# Wolters Kluwer
## Softwarelösungen

# Hinweise zur Datensicherung

Wolters Kluwer

## Benutzerhandbuch

Stand September 2017

Gültig ab DVD 3/2017

bzw. 1/2017
für ADDISON Handwerk

Wolters Kluwer Softwarelösungen - Hinweise zur Datensicherung
Benutzerhandbuch

Stand: September 2017




Wolters Kluwer Software und Service GmbH
ADDISON Zentrale
Stuttgarter Straße 35
71638 Ludwigsburg

## Inhaltsverzeichnis

# 1. Einleitung

Dieses Dokument enthält sowohl allgemeine Hinweise und Grundsätze zur Datensicherung als auch produktspezifische für die jeweils eingesetzte ADDISON Softwarelösung.

Zu den ADDISON Softwarelösungen zählen:

- ADDISON Software
- ADDISON Aktenlösung (tse:nit | cs:Plus) und
- ADDISON Handwerk

Dieses Dokument ersetzt nicht die von Microsoft® oder Drittherstellern gelieferten Dokumentationen zu angesprochenen Themen.
Sollten die Empfehlungen dieses Dokumentes von denen der Dokumentation „Systemvoraussetzungen“ abweichen, so gelten die Angaben der zuletzt genannten Dokumentation als Mindestvoraussetzung (insbesondere hinsichtlich der notwendigen Service Packs).

Bitte beachten Sie, dass zum ordnungsgemäßen Betrieb der ADDISON Softwarelösungen bestimmte Einstellungen zwingend notwendig sind. Andere Einstellungen und Maßnahmen sind Vorschläge, die Sie an Ihre individuellen Bedürfnisse anpassen können oder sogar müssen.

Wenden Sie sich an Ihren Systembetreuer zur Einrichtung der genannten Einstellungen und Maßnahmen, um kostenintensive Fehler zu vermeiden.


Die Wolters Kluwer Software und Service GmbH übernimmt keine Haftung für Schäden, die durch den Verlust von Daten entstehen.

Die Verantwortung für die regelmäßige Datensicherung liegt beim Kunden. Sowohl für den Einzelplatz als auch für das Netzwerk muss eine externe Datensicherung vorhanden sein.

# 2. Allgemeine Hinweise zur Datensicherung

## 2.1. Grundregeln der Datensicherung

Hier werden die wichtigsten Grundregeln der Datensicherung aufgeführt. Auf einzelne Punkte wird in den folgenden Abschnitten näher eingegangen.

- Sicherungen sollten außer Haus und sicher (z.B. im Bankschließfach) aufbewahrt werden.
- Sicherungen auf gleicher Festplatte bzw. Partition sind nutzlos, wenn die Festplatte zerstört ist.
- Bewahren Sie ältere Sicherungen für eine bestimmte Zeit auf, falls die neueste Sicherung beschädigt oder zerstört wird, verloren geht oder Probleme erst später bemerkt werden.
- Implementieren Sie ein System zum Überschreiben von Sicherungen, bei dem die ältesten Sicherungen zuerst wiederverwendet werden.
- Verwenden Sie Ablaufdaten für Sicherungen, um ein verfrühtes Überschreiben zu vermeiden.
- Beschriften Sie die Sicherungsmedien, damit wichtige Sicherungen nicht versehentlich überschrieben werden. Dies ermöglicht eine problemlose Identifizierung der auf den Sicherungsmedien gespeicherten Daten oder eines bestimmten Sicherungssatzes.
- Testen Sie Ihre Sicherungsroutine. Häufig wird erst im Ernstfall festgestellt, dass die Sicherungsroutine nicht oder sogar noch nie funktioniert hat oder dass der gesicherte Datenbestand selbst schon defekt war.
- Klären Sie die für Sie geeignete Sicherungsroutine mit Ihrem Systembetreuer.

Eine ordnungsgemäß durchgeführte **Datensicherung** ist - wie der Name bereits ausdrückt - eine **Versicherung gegen Datenverlust** und die damit evtl. einhergehenden wirtschaftlichen Folgen: Das Sicherungsverfahren sowie auch die Sicherungshardware und das Sicherungsmedium müssen stimmen. Hard- und Software-Hersteller bieten sehr zuverlässige, komfortable und schnelle Komponenten an, sodass ein Verzicht auf eine individuelle Vorort-Datensicherung (in-house) nicht mehr zu begründen ist.

## 2.2. Datensicherheit in einem IT-Umfeld

Auszug aus den GoB,
„Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“:

„Voraussetzungen für ein geeignetes IT-Umfeld sind eine angemessene Grundeinstellung zum Einsatz von IT und ein Problembewusstsein für mögliche Risiken aus dem IT-Einsatz bei den gesetzlichen Vertretern und Mitarbeitern.
Das Sicherungskonzept muss in Übereinstimmung mit der IT-Strategie und der IT-Organisation stehen und eine Bewertung der spezifischen Sicherheitsrisiken des Unternehmens enthalten. Ein solches Sicherheitskonzept wird durch Ausführungsanweisungen etwa im Bereich des IT-

Betriebes, des Netzbetriebes und der Administration sowie bei der Gestaltung von Zugriffsschutzverfahren konkretisiert.
Die aus dem Sicherheitskonzept abgeleiteten Sicherungsmaßnahmen umfassen physische Sicherungsmaßnahmen und logische Zugriffskontrollen, Datensicherungs- und Auslagerungsverfahren“.

Physische Sicherungsmaßnahmen dienen dem Schutz der Hardware sowie der Programme und **Daten** vor Verlust, Zerstörung und unberechtigter Veränderung. Hierzu zählen u.a. Zugangskontrollen und Datensicherungskonzepte.
Über logische Zugriffskontrollen unter Verwendung von Benutzer-ID und Passwörtern ist die Identität der Benutzer von IT-Systemen eindeutig festzustellen, um damit nicht autorisierte Zugriffe zu verhindern.

Die Durchführung regelmäßiger Datensicherungen ist im Allgemeinen Voraussetzung für

- die Rekonstruktion historischer Bestände (Programme und Daten),
- die Rekonstruktion aktueller Software- und Datenbestände bei Funktionsstörungen der Hardware.

Im Rahmen des Datensicherungsverfahrens für die Wiederherstellbarkeit des IT-Systems sind die Zahl bzw. die regelmäßige Wiederkehr der Sicherungen (Generationskonzept), die verwendeten Sicherungsmedien und die Art der Aufbewahrung der Sicherungen festzulegen.
Für die Erstellung eines **Datensicherungskonzeptes** sowie die Einhaltung des Konzeptes sind die gesetzlichen Vertreter verantwortlich.

