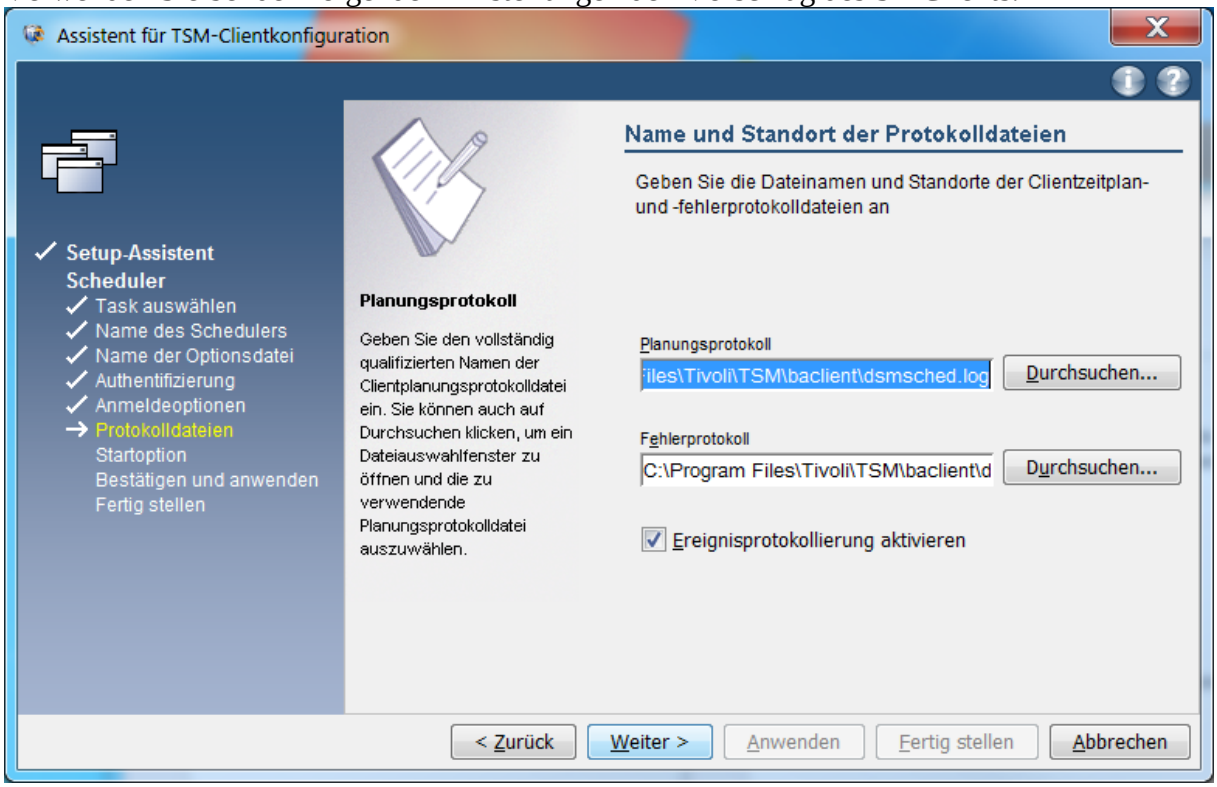
Geben Sie den Node-Namen und das dazugehörige Passwort an und aktivieren Sie die Option, das Passwort zu verifizieren.



Geben Sie an, dass das Systemkonto verwendet werden soll und dass der Dienst automatisch beim Booten von Windows gestartet werden soll.



Verwenden Sie bei den folgenden Einstellungen den Vorschlag des SP-Clients.



Sobald Sie den SP-Scheduler nun manuell starten oder Ihr System neu starten, wird SP Ihr System automatisch sichern.

5.2 Aufteilung der Daten in mehrere Nodes Archive & Backup

Wie in Abschnitt 3.1.3 bereits erwähnt wurde, ist es ratsam, ab einem gewissen Datenvolumen oder einer gewissen Dateianzahl mehrere Nodes zu verwenden oder zumindest mehrere virtuelle Filespaces zu definieren. Im Folgenden werden wir erläutern, wie Sie eine Aufteilung in mehrere Nodes bzw. mehrere virtuelle Filespaces bewerkstelligen können. Beachten Sie jedoch, dass davon ausgegangen wird, dass Sie diese Konfigurationen vornehmen, bevor Sie Dateien archivieren. Falls Sie bereits Daten gesichert oder archiviert haben und eine Umstellung auf mehrere Nodes oder Filespaces planen, setzen Sie sich bitte mit dem LRZ in Verbindung, da es eventuell einige weitere Dinge zu beachten gibt, um auf die bereits archivierten Daten wie gewohnt zugreifen zu können. Die folgende Darstellung basiert auf der Umsetzung unter Linux.