## 2.3. Häufigkeit der Sicherung

Wir empfehlen, den Datenbestand mindestens einmal täglich komplett zu sichern. Darüber hinaus muss unmittelbar vor dem Einspielen einer neuen Version der ADDISON Softwarelösungen eine Sicherung des Datenbestandes durchgeführt werden.

Bitte beachten Sie, dass für Sicherungsmedien in Abhängigkeit z.B. vom Umfang des Datenbestandes und der täglich anfallenden Änderungen am Datenbestand Aufbewahrungsfristen vorgesehen werden sollten.

Die Häufigkeit der Datensicherung bei einer Einplatzinstallation hängt von der Veränderung Ihrer Daten ab. Da diese vermutlich nicht so hoch wie bei einer Mehrplatzinstallation ist, wird eine tägliche Sicherung nicht zwingend notwendig sein. Berücksichtigen Sie jedoch den notwendigen Aufwand für die Wiederherstellung der verlorenen Daten, wenn Ihre Sicherung zum Beispiel mehrere Tage alt ist.

Aber auch hier gilt: Bitte erstellen Sie Sicherungen generationsweise und bewahren Sie diese über einen längeren Zeitraum auf.

### 2.3.1. Rotationsverfahren: Monats-, Wochen- und Tagesbänder

Es ist sehr wichtig, dass ein sinnvolles Sicherungsverfahren angewendet wird, damit auch auf Datenbestände eines länger zurückliegenden Zeitraums zurückgegriffen werden kann.
**Ein Band, das jeden fünften Tag oder gar jeden Tag überschrieben wird, stellt keine sinnvolle Datensicherung dar!**
Hier hat sich das sog. „Großvater-Vater-Sohn-Prinzip“ (englisch GFS-Rotation) bewährt und etabliert. Es werden dazu insgesamt mindestens 20 Bänder benötigt - die genaue Anzahl ist natürlich von der zu sichernden Datenmenge abhängig -, welche wie folgt eingesetzt werden:

#### Monatsbänder

Diese Bänder (12) werden nach 12 Monaten wieder überschrieben. Das Band vom Januar 2014 wird also im Januar 2015 überschrieben.

#### Wochenbänder

Diese Bänder (4) werden 4 Wochen aufbewahrt. Das Band der 1. Woche eines Monates wird wieder Ende der 1. Woche des nächsten Monates überschrieben.

#### Tagesbänder

Diese Bänder (4 Mo.-Do. oder 5 Mo.-Fr.) werden max. 7 Tage aufbewahrt. Das Band von Montag wird immer am nächsten Montag überschrieben. Wahlweise kann die Aufbewahrungsfrist auch auf 14 Tage ausgeweitet werden, wodurch sich jedoch die benötigte Anzahl der Tagesbänder verdoppelt.
Weiterhin empfiehlt es sich eine Jahressicherung zu erstellen. Diese sollte keine Aufbewahrungsfrist bekommen, d.h. nicht überschrieben werden.

## 2.4. Sicherungsverfahren

Je nach Art der gesicherten Daten werden folgende Methoden unterschieden:

### 2.4.1. Komplettsicherung

Dabei werden immer alle Daten komplett gesichert. Dies ist die höchste Sicherheitsstufe, da eine Wiederherstellung mit dem geringsten Aufwand (d.h. im Regelfall mit einem Medium) durchgeführt werden kann. Nachteil des Verfahrens ist der hohe Aufwand an Zeit und ggf. Sicherungsmedien.

### 2.4.2. Inkrementelle Sicherung

Dabei werden immer nur die Daten gesichert, die sich seit der letzten Sicherung geändert haben. Dies hat den Nachteil, dass bei einer Wiederherstellung u.U. neben der letzten Komplettsicherung auch mehrere Medien der inkrementellen Sicherung zurückgesichert werden müssen.

### 2.4.3. Differenzielle Sicherung

Dabei werden nur die Daten gesichert, die sich seit der letzten Komplettsicherung (Wochen- bzw. Monatssicherung) geändert haben. Vorteil ist, dass bei einer Wiederherstellung neben der letzten Komplettsicherung nur das Medium der letzten differenziellen Sicherung zurückgesichert werden muss. Beispiel: Im Falle einer Rücksicherung des Gesamtdatenbestandes muss neben dem Medium der letzten Wochen- bzw. Monatssicherung nur das Medium der letzten Tagessicherung verwendet werden.

Für die Monats- und Wochensicherung kommt ausschließlich eine Komplettsicherung in Frage. Für die Tagessicherung empfehlen wir die differenzielle Sicherung.

Zusätzlich zu diesen regelmäßigen Sicherungen sind Sondersicherungen (z.B. vor dem Jahreswechsel oder dem Einspielen von neuen Programmreleases) auf separaten Medien durchzuführen.

## 2.5. Speicherort der Sicherungsbänder

**Die Bänder der Sicherungen müssen an entsprechend gesicherten Orten gelagert werden**, sodass im Notfall darauf zurückgegriffen werden kann.

Beispiel: Wenn alle Sicherungsbänder im Serverraum gelagert werden und dieser durch höhere Gewalt (Feuer, Wassereinbruch, Diebstahl, Vandalismus, ...) zerstört wird, war die Sicherung nutzlos.

Allgemeine Empfehlung zur Lagerung der Sicherungsbänder:

- **Monatssicherung (Jahressicherung):**
  Schließfach bei der Hausbank oder bei der beauftragten Sicherheitsfirma
- **Wochensicherung:** Wie Monatssicherung oder Firmen-Safe
- **Tagessicherung:** Firmen-Safe, um bei Bedarf schnellen Zugriff zu erhalten

## 2.6. Sicherungsmedium/Sicherungsgerät

Welches Medium – welches Sicherungsgerät - eingesetzt wird, hängt von der Datenmenge ab, die gesichert werden muss.
Das Sicherungsmedium wird i.d.R. ein Magnetband sein. Die Speicherkapazität reicht von 8 GB (DDS-2-Band) bis 2500 GB (LTO-Band).
Für ein zu sicherndes Datenvolumen von bis zu 40 GB können 4mm-DAT-Bänder des DDS-4-Standards (40 GB) als Standardsicherungsmedium mit einem optimalen Preis-/Leistungsverhältnis betrachtet werden. Für größere Datenmengen kommen vor allem

DLT- und DLO-Bänder (mit einer Sicherungskapazität von bis zu 200 GB) in Frage. Anhand der Anzahl der für die gesamte Sicherung - siehe Sicherungsverfahren - benötigten Bänder kann auch kalkuliert werden, ob der Einsatz von DAT-, DLT- oder LTO-Bändern günstiger ausfällt.
Für größere Datenmengen und vollautomatische Datensicherungen ohne täglichen Bandwechsel - außer bei Wochen-/Monatssicherungen - empfehlen wir den Einsatz eines sog. Autoloaders. Diese Geräte werden in unterschiedlichen Bauarten und mit unterschiedlichen Kapazitäten angeboten.

## 2.7. Maßnahmen bei Gesamtausfall (Notfallzustand)

Das Datensicherungskonzept ist dann vollständig, wenn der „Ernstfall“ berücksichtigt wird. Maßnahmen müssen definiert werden, die im Notfall zu ergreifen sind, um z.B. die Ausfallzeit zu minimieren.

Definition des Notfallzustandes (BSI: Bundesamt für Sicherheit in der Informationstechnik):

„Der Notfall tritt erst dann ein, wenn ein Zustand erreicht wird, bei dem innerhalb der geforderten Zeit eine Wiederherstellung der Verfügbarkeit nicht möglich ist und sich daraus ein sehr hoher Schaden ergibt. Schon bei Eintritt eines Ereignisses, in dessen Folge der Notfall entstehen könnte, sind die erforderlichen Maßnahmen zu ergreifen, die zu einer Schadensreduzierung führen. Für die autorisierte und rechtzeitige Einleitung von Notfallmaßnahmen bedarf es der Benennung eines Notfall-Verantwortlichen. Die Behörden- bzw. Unternehmensleitung muss den Notfall-Verantwortlichen sowohl für die Entscheidung autorisieren, ob ein Notfall eingetreten ist, als auch für die Einleitung erforderlicher Notfallmaßnahmen“.

# 3. Schritte zur Einführung der Datensicherung

## 3.1. Festlegung der Komponenten

### Schritte zur Einführung einer Datensicherung

Vor der Einführung der Datensicherung im Unternehmen müssen folgende Arbeitsschritte durchgeführt werden:

- Ermittlung der zu sichernden Datenmenge
- Festlegen des Sicherungsverfahrens
- Festlegung des Sicherungsmediums
- Auswahl der Sicherungshardware
- Auswahl der Sicherungssoftware
- Installation Sicherungshardware und -Software
- Einrichtung der Datensicherung
- Testen der Datensicherung
- Benennung einer verantwortlichen Person für die Datensicherung

### Schritt 1: Ermittlung der zu sichernden Datenmenge

Stellen Sie zuerst fest, wie umfangreich die Menge der Daten ist, die gesichert werden muss. Die Menge wird u.a. bei der Auswahl des Sicherungsmediums und des Sicherungsgerätes eine Rolle spielen. Sie wird auch eine Rolle spielen bei der Lizenzierung der Sicherungssoftware (z.B. dann, wenn Sie mehrere Server sichern müssen).

### Schritt 2: Festlegung des Sicherungsverfahrens

Dass wir über die Einführung einer Datensicherung mit GFS-Rotationsverfahren sprechen, steht außer Frage.
Sie müssen noch festlegen, wie Sie die Daten sichern wollen: komplette Sicherung, differenzielle oder inkrementelle Sicherung?
I.d.R. wird eine komplette tägliche Datensicherung angestrebt, da im Falle einer Sicherung die Daten schneller wiederhergestellt werden können, ohne mehrere Bänder zurücksichern zu müssen. Bei sehr großer Datenmenge (> 200 GB) spielt hier das Zeitfenster für die Durchführung der Datensicherung eine Rolle. Es muss geklärt werden, ob die komplette Datensicherung jeden Tag ausgeführt werden kann, ohne dass die Gefahr besteht, dass die Daten im Zugriff sind.

### Schritt 3: Festlegung des Sicherheitsmediums

Wenn Klarheit darüber besteht, wie umfangreich die Daten sind (Datenmenge), die gesichert werden müssen, können auch das Sicherungsmedium und das Sicherungsgerät ausgewählt werden: DAT-, DLT- oder LTO-Bänder?

### Schritt 4: Auswahl Sicherungshardware

Nachdem Sie das Sicherungsmedium festgelegt haben, können Sie das Sicherungsgerät aussuchen und auswählen, das zu den von Ihnen definierten Anforderungen (DAT, DLT, LTO, einfaches oder Gerät mit Autoloaderunterstützung?) passt.

### Schritt 5: Auswahl der Sicherungssoftware

Für die Auswahl der Sicherungssoftware müssen Sie wissen, ob die Software die von Ihnen ausgewählte Hardware unterstützt (z.B. Autoloaderunterstützung?).
Bezogen auf die Lizenzierung der Software spielt u.a. die Anzahl der Server und Anzahl der Clients, die gesichert werden müssen, eine Rolle.

### Schritt 6: Installation der Sicherungshardware und -Software

Wenn die Software und Hardware ausgewählt, bestellt und geliefert worden sind, können sie installiert werden.

### Schritt 7: Einrichtung der Datensicherung

Nach der erfolgreichen Installation der Sicherungskomponenten kann die Sicherungssoftware nach Ihrer Vorgabe konfiguriert werden (Einrichtung der GFS-Rotation, Festlegung des Sicherungsverfahrens ...).

Nachdem die Sicherungssoftware grundsätzlich konfiguriert worden ist, müssen Sie sich zeigen lassen,

- wie die Sicherungsprotokolle überprüft werden können,
- wie Rücksicherungen durchgeführt werden können und
- wie gesonderte Sicherungen gestartet werden können.

Die Überprüfung der Protokolle kann entweder direkt vor Ort stattfinden (über die Sicherungssoftware) oder – je nach Software – die Protokolle werden per Fax/E-Mail an den Systembetreuer, der die Überprüfung übernimmt, automatisch versandt.

### Schritt 8: Testen der Datensicherung

Nachdem die Datensicherung jetzt funktionsfähig eingerichtet ist, sollte noch überprüft werden, ob sich die gesicherten Daten auch wieder zurücksichern lassen. Legen Sie dazu ein Testverzeichnis auf dem Server an. In dieses Verzeichnis kopieren Sie verschiedene Dateien (kleine und große). Nachdem diese Daten dann gesichert wurden, löschen Sie das Testverzeichnis und sichern diese Daten wieder vom Bandlaufwerk zurück.
Dieser Test sollte in regelmäßigen Abständen durchgeführt werden.

### Schritt 9: Benennung einer verantwortlichen Person für die Datensicherung

Benennen Sie eine Person innerhalb Ihres Unternehmens inkl. eines Stellvertreters, die für die Überwachung der Datensicherung und eine eventuelle Wiederherstellung der Daten verantwortlich sowie Ansprechpartner rund um die Datensicherung ist.