5.2.1 Aufteilung in mehrere Nodes unter Linux, Unix und Mac

Um mehrere Nodes auf einer Client-Maschine anzusprechen, sieht die Serverdefinition in der Konfigurationsdatei `dsm.sys` etwa folgendermaßen aus:

```
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>
...
```

und die `dsm.opt` so:

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

Um nun mit dem SP-Client auf einen bestimmten Node zuzugreifen, kann man das `dsmc`- oder `dsmj`-Kommando mit dem Parameter `-se=<nodenameX>` aufrufen.

5.2.2 Aufteilung in mehrere Filespaces unter Linux, Unix und Mac

Die sogenannten *Virtual Filespaces* werden in der Konfigurationsdatei `dsm.sys` folgendermaßen festgelegt:

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

5.2.3 Aufteilung der Daten in mehrere Nodes unter Windows

Wenn Sie aktuell nur einen Node konfiguriert haben, dann ist die Konfiguration des Nodes in der dsm.opt Datei unter C:\Program Files\Tivoli\TSM\baclient gespeichert. Um auf zwei oder mehrere Node zugreifen zu können müssen Sie nun eine neue .opt Datei in dem Pfad C:\Program Files\Tivoli\TSM\baclient für den neuen Node anlegen. Diese würde man dann optimaler Weise <nodename>.opt nennen. Beispiel:
Nodename TESTWIN2 -> Name der n-ten .opt Datei testwin2.opt
Die Konfiguration des TESTWIN2 Nodes erfolgt wie in Kapitel 5.1.2.2 beschrieben.

Öffnen Sie cmd als Administrator und wechseln Sie mit `cd C:\Program Files\Tivoli\TSM\baclient` in den Pfad des SP Clients. Nun können Sie die ISP GUI (grafische Oberfläche) des den neuen Node mit dem Befehl `dsm -optfile=testwin2.opt` und mit `dsmc -optfile=testwin2.opt` die ISP commandline starten.

6 Test der Konfiguration

Um sicherzustellen, dass Ihre SP-Clientkonfiguration auch so funktioniert, wie Sie es geplant haben, sollten Sie diese testen. Im Folgenden wollen wir alle Schritte zur Überprüfung der SP-Clientkonfiguration vorstellen. Sie sollten diesen Test nicht nur nach der Erstkonfiguration von SP durchführen, sondern idealerweise in regelmäßigen Abständen, mindestens aber jedes Mal, wenn Sie die SP-Clientkonfiguration oder die Spracheinstellungen wie die Zeichenkodierung Ihres Betriebssystems ändern. Nicht gesicherte oder archivierte Dateien können nicht wiederhergestellt werden. Prüfen Sie Ihre Konfiguration.

6.1 Auswerten der Preview-Funktion

Der SP-Client bietet eine Vorschau. Preview erzeugt eine Datei `dsmprev.txt`, in der für jede Datei festgehalten wird, ob sie gesichert wird oder nicht. Dazu rufen Sie das folgende Kommando für jedes Dateisystem Ihres Rechners auf:

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

Die nun erzeugte Datei `dsmprev.txt` sollten Sie auf Auffälligkeiten überprüfen. Vergewissern Sie sich, dass wirklich alle Dateien als zu sichernd angegeben werden, die zu sichern sind.

6.2 Testen der Backup-Funktion

Um die Backup-Funktion zu testen, können Sie ein Testverzeichnis anlegen. In diesem Verzeichnis legen Sie nun ein paar Dateien an. Erzeugen Sie für den Test am besten gleich einige Sonderfälle wie Umlaute oder Leerzeichen im Dateinamen. Danach sichern Sie das Verzeichnis, indem Sie folgendes Kommando ausführen:

```
dsmc incremental -subdir=yes /Pfad/zum/Testverzeichnis/
```

In der Ausgabe des Kommandos können Sie überprüfen, ob alle Dateien gesichert wurden. Zusätzlich können Sie sich mit dem folgenden Kommando anzeigen lassen, welche Dateien aus dem Testverzeichnis nun auf dem SP-Server vorhanden sind:

```
dsmc query backup -subdir=yes /Pfad/zum/Testverzeichnis/
```

Im letzten Schritt versuchen Sie, die gesicherten Dateien zurückzuspielen. Dazu führen Sie das folgende Kommando aus:

```
dsmc restore -subdir=yes /Pfad/zum/Testverzeichnis/
                                    /Pfad/zur/Ausgabe/von/Testverzeichnis/
```

Überprüfen Sie die Ausgabe des Restore-Kommandos daraufhin, ob alle Dateien restauriert werden konnten. Zusätzlich sollten Sie den Inhalt der restaurierten Dateien mit dem der Originaldateien vergleichen.