## 3.2. Beispiel

Für die Datensicherung des Unternehmens-Servers hat sich herausgestellt, dass insgesamt ca. **30 GB** gesichert werden müssen. Da die zu sichernde Datenmenge relativ klein ist, wird damit gerechnet, dass die komplette Datensicherung innerhalb kürzester Zeit (ca. 1 Stunde) durchgeführt ist. Es ist entschieden worden, dass die Daten **täglich komplett** gesichert werden (somit gestaltet sich die Rücksicherung etwas einfacher).
Auf Grund der aktuellen Datenmenge wird ein **DDS4-Streamerlaufwerk** mit Autoloader (für 6 DDS4-Bänder) eingesetzt.

Die Sicherungssoftware, die eingesetzt wird, ist eine Standardsoftware von Computer Associates International, Inc.: Brightstor ARCserve Backup für Windows. Die Software ermöglicht die Sicherung von Windowsserver-Systemen und unterstützt das ausgewählte Autoloader-Streamergerät.
Mit Hilfe der Software wird ein sog. Job konfiguriert (GFS-Rotation), der die automatische komplette Sicherung des Servers übernimmt.

Folgende Sicherungsbänder werden benötigt:

- **4 Bänder** für die täglichen Sicherungen (Band **T1-T4**)
- **4-5 Bänder** für die Wochensicherungen (Band **W1-W5**) und
- **12 Bänder** für die Monatssicherungen (Band **M1-M12**)

Im Autoloader werden 5 Bänder geladen: Sicherungsbänder **T1-T4** (tägliche Datensicherungen Montag-Donnerstag). Somit wird der Bandwechsel für die tägliche Sicherung automatisch vom Autoloader übernommen. Das Sicherungsband **W1** wird für die Datensicherung am Freitag ebenfalls im Autoloader geladen.

Die Aufbewahrung der Bänder findet wie folgt statt:

- Die Bänder T1-T4 werden permanent im Autoloader belassen.
- Die Bänder W1-W5 werden an einem sicheren Ort hinterlegt (Beispiel: Firmen-Safe oder Bankschließfach). Der EDV- bzw. Sicherheitsverantwortliche muss spätestens Freitag das benötigte Band mitbringen.
- Die Bänder M1-M12 werden ebenfalls außerhalb des Firmengeländes aufbewahrt und zwar in einem Schließfach bei der Hausbank. Am Monatsende muss der EDV-Verantwortliche das benötigte Band aus dem Bank-Schließfach holen.

Im darauf folgenden Jahr müssen – aus Gründen des Materialverschleißes – mindestens die Bänder T1-T4 gegen neue Bänder ausgetauscht werden.

# 4. Datensicherung der ADDISON Softwarelösungen

## 4.1. Umfang der zu sichernden Daten

Der Umfang der zu sichernden Daten beinhaltet zum einen die Sicherung der entsprechenden Datenverzeichnisse und zum anderen die Sicherung der entsprechenden Datenbanken. Falls zusätzlich das ADDISON Online-Portal genutzt wird, sind hierzu ebenfalls Maßnahmen zu treffen.

Beachten Sie bitte auch den Abschnitt ***DocuWare***
***Zur (Rück-)***Sicherungen im Umfeld von DocuWare verweisen wir auf die Informationen des Herstellers selbst: http://help.docuware.com/de/#b57864t59282n56783

## 4.2. tse:nit banking

### 4.2.1. Zu (rück)sichernde Bewegungsdaten

Die tse:nit banking Bewegungsdaten befinden sich in der Regel auf dem Datenserver im Verzeichnis **10it_Banking_Daten.** Dies gilt sowohl für die lokale Ordnerbezeichnung, als auch für eine UNC-Freigabe.

Zu den Bewegungsdaten zählen die Dateien in folgenden Unterverzeichnissen

**..\Backup**

Kopien der DB_zp_10it_Banking (erstellt mit dem tse:nit banking administrations tool)

**..\TEMP**

internes Verzeichnis für die Ablage temporärer Dateien

**..\XMLExport**

Exportpfad der Kontoumsätze für den tse:nit Bankauszug

### 4.2.2. SQL Server Datenbank

Zum Sicheren und Wiederherstellen beachten Sie bitte die Abschnitte ***Empfohlene Vorgehensweisen zur Sicherung von SQL Server*** Datenbanken und *Fehler! Verweisquelle konnte nicht gefunden werden.* aus dem Kapitel der ADDISON Aktenlösung.

## 4.3. tse:nit DMS

Da die Informationen im Archiv selbst, in der Verwaltungsdatenbank für SAPERION (DB_SAPERION) und in der tse:nit Datenbank (standardmäßig: DB_10IT) zueinander passen müssen, muss eine möglichst zeitnahe Sicherung des 10itDMS-Verzeichnisses auf dem Archivserver sowie der Datenbank DB_SAPERION und der tse:nit-Datenbank eingerichtet werden.

Daten außerhalb der Software-Verzeichnisstruktur.

## 4.4. Synchronität der Sicherung

Um eine Synchronität zwischen den in der Datenbank enthaltenen Daten und den Datenverzeichnissen zu erreichen, sollte die Sicherung zu einem Zeitpunkt erfolgen, an dem keine Änderungen im Datenbestand vorgenommen werden. Im Idealfall bedeutet das, dass kein Mitarbeiter mehr in der entsprechenden Software angemeldet ist.

# 5. ADDISON Software

## 5.1. Zu (rückzu)sichernde Datenverzeichnisse

Bei einer Standardinstallation der ADDISON-Anwendungen (wie Kanzleiorganisation, Finanzbuchhaltung, Controlling ...) werden die **kundenspezifischen Daten unterhalb des ADDISON-Applikationsverzeichnisses gespeichert**. Das Installationsverzeichnis wird im Rahmen der ersten Installation abgefragt und lautet standardmäßig „ADDISON\Software“.
Kundenspezifische Daten/Dateien werden in folgenden Unterverzeichnissen gespeichert:

### ...\DB\DBKANZ (inkl. aller Unterverzeichnisse)

Darunter befindet sich die **ADDISON-Datenbank mit allen Daten, die pro Projekt** (Kanzleiorganisation, Finanzbuchhaltung usw.) **und pro Mandant/Firma erfasst worden sind**. Die Daten als solche sind in der Datei „“bjects.dat“ gespeichert. Weitere Informationen finden Sie im Abschnitt ***FastObjects Server Datenbank***.

### ...\CMS (inkl. aller Unterverzeichnisse)

Darunter werden u.a. die Office-Dokumente gespeichert, die innerhalb der Projekte ADDISON Jahresabschluss, ADDISON Controlling, ADDISON Jahresabschlusserstellung erstellt worden sind (unterhalb des Verzeichnisses „...CMS\BERICHTE“).

### ...\CONFIG (inkl. aller Unterverzeichnisse)

Darunter werden u.a. Konfigurations-/Steuerungsdaten für die ADDISON-Anwendungen (wie z.B. ADDISON Software, ADDISON Lohn- und Gehaltsabrechnung und ADDISON Steuern) gespeichert.

### ...\DATEN (inkl. aller Unterverzeichnisse)

Darunter werden benutzerspezifische Daten/Dateien aus ADDISON-Anwendungen gespeichert wie z.B. Office-Dokumente, die aus den ADDISON-Anwendungen erstellt worden sind, Listen aus dem Listenmanager, Daten aus dem ADDISON Online-Portal, von der Finanzverwaltung abgerufene E-Steuerbelege sowie diverse Dateien aus Controlling, Finanzmanager und anderen Beratungsprodukten.

Darunter werden auch benutzerspezifische Einstellungen (unterhalb von UserProfile) gespeichert.

### ...\Internet Assistent\ISetup.ini

In dieser Datei werden u.U. individuelle Anpassungen zur automatischen Installation, E-Mail-Benachrichtigung etc. gespeichert.

### ...\LISTEN (inkl. aller Unterverzeichnisse)

Darunter werden u.U. individuelle Anpassungen für div. Projekte gespeichert wie kundenspezifische Rechnungsvorlagen im Verzeichnis „...\listen\kanzlei\custom“ bzw. BMP-Dateien.

### ...\Vorlagen (inkl. aller Unterverzeichnisse)

Darunter werden die (Office-)Vorlagen gespeichert, die gegebenenfalls kundenindividuell erstellt worden sind.

Zur Sicherung der ADDISON-Daten empfehlen wir das komplette ADDISON-Software-Verzeichnis zu sichern, jedoch mindestens alle o.g. Verzeichnisse inkl. aller Unterverzeichnisse.

### Änderung der Datenverzeichnisstruktur

Mit der Auslieferung der DVD 3/2010 sind Datenverzeichnisse, die direkt unterhalb des Installationsverzeichnisses der ADDISON Software vorhanden waren, unterhalb von „...\DATEN“ migriert/übertragen worden.
Sollten Sie im Rahmen der Datensicherung die Verzeichnisse einzeln/gezielt sichern, so müssen die u.g. Verzeichnisse nicht mehr zwingend gesichert werden, da sie keine aktuellen kundenspezifischen Daten enthalten (sie wurden migriert).

Es handelt sich um:

### ...\ERIC (inkl. aller Unterverzeichnisse)

Darunter wurden u.a. die Elster-Protokolle der komprimiert gesendeten Jahreserklärungen, einschl. Anlagen EÜR und § 34 a, gespeichert.
Die PDF-Erläuterungen werden mittlerweile unter „...\DATEN\Mandantennummer“ gespeichert.

### ...\EXTERN (inkl. aller Unterverzeichnisse)

Darunter wurden Daten, die im Zusammenhang mit Datenübernahmen stehen, gespeichert.
Die Debitor- und Sollstellung-Ausgabedateien der Kanzleiorganisation werden mittlerweile unter „...\DATEN\Extern“ gespeichert.

### ...\FACTORING (inkl. aller Unterverzeichnisse)

Darunter wurden Ausgabedateien gespeichert, bevor sie an die DEGEV übermittelt werden.
Die DEGEV-Daten werden mittlerweile unter „...\DATEN\Factoring“ gespeichert.

### ...\FIBU (inkl. aller Unterverzeichnisse)

Darunter wurden Debitor-Sollstellung-Ausgabedateien aus der Kanzleiorganisation gespeichert. Die Debitor-Sollstellung-Ausgabedateien der Kanzleiorganisation werden mittlerweile unter „...\DATEN\Kanzlei\Fibu“ gespeichert.

### ...\IMPORT (inkl. aller Unterverzeichnisse)

Darunter wurden u.U. individuelle Anpassungen aus dem Controlling-Projekt gespeichert.
Der ADDISON Controlling-Anwender konnte auch unter „...\import\kost\“ ein Unterverzeichnis „custom“ angelegt haben, in das ggf. individuell abgeänderte Dateien zur Definition der Import- und Exportformate (kostimp.ini oder kostexp.ini) kopiert werden konnten.
In das Unterverzeichnis „...\import\kost\modelle“ konnten eigene Stammdatenmodelle exportiert werden - diese sind i.d.R. aber auch in der Datenbank gespeichert. Der Export dient zum Austausch der Stammdatenmodelle mit anderen Rechnern.

Diese Daten werden mittlerweile unter „...\DATEN\Import\Kost“ gespeichert.

### ...\Rechnungen (inkl. aller Unterverzeichnisse)

Darunter wurden die (Rechnungs-)Dokumente gespeichert, die in der ADDISON Kanzleiorganisation erstellt wurden.

Die (Rechnungs-)Dokumente der Kanzleiorganisation werden mittlerweile unter „...\DATEN\Rechnung“ gespeichert.

### ...\SRZ (inkl. aller Unterverzeichnisse)

Darunter wurden neben den eigentlichen Software-Komponenten für das Service-Rechenzentrum auch Daten für das bzw. vom SRZ gespeichert.
Die Daten für das bzw. vom SRZ werden mittlerweile unter „...\DATEN\SRZ“ gespeichert.

## 5.2. Datenbankserver

Beachten Sie hierzu bitte den Abschnitt ***FastObjects Server Datenbank***.

# 6. ADDISON Aktenlösungen

## 6.1. Zu (rückzu)sichernde Bewegungsdaten

Die Bewegungsdaten der ADDISON Aktenlösungen 8tse:nit und cs:Plus) befinden sich in der Regel auf dem Datenserver im Verzeichnis **10it_Daten bzw. csPlus_Daten.** Dies gilt sowohl für die lokale Ordnerbezeichnung als auch für eine UNC-Freigabe.

Zu den Bewegungsdaten zählen die Dateien in folgenden Unterverzeichnissen:

### ...\Banking

Dateien für tse:nit banking (Kontoauszüge und DTAUS-Dateien)

### ...\BerSt

Vorlagen für die Steuerberechnung (Excel)

### ...\Daten\Beratungssysteme

Dateien für Beratungswerkzeuge

### ...\Daten\DatenElster

Dateien für das integrierte Elster-Versendemodul

### ...\Daten\E-Mail

Dateien der „Liste der E-Mails“

### ...\Daten\Kanzleimonitoring

Dateien des Kanzleimonitorings

### ...\Daten\NGCMS

Vorlagen-Dateien für NG-Komponenten

### ...\Daten\NGDaten

Daten für NG-Komponenten

### ...\Daten\NGDB[1]

FastObjects Datenbank. Weitere Informationen finden Sie im Abschnitt ***FastObjects Server Datenbank***.