6.3 Testen der Archive-Funktion

Um die Archive-Funktion zu testen, gehen Sie analog zum vorangehenden Abschnitt vor, verwenden aber die Kommandos:

```
dsmc archive -subdir=yes /Pfad/zum/Testverzeichnis/
dsmc query archive -subdir=yes /Pfad/zum/Testverzeichnis/
dsmc retrieve -subdir=yes /Pfad/zum/Testverzeichnis/
                                    /Pfad/zur/Ausgabe/von/Testverzeichnis/
```

6.4 Überprüfen der Scheduler-Log-Datei

Nachdem Sie sich durch die vorherigen Schritte davon überzeugt haben, dass Ihre SP-Konfiguration einsatzfähig ist, sollten Sie auf jeden Fall überprüfen, ob ein Sicherungslauf auch ohne Probleme durchgeführt werden konnte. Dazu müssen Sie die Scheduler-Log-Datei auswerten, dessen Speicherort Sie bei einem Linux-System als Wert der Variable `schedlogname` in der `dsm.sys`-Konfigurationsdatei definiert haben.

Bei Windows finden Sie die Datei normalerweise unter

```
C:\Programme\Tivoli\TSM\baclient\dsmsched
```

Bei der Auswertung sollten Sie insbesondere auf nicht gesicherte Dateien und Abbrüche des Sicherungsvorgangs achten.

7 Zurückholen von Archivdaten

Wenn Sie Archivdaten aus dem SP-Archiv auf Ihren lokalen Rechner zurückholen wollen, sollten Sie möglichst alle benötigten Daten auf einmal, also durch eine einzige `Retrieve`-Anforderung, zurückholen. Dieses Vorgehen hat zwei Gründe:

1. Bei jeder Retrieve-Anforderung wird das Band mit den Archivdaten neu aufgespannt und es muss neu positioniert werden. Einzelne Rückholungen dauern daher länger als im Pulk.
2. Durch häufiges Einlegen werden die Bandmedien sehr belastet, was im schlimmsten Fall zu einer Zerstörung des Bands und somit zu Datenverlust führen kann.

Falls es aus Platzgründen nicht möglich sein sollte, die benötigten Archivdateien auf einmal zurückzuholen, sollten Sie auf jeden Fall mit jedem Retrieve möglichst große Datenmengen zurückholen. Sollte das LRZ eine zu hohe Anzahl von Mounts beobachten, behalten wir uns das Recht vor, dies zu unterbinden, um unsere Hardware und die darauf gespeicherten Daten vor Defekten zu schützen.

8 Aufgaben eines SP-Betreuers

Auch nach der Installation und Konfiguration des SP-Clients ist noch ein Mindestmaß an Pflege unerlässlich. Auch wenn die SP-Client-Software in der Regel wartungsarm ist, wollen wir Sie auf ein paar Aufgaben hinweisen, durch die Sie, wenn sie regelmäßig und gewissenhaft durchgeführt werden, auf lange Sicht Zeit einsparen können:

- Regelmäßiges Kontrollieren der Log-Daten, ob und, wenn ja, welche Fehler auftreten. Vor allem, wenn Sie den SP-Scheduler nicht nutzen.
- Beachten der Hinweis- und Statistiknachrichten des LRZ und Überprüfen der darin zu lesenden Angaben zu potentiellen Inkonsistenzen wie z.B. außergewöhnlich hohen Speicherplatzverbrauchs.
- Regelmäßige Versionsupdates des SP-Clients (siehe Kapitel 4).
- Regelmäßiges Testen der SP-Konfiguration (siehe Kapitel 7) insbesondere bei Updates oder Konfigurationsänderungen.
- Organisatorische Änderungen (Ansprechpartner, etc.) sind zeitnah dem LRZ mitzuteilen. Bitte beachten Sie, dass sicherheitskritische Vorgänge wie Zurücksetzen eines Node-Passwortes nur von dem am LRZ registrierten Ansprechpartner für den Node durchgeführt werden.
- Gravierende Änderungen am zu sichernden Datenvolumen sind dem LRZ möglichst bald mitzuteilen.
- Ausschluss von offenen Dateien bzw. unter Windows Einsatz von OFS. Nähere Informationen dazu finden Sie im offiziellen SP-Client-Handbuch von IBM.