[1] Gilt nur für tse:nit

**...\Daten\Offenlegung**

Dateien für die Offenlegung

**...\Daten\Portal**

Dateien für das ADDISON Mandantenportal

**...\Daten\Rating**

Dateien für das Rating

**...\Daten\Sync**

Dateien für programminterne Abgleichvorgänge

**...\Daten\Unternehmensdiagnose**

Dateien für die Unternehmensdiagnose

**...\Daten\ZM_Online**

EG-ZM-Daten

**...\Doku**

Ablage von über tse:nit | cs:Plus erstellten Office-Dokumenten (Word und Excel)

**...\Elster**

Dateien für das separate Elster-Versendemodul

**...\GDPdU**

GDPdU-Auslagerungsdateien

**...\LST**

Druckvorlagen

**...\Prima**

Daten der Primanoten-Erfassung

**...\Protokolle**

Verschiedene Protokolldateien

**...\RechAnl**

Rechnende Anlagen zu Steuererklärungen

**...\SAP**

Übergabedateien zu SAP

### ...\Stempeltext

Stempeltexte für Mantelbögen

### ...\Textbausteine

Dateien der Textbausteine inkl. Vorlagen

### ...\Transfer

Transferdateien

### ...\TransferSave

Transferdateien

### ...\User

Mitarbeiter-spezifische Dateien

### ...\Vorlagen

Vorlagen für über tse:nit | cs:Plus erfasste Office-Dokumente (Microsoft Word, Microsoft Excel)

### ...\WebDokumente

Ablage von Dokumenten aus dem Internet

### ...\WiederBuchungen

Wiederholungsbuchungen

Darüber hinaus empfehlen wir, auf jedem Arbeitsplatz die Datei Normal.dot der Microsoft-Office-Installation sowie die Dateien und Verzeichnisse in folgenden Unterverzeichnissen des Installationsverzeichnisses von tse:nit | cs:Plus zu sichern:

### ...\Metafile

Metafiles

### ...\ExpCSV

Exportdateien

### ...\LogFile

Log-Dateien des Datenexports

### ...\Prima

Primanota für Buchungssätze

Bei einer Einzelplatzinstallation können die o.a. Verzeichnisse im Programmverzeichnis von tse:nit | cs:Plus vorhanden sein. Dies gilt insbesondere für ältere Installationen.

### 6.1.1. Methoden der Sicherung

Die Bewegungsdaten können zum Beispiel mit einer gängigen Sicherungs-Software gesichert werden. Es wird empfohlen, das Verzeichnis der Bewegungsdaten komplett inkl. aller Unterverzeichnisse zu sichern.

## 6.2. FastObjects Datenbank

Beachten Sie hierzu bitte den Abschnitt ***FastObjects Server Datenbank***.

## 6.3. SQL Server Datenbank

### 6.3.1. Voraussetzungen

Um eine Datensicherung durchzuführen oder die nachfolgend beschriebenen Einstellungen vorzunehmen, benötigen Sie das Microsoft SQL Server Management Studio. Das Microsoft SQL Server Management Studio ist das primäre Administrationstool für Microsoft® SQL Server™ und ist Bestandteil des SQL Servers.

Nachfolgend werden weitere wichtige Voraussetzungen genannt.

#### Service-Pack-Versionen

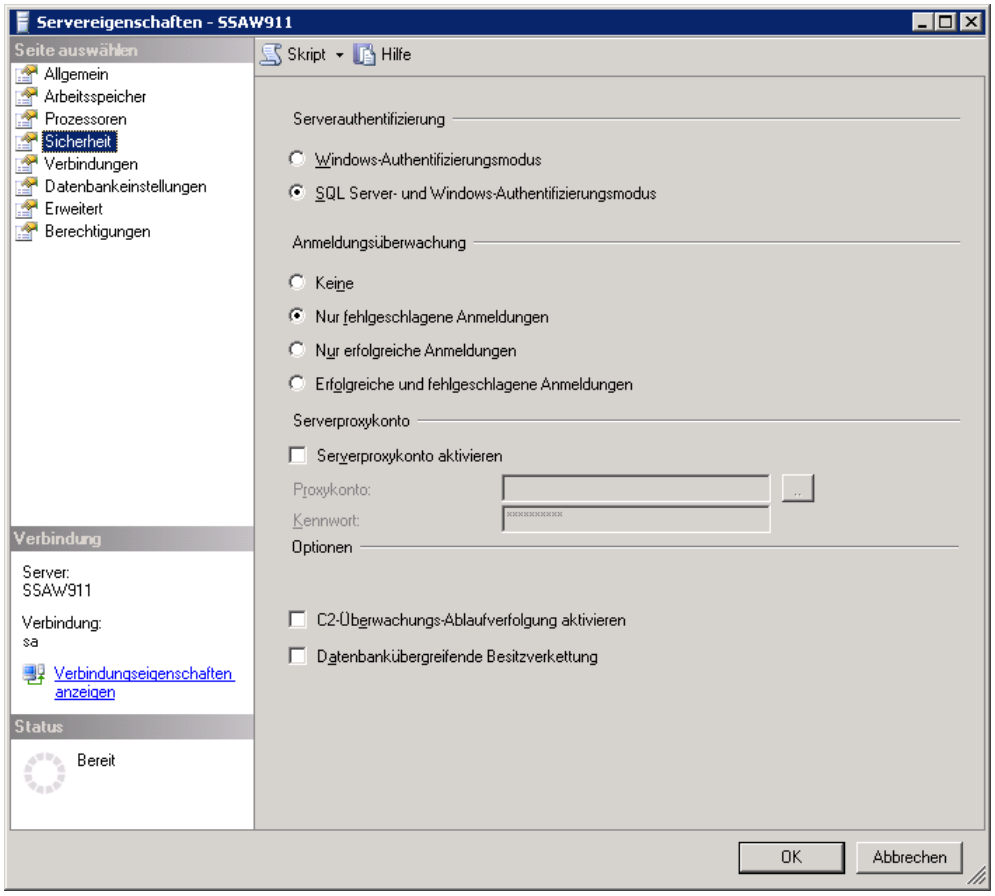
Installieren Sie nach dem SQL Server auch das aktuell verfügbare Service Pack.
Für den Einsatz des SQL Servers werden bestimmte Service Packs vorausgesetzt. Entsprechende Informationen hierzu finden Sie in dem Dokument „Systemvoraussetzungen“.

Über welches Service Pack Ihr SQL Server verfügt, können Sie mit Hilfe der Task **Analyse | Datenbankinformation | Ausführen ...** im Programm tse:nit | cs:Plus administration tools feststellen. Oder entnehmen Sie diese Information dem Microsoft SQL Server Management Studio, indem Sie im Kontextmenü des Objekt Server den Befehl „Info“ aufrufen.

#### Administrator-Passwort

Bitte achten Sie darauf, dass bei Ihrem SQL Server unbedingt ein Passwort für den Administrator-Zugang (Datenbankbenutzer sa) vergeben wird. Wie heise online berichtete, besteht ansonsten die Gefahr eines Befalls durch Computerviren. Fragen Sie gegebenenfalls Ihren Systembetreuer, ob er für den Benutzer sa ein Kennwort vergeben hat.

Dieses Passwort sollte zur Administrierung der Datenbank bekannt sein. Bei der - von uns empfohlenen - gemischten Authentifizierung besteht weiterhin die Möglichkeit, sich mit einem Windows-Benutzer-Konto anzumelden. Diese Eigenschaft des SQL Servers kann im Microsoft SQL Server Management Studio (Rechtsklick auf **Objekt Server | Eigenschaften | Object Sicherheit**) eingestellt werden.




## Microsoft SQL Server Management Studio

Das Microsoft SQL Server Management Studio ist ein Programm des SQL Servers, das Ihnen Möglichkeiten zur Wartung und Administration Ihrer tse:nit | cs:Plus Datenbank zur Verfügung stellt.

### 6.3.2. Eigenschaften der Datenbank

Starten Sie das Microsoft SQL Server Management Studio und öffnen Sie den Eigenschaftendialog für Ihre Datenbank.


Die Option „Rekursive Trigger“ muss aktiviert sein. Ist diese Option nicht aktiviert, sind schwerwiegende Fehler in der Datenbank nicht auszuschließen, die eine Weiterarbeit mit tse:nit | cs:Plus unmöglich machen. Sie finden diesen Punkt unter den Optionen der Datenbankeigenschaften.

### 6.3.3. Wiederherstellungsmodell

Sie können für jede Datenbank in Microsoft® SQL Server™ unter drei Wiederherstellungsmodellen auswählen, um zu bestimmen, wie die Daten gesichert werden sollen und welches Risiko des Datenverlustes Sie eingehen möchten. Die folgenden Wiederherstellungsmodelle sind verfügbar:

#### Einfache Wiederherstellung

Mit der einfachen Wiederherstellung kann die Datenbank bis zur letzten vollständigen Sicherung der Datenbank wiederhergestellt werden. Es wird keine Folge von Transaktionsprotokollen gesichert. Eine einfache Wiederherstellung kann empfohlen werden, wenn es sich zum Beispiel um eine Einzelplatzinstallation mit geringen Veränderungen des Datenbestandes handelt oder nur wenig freier Speicherplatz auf der Festplatte zur Verfügung steht.

#### Vollständige Wiederherstellung

Mit der vollständigen Wiederherstellung kann die Datenbank bis zum Auftreten des Fehlers wiederhergestellt werden.
Beim Verlust einer Datenbank können Sie die Daten wiederherstellen, indem Sie die letzte Datenbanksicherung und anschließend jede Protokollsicherung wiederherstellen, die seit der Datenbanksicherung erstellt wurde. Hierzu muss die Folge von Protokollsicherungen jeden Protokolleintrag enthalten, der seit der letzten Datenbanksicherung geschrieben wurde. Wenn Sie eine Folge von Transaktionsprotokollsicherungen verwalten, darf ein Protokolleintrag erst dann abgeschnitten werden, wenn er in eine Protokollsicherung geschrieben worden ist.
Wir empfehlen, bei der Option „Wiederherstellungsmodell“ die Auswahl „vollständig“ zu wählen. Die im Folgenden beschriebene Transaktionsprotokollsicherung ist nur bei dieser Einstellung möglich. In tse:nit | cs:Plus Datenbanken ist dieses Wiederherstellungsmodell standardmäßig eingestellt.

#### Massenprotokollierte Wiederherstellung

Das Modell der massenprotokollierten Wiederherstellung bietet Schutz vor Medienfehlern und zugleich die beste Leistung und den geringsten Verbrauch an Protokollspeicherplatz für bestimmte umfangreiche Vorgänge oder Massenkopiervorgänge.
Beim Modell der massenprotokollierten Wiederherstellung ist die Gefahr des Datenverlustes bei diesen Massenkopiervorgängen höher als beim Modell der vollständigen Wiederherstellung. Eine beschädigte Datendatei kann dazu führen, dass Daten erneut manuell eingegeben werden müssen.

### 6.3.4. Verkleinern der Datenbankdateien beim SQL Server

SQL Server ermöglicht, dass jede Datei innerhalb einer Datenbank verkleinert wird, um nicht verwendete Speicherbereiche zu entfernen. Sowohl Daten- als auch Transaktionsprotokolldateien können dabei verkleinert werden.
Ist also z.B. die Festplatte mit den SQL Server Datenbanken voll und ist im Microsoft SQL

Server Management Studio oder im Explorer (Datei db_10it_log.ldf | db_rewe_log.ldf) zu sehen, dass das Transaktionsprotokoll viel zu groß ist (mehrere Hundert Megabyte), sind folgende Aktionen durchzuführen:

### Datenbank verkleinern

Im Microsoft SQL Server Management Studio über die rechte Maustaste das Kontextmenü der Datenbank aufrufen. Über **Tasks | Verkleinern | Datenbank** kann die Datenbank verkleinert werden.

Das Verkleinern einer Transaktionsprotokolldatei führt nicht zum sofortigen Verkleinern der Datei; stattdessen wird die Datei für die spätere Verkleinerung beim nächsten Abschneiden des Transaktionsprotokolls gekennzeichnet.

## 6.3.5. Methoden der Sicherung

Beim Microsoft SQL Server besteht eine Datenbank aus zwei Dateien, die sich im Unterverzeichnis „Data“ des während der Installation des Microsoft SQL Server angegebenen Datenverzeichnisses befinden.

Diese Dateien heißen **db_10it.mdf | db_rewe.mdf** (Datenbankdatei) und **db_10it_log.ldf | db_rewe_log.ldf** (Transaktionsprotokoll) und befinden sich bei einer Standardinstallation im Datenverzeichnis

- C:\PROGRAMME\MICROSOFT SQL SERVER\MSSQL.1\DATA (Neuinstallation von SQL Server) oder
- C:\PROGRAMME\MICROSOFT SQL SERVER\MSSQL$ADDISON_AKTE\DATA (Installation der SQL Server Express Edition über die tse:nit | cs:Plus administration tools).

Diese Dateien können nicht direkt mit einer externen Sicherungssoftware gesichert werden, solange der Dienst MSSQLServer läuft.