9 Was tun, wenn etwas nicht funktioniert

Konsultieren Sie die folgenden Informationsquellen:

- SP FAQs
- *SP Best Practice Guide* des LRZ, also dieses Dokument, das wir regelmäßig aktualisieren und verbessern
- Offizielles SP-Client-Handbuch von IBM
- Lösungen suchen auf dem SP-Forum

Sollten Sie mit den oben genannten Hilfen Ihr Problem nicht lösen können, können Sie sich über den Servicedesk *Service: Datenhaltung – Archiv und Backup* an uns wenden. Zur Problembearbeitung benötigen wir mindestens folgende Informationen von Ihnen:

- Betriebssystem des SP-Clientrechners
- bei Linux bitte auch:
  - Verwendete Distribution und Version
  - Kernelversion, d.h. die Ausgabe von `uname -a`
  - Version von `glibc`, `libstdc++`, `rpm`
- Verwendete Rechnerarchitektur
- SP-Client-Version
- die Datei, die durch den Aufruf von `dsmc query systeminfo` erzeugt wird,
- detaillierte Problembeschreibung

Wir bitten Sie, sämtliche Support-Anfragen ausschließlich über den Servicedesk zu stellen. Nur dadurch können wir sicherstellen, dass Ihre Anfragen schnellstmöglich und transparent wie qualifiziert bearbeitet werden. Direkte Anfragen bei unseren Mitarbeitern werden nicht als offizielle Anfragen gewertet und werden deshalb nur mit niedrigster Priorität bearbeitet.

Außerdem können durch Urlaub und sonstige Abwesenheiten der Mitarbeiter Verzögerungen in der Bearbeitung auftreten.

10 Allgemeine Tipps

In diesem Abschnitt präsentieren wir einige ausgewählte, häufig auftretende Fragen, Antworten und Tipps. Vorab sei darauf hingewiesen, dass wir oben die jeweiligen `dsmc`-Kommandos explizit in der Langform angegeben haben. Oft lassen sich aber auch nahezu beliebige Kurzformen verwenden, sofern sie für SP eindeutig interpretierbar sind:

```
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
```

Entsprechend lassen sich die Kommandos `q` für `query`, `ba` für `backup`, `ar` für `archive`, `rest` für `restore` und `ret` für `retrieve` verwenden.

10.1 Wie kann ich meinen Linux-SP-Client auf eine neuere Version aktualisieren?

Bitte lesen Sie sorgfältig Kapitel 4. und die `README`-Datei der SP-Version, auf die Sie Ihren SP-Client aktualisieren wollen.

Grundsätzlich besteht die sauberste Vorgehensweise aus 4 Schritten:

- Erstellung der Kopien von Konfigurationsfiles (siehe Bemerkungen von 4.2.2)
- Deinstallation Ihrer alten SP-Client-Software (siehe 4.3)
- Neuinstallation der neuen Version von der SP-Client-Software (siehe 4.1)
- Wiederherstellung von Konfigurationsfiles aus den am Anfang angefertigten Kopien an der Stelle der Neukonfiguration des SP-Clients.

10.2 Ich möchte von meinem Windows Notebook auf die gesicherten Daten eines Linux-Servers zugreifen.

In Abhängigkeit von der installierten SP-, Windows- und Linux-Version kann der Versuch zu sehr bösartigen Problemen führen, so dass unter Umständen mit Datenverlust zu rechnen ist. Windows benutzt eine andere Zeichenkodierung und teilt dem SP-Server einige Windows-spezifische Informationen mit. Für die Zugriffe aus Linux wird dann der Node gesperrt. Für die Entsperrung des Nodes ist dann ein manueller Eingriff in die interne Datenbank des Servers nötig. Die dabei entstehenden Seiteneffekte sind nicht abschätzbar.

10.3 Ich möchte einen Linux-Rechner ersetzen und möchte von der Kommandozeile auf die Daten eines anderen von mir verwalteten Linux-Rechners zugreifen. Wie kann ich das machen?

Die dsmc-Option -virtualnodename=<Other Node_Name> erlaubt es, von Ihrem Node auf die Daten des Nodes mit dem Namen Other Node_Name zuzugreifen. Sie müssen allerdings das Password dazu kennen, dieselbe SP-Client-Version und dieselbe Zeichenkodierung verwenden.

Beispiel: Zugriff auf Node N1 mit den Daten auf SP-Server-Instanz S12 von dem Rechner N2 mit den Daten auf SP-Server-Instanz S22:

```
dsmc –se=S12 –virtualnodename=N1
```

Ein Schreib-Zugriff eines neueren SP-Clients kann dazu führen, dass ein älterer SP-Client nicht mehr oder nicht korrekt auf die Daten zugreifen kann.

10.4 Unter Scientific Linux funktioniert Ihre Anleitung für die Einrichtung des SP-Schedulers nicht. Wie kann ich den Scheduler zum Laufen bringen?

Scientific Linux wird nicht vollständig von SP unterstützt, daher orientiert sich unser *Best Practice Guide* an SuSE Linux. Die Linux-Distributionen unterscheiden sich in vielen Details, u.a. darin, wie die Scripte beim Start des Rechners gesteuert werden. Z.B. ist unter Scientific Linux das Hinzufügen des Eintrags wie in Abschnitt 5.1.1.6 beschrieben

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

Eintrag in die Datei /etc/inittab bleibt wirkungslos, wenn zudem darin zu lesen steht:

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

Folgendes Beispiel eines dsmsched-init-Scripts kann hilfreich sein, um den SP-Scheduler zu starten:

```
------------------------------------------------------------
#!/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! ..."
```

```
            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
-------------------------------------------------------------
```

Dieses Script sollte in dem Ordner `/etc/init.d` platziert und ausführbar gemacht werden. Unter SuSE Linux können Sie dann das Kommando `insserv dsmsched` ausführen. Dieses Kommando wird `dsmsched` in die `Init`-Prozedur aufnehmen.

Bei RedHat-Ablegern, zu denen auch Scientific Linux gehört, sollte der Eintrag für `dsmsched` in der Datei `/etc/rc.local` gemacht werden oder die Softlinks in den Ordner `/etc/init.d/rc3.d` und `/etc/init.d/rc5.d` per Hand angelegt werden, welche auf das Script `/etc/init.d/dsmsched` zeigen.

Bei dem oben dargestellten Script handelt es sich um ein Beispiel. Die gesetzten Werte der Variablen `PATH`, `DSM_LOG` und `LANG` sollten auf Ihrem System gegebenenfalls anders gesetzt werden.

10.5 SP-Client und NAS-Backup unter Windows 7, 8 und 10

Wie kann man eine NAS-Partition auf einem Windows 7, 8 oder 10 bzw. auf Windows Server 2008/R2, 2012/R2 und 2016 sichern, der kein Domänenrechner ist?

1. lokaler Nutzer muss Administrator und Backup-Operator sein. 2. Der User mit dem sich auf dem Rechner angemeldet wird muss in die Gruppe Sicherungsoperatoren und Administratoren (lokaler Administrator) hinzugefügt werden -> Einstellungen werden erst nach Neustart des Rechners übernommen
2. Die `dsm.opt`-Datei muss folgendermaßen ergänzt werden:

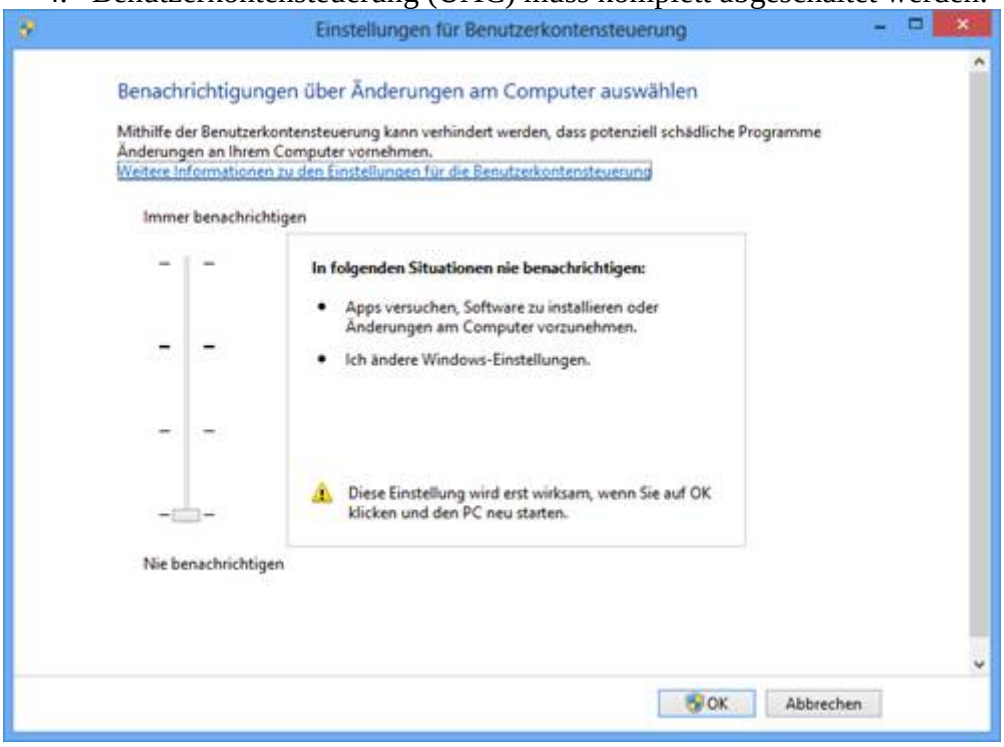
```
INCLUDE "<NAS SHARE>" STANDARD
DOMAIN "<NAS SHARE>"
SKIPNTPERMISSIONS YES
SKIPNTSECURITYCRC YES
```

z.B.

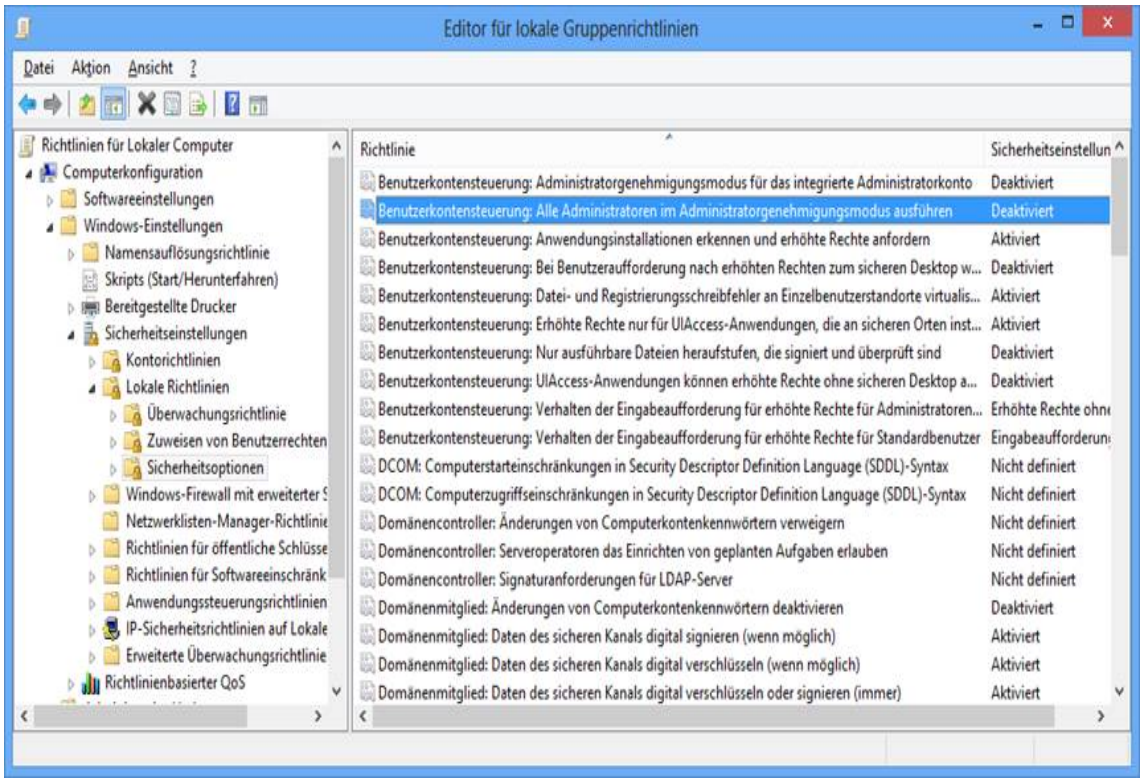
```
INCLUDE "\\nas.ads.mwn.de\a123456" STANDARD
```

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

3. Netzlaufwerk verbinden und Kennung und Passwort speichern
4. Benutzerkontensteuerung (UAC) muss komplett abgeschaltet werden:



5. In den lokalen Gruppenrichtlinien in den Sicherheitsoptionen: *Benutzerkontensteuerung: Alle Administratoren im Administratorengenehmigungsmodus ausführen* auf *deaktiviert* setzen.



Nun sollte das Netzlaufwerk auch in den TSM Einstellungen in der Domain List aufgelistet werden (Edit -> Client Preferences -> Backup)

Trotz diesen Einstellungen kann es nun vorkommen (vor allem unter Windows 10), dass das Netzlaufwerk bei einem manuellen Backup/Archive über die GUI (unter Netzwerk) nicht angezeigt wird.

Falls es nicht angezeigt wird, kann das Netzlaufwerk nur manuell über die ISP commandline oder über die Funktion Action -> Backup Domain (Achtung hier wird das Backup mit der dsm.opt config gestartet und entspricht dem Umfang der automatischen Sicherung) gesichert werden.

Ansonsten kann noch über die TSM Preview Funktion überprüft werden, ob das Netzlaufwerk gesichert wird (Utilities -> Preview Include-Exlcude)

10.6 Wie kann man eine nicht "Default Management Klasse", z.B. B10V oder B7V7D nutzen?

Die Steuerung von Management-Klassen (MGM) wird in SP durch die include/exclude Liste mit Hilfe von "include" Anweisung gesteuert.
Die explicite Angabe von der Management-Klasse erfolgt nach der Dateispezifikation. Ohne expilicite Angabe wird die s.g. "Default Management Class" benutzt.
Am LRZ heißt diese STANDARD

Beispiel einer Zeile aus inclexcl File:

include /home/.../ # <- wird in die Default MGM "STANDARD",
d.h. 3 Versionen 180 Tage, gesichert.

include /home/.../ *STANDARD* # <- dasselbe wie die Zeile oben nur explizit
ausgeschrieben = wird in die Default MGM "STANDARD",
d.h. 3 Versionen 180 Tage gesichert.

include /home/.../ *B10V* # <- wird in die "B10V" MGM,
d.h. 10 Versionen 180 Tage, gesichert

include /home/.../ B7V7D # <- wird in die "B7V7D" MGM,
d.h. 7 Versionen 7 Tage, gesichert

Ihre inclexclude Liste können Sie mit folgendem Befehl überprüfen:

Q INCLEXCLUDE

Wie die Dateien gesichert werden können Sie mit Hilfe von PREVIEW Befehl feststellen:

PREVIEW BA <Dateispezifikation>

z.B.

PREVIEW BA "/tmp/MEINE_DATEI"

Wie die Dateien bereits gesichert wurden, können Sie mit folgendem Befehl feststellen:

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

z.B.

Q BA "/tmp/MEINE_DATEI" -DETAIL

oder

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

Mit folgendem Befehl können die verfügbaren Managementklassen aufgelistet werden:

Q MGM –DETAIL

10.7 Verschlüsselung (Encryption)

Ich habe zum Teil sehr sensible Daten und möchte diese Daten verschlüsselt automatisiert per SP-Schedule sichern. Wie konfiguriere ich das und wie kann ich überprüfen, ob die Daten tatsächlich verschlüsselt gesichert werden?

Einrichten der Verschlüsselung

Die Einrichtung von SP-Verschlüsselung besteht aus drei Schritten:

1. *Encryption* in Client-Option-Datei `dsm.opt` (Windows) und in Client-System-Option-Datei `dsm.sys` (Linux) erlauben. Dafür müssen zwei Zeilen eingefügt werden:

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

`Keytype` hat einen der Werte `prompt`, `save` oder `generate`.
`Type` hat einen der Werte `AES256, AES128` oder `DES56`.

`Keytype=save` gilt nur, wenn

```
passwordaccess generate
```

eingestellt ist und ist für die verschlüsselte Sicherung per SP-Schedule notwendig.

z. B.
```
passwordaccess generate
encryptkey  save
ENCRYPTIONTYPE  AES128
```

2. In der `inclexcl`-Datei die Spezifikation für die zu verschlüsselnden Objekte einfügen.

```
include.encrypt <Spezifikation>
```

z.B.

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

3. Verschlüsselungspasswort muss eingegeben werden.

Starten Sie den SP-Client und sichern Sie eine Datei aus einem Ihrer Verzeichnisse, das verschlüsselt gesichert werden soll. Bei der ersten verschlüsselten Sicherung wird SP das Verschlüsselungspasswort abfragen und in der Datei `TSM.PWD` verschlüsselt speichern.

Wichtige Bemerkung: Im Fall vom Verlust des Verschlüsselungspasswortes gibt es keine Möglichkeit, die Daten wiederherzustellen. Aus diesem Grund hüten Sie das Verschlüsselungspasswort gut.

Überprüfen der Verschlüsselung

1. In der Kommandozeile

```
dsmc query backup <Dateispezifikation> -subdir=yes -detail
```

z.B.

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

gibt die detaillierte Information über die Datei aus (u.a. Verschlüsselungstyp).

Die Ausgabe sieht dann so aus:

```
      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  Zugegriffen: 25.02.2013 13:35:17
Komprimiert: NEIN       Verschlüsselungstyp: 128-Bit-AES
Vom Client dedupliziert: NEIN
```

oder für eine nicht verschlüsselte Datei:

```
      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  Zugegriffen: 18.02.2013 13:49:39
Komprimiert: NEIN       Verschlüsselungstyp:    Keine
```

2. Grafischer Client

Wählen Sie eine Datei, die Sie verschlüsselt gesichert haben. Mit rechter Maustaste erhalten Sie „Dateiinformationen“ aus dem Menü. Unter anderem wird der Verschlüsselungstyp angezeigt:

```
Verschlüsselungstyp:  128-Bit-AES
```

für das obere Beispiel, wenn alles richtig konfiguriert worden ist.

```
Verschlüsselungstyp: NONE
```

falls keine Verschlüsselung SP-seitig gemacht worden ist.

10.8 Wiederherstellung (Restore) der Daten zu einem bestimmten Zeitpunkt

Ich möchte die Versionen meiner Backup Daten so wiederherstellen, dass sie dem Zustand von einem bestimmten Zeitpunkt entsprechen. Wie kann ich das machen?

Für diese Art der Wiederherstellung ist der grafische Client von Vorteil. Unter Windows wird er standardmäßig genutzt. Unter Linux wird dieser Client mit dem Befehl `dsmj` gestartet.

Wählen Sie *Zurückschreiben* aus. Das entsprechende Programm Zurückschreiben wird dann gestartet. Neben den *Optionen* befindet sich die Schaltfläche *Nach Zeitpunkt*. Klicken Sie darauf, dann erscheint das Menü *Zurückschreiben nach Datum*, wo Sie dann den Zeitpunkt angeben und dann im Menü *Zurückschreiben* die wiederherzustellenden Daten auswählen und wiederherstellen können.

10.9 Mein Rechner ist kaputtgegangen (gestohlen worden). Wie stellt man die gesicherten Daten auf einem neuen Rechner am besten wieder her?

Bitte gehen Sie wie folgt vor:

1. Installieren Sie den SP-Client auf Ihrem neuen Rechner. Beachten Sie dabei folgende Punkte:

    1. Die SP-Client-Version sollte dieselbe sein wie bei Ihrem alten Rechner. Falls dies nicht möglich ist, darf die SP-Version auf dem neuen Rechner auf keinen Fall älter sein als auf dem alten. Die SP-Version von Ihrem alten Rechner können Sie am LRZ erfragen, falls Sie sie nicht mehr wissen.
    2. Das Betriebssystem auf Ihrem neuen Rechner sollte gleichbleiben. Wenn das nicht möglich ist, sollte eine neuere Version des Betriebssystems eingesetzt werden. Die Nichtbeachtung von diesem Punkt kann zu Datenverlust führen. Insbesondere ist der Austausch zwischen Linux und Windows sehr problematisch (s.o.).
    3. Die Zeichenkodierung auf dem neuen und alten Rechner sollte gleich sein. Sonst ist die richtige Darstellung der Sonderzeichen nicht gewährleistet.

2. Konfigurieren Sie den SP-Client auf Ihrem neuen Rechner, so dass der Node-Name und die Server-Einstellungen denen auf dem alten Rechner entsprechen, ebenso wie die *Include/Exclude*-Einstellungen (`inclexcl`-Datei (Linux), entsprechender Abschnitt der `dsm.opt` (Windows)). Falls die *Include/Exclude*-Einstellungen Ihnen nicht mehr bekannt sind, tragen Sie bitte erst nur

```
include *
```

ein. Falls Sie die SP-Client-Verschlüsselung auf Ihrem alten Rechner benutzt haben, müssen Sie für die Wiederherstellung der Daten das Verschlüsselungspasswort und die Spezifikation der verschlüsselten Objekte kennen. Bitte tragen Sie dann Ihre

```
include.encrypt <Spezifikation>
```

bei den *Include/Exclude*-Einstellungen dazu (s.o.).

3. Aktivieren Sie die Option *aktive/inaktive Dateien anzeigen*. Wenn der SP-Client auf dem neuen Rechner gestartet wird, führt er den Abgleich zwischen den Daten durch, die auf dem Rechner liegen und denen, die in SP gesichert worden sind. Da Sie den Rechner ersetzt haben, sind die meisten gesicherten Daten nicht auf dem neuen Rechner vorhanden und werden dann als gelöscht vom SP-Client angesehen. Diese Daten werden somit als inaktiv markiert. Da aber dieser Abgleich eine Weile dauert, wird verwirrenderweise ein Teil als aktiv und ein Teil als inaktiv sichtbar. Aus diesem Grund müssen Sie die Option *aktive/ inaktive Dateien anzeigen* aktivieren, sonst sehen sie gegebenenfalls Ihre gesicherten Daten unvollständig. Dafür klicken Sie bitte im grafischen Client auf *Zurückschreiben* und dann in Menü-Punkt *Ansicht* auf *aktive/inaktive Dateien anzeigen* oder Sie benutzen in der Kommandozeile die Option `-ina`. Erst nach dieser Aktivierung können Sie die älteren Versionen und gelöschten Dateien auswählen.

4. Beginnen Sie nun mit der Wiederherstellung Ihrer Daten.

10.10 Weiterführende Links

Servicedesk

Nutzungsbedingungen des Archiv- und Backup-Systems

SP-Client-Handbuch von IBM

SP FAQs

SP-Forum

SP-Supportmatrix