Zum Durchführen der Sicherung der Datenbank sind grundsätzlich drei Varianten möglich:

1. Interne Sicherung der Datenbank inklusive des Transaktionsprotokolls über das SQL Server Management Studio auf Festplatte und Sichern der bei dieser Sicherung erstellten Dateien mit einer externen Sicherungssoftware. Dieses ist die von uns empfohlene Methode und im Abschnitt ***Empfohlene Vorgehensweisen zur Sicherung von SQL Server Datenbanken*** werden entspechende Verfahren näher beschrieben.

2. Wenn Sie gängige Sicherungssoftware zur Sicherung der Datenbank nutzen wollen, bieten Ihnen diese Programme eine Erweiterung um einen sog. „SQL Server Agenten“, die auch ohne weitere Maßnahmen des Anwenders das Sichern von SQL Server Datenbanken ermöglicht.

Wenn Sie eine derartige Sicherungsmethode nutzen wollen, so lassen Sie sich durch einen Fachmann über die Einsatzmöglichkeiten und Voraussetzungen informieren.

3. Beenden der Dienste MSSQLServer und SQLServerAgent mit dem SQL Server Configuration Manager vor dem Start der Sicherung und erneutes Starten nach dem Beenden der Sicherung, um die Datenbankdateien **db_10it.mdf | db_rewe.mdf** und die LOG-Datei **db_10it_log.ldf | db_rewe_log.ldf** direkt zu sichern.

   Geben Sie in **Start | Ausführen** folgende Befehle ein:

   vor der Sicherung:
   ```
   NET STOP MSSQLSERVER
   ```
   oder
   ```
   NET STOP MSSQL$<NAME DER SQL SERVER-INSTANZ>

   NET STOP SQLSERVERAGENT
   ```
   oder
   ```
   NET STOP SQLAgent$<NAME DER SQL SERVER-INSTANZ>
   ```

   nach der Sicherung:
   ```
   NET START MSSQLSERVER
   ```
   oder
   ```
   NET START MSSQL$<NAME DER SQL SERVER-INSTANZ>

   NET START SQLSERVERAGENT
   ```
   oder
   ```
   NET START SQLAgent$<NAME DER SQL SERVER-INSTANZ>
   ```

Wenn Sie den mit Hilfe der tse:nit | cs:Plus administration tools installierten SQL Server Express Edition nutzen und bei der Installation den Standardvorschlag bei „Name der Instanz“ auf ADDISON_AKTE belassen haben, dann heißt der Befehl:

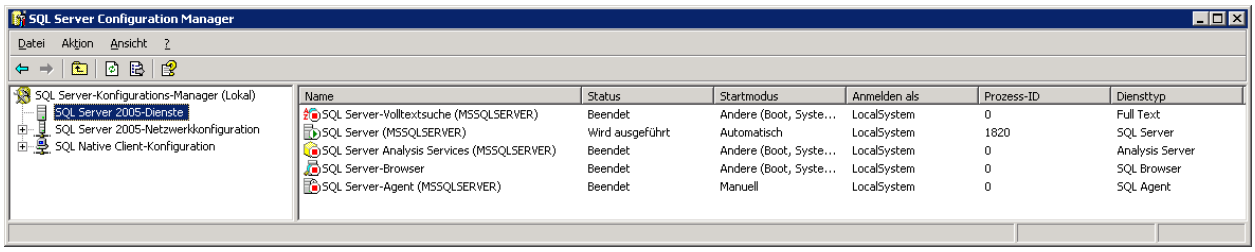
vor der Sicherung:
```
NET STOP MSSQL$ADDISON_AKTE
```

und nach der Sicherung:
```
NET START MSSQL$ADDISON_AKTE
```

Werden diese Befehle eingegeben, dann kann direkt kopiert oder durch eine Sicherungssoftware ein Backup erstellt werden. Sollen diese Befehle automatisch ausgeführt werden, so besteht die Möglichkeit, die Befehlsfolge als entsprechende Aufgabe in

**Systemsteuerung | Geplante Tasks** einzurichten.

Vergleichbar ist dies mit dem Ausführen des Befehls „Beenden“ bzw. „Starten/Weiter“ im SQL Server Configuration Manager.




Die Methoden 2 und 3 werden von uns für Mehrplatzinstallationen mit vollständigem Wiederherstellungsmodell (Standardeinstellung für Mehrplatzinstallationen, vgl. Abschnitt ***Wiederherstellungsmodell***) als alleinige Methode jedoch nicht empfohlen. Falls Sie diese Variante dennoch verwenden wollen, richten Sie Wartungspläne für den SQL Server ein, um unter anderem einem übermäßigen Anwachsen des Transaktionsprotokolls vorzubeugen (siehe Datenbank-Wartungsplan). Sollte es sich aber um eine Einzelplatzinstallation mit einfachem Wiederherstellungsmodell handeln (Standardeinstellung für Einplatzinstallationen, vgl. Abschnitt ***Wiederherstellungsmodell***), dann ist dies nicht notwendig.

Außerdem empfehlen wir, zusätzlich zur tse:nit | cs:Plus Datenbank auch die Datenbanken MASTER und MSDB zu sichern, damit bei einer Neuinstallation des SQL Servers die Datenbank ohne weitere auszuführende Befehle und Prozeduren zurückgesichert werden kann.

Die msdb-Datenbank enthält zum Beispiel einen vollständigen Verlauf aller Sicherungs- und Wiederherstellungsvorgänge auf dem Server. Das Management Studio verwendet diese Informationen, um einen Wiederherstellungsplan vorzuschlagen und auszuführen, der im Bedarfsfall zum Wiederherstellen einer Datenbank verwendet werden kann. Wenn z.B. jede Nacht eine Datenbanksicherung für eine Benutzerdatenbank erstellt wird und die Sicherungen des Transaktionsprotokolls tagsüber stündlich erstellt werden, werden die im Sicherungsverlauf enthaltenen Informationen in der msdb-Datenbank gespeichert. Wenn die Benutzerdatenbank wiederhergestellt werden muss, kann Microsoft SQL Server Management Studio mit Hilfe der in der msdb-Datenbank gespeicherten Verlaufsinformationen alle Sicherungen des Transaktionsprotokolls, die sich auf eine bestimmte Datenbanksicherung beziehen, beim Wiederherstellen der Datenbanksicherung anwenden.

Sollten Sie sich für den Einsatz von SQL Server Express Edition als Datenbankserver entschieden haben, so steht Ihnen die Methode 1 nicht zur Verfügung. Hier sollten Sie, wie in ***Methode 3*** geschildert, die Dienste stoppen und die entsprechenden Datenbankdateien und das Verzeichnis der Bewegungsdaten sichern.

### 6.3.6. Empfohlene Vorgehensweisen zur Sicherung von SQL Server Datenbanken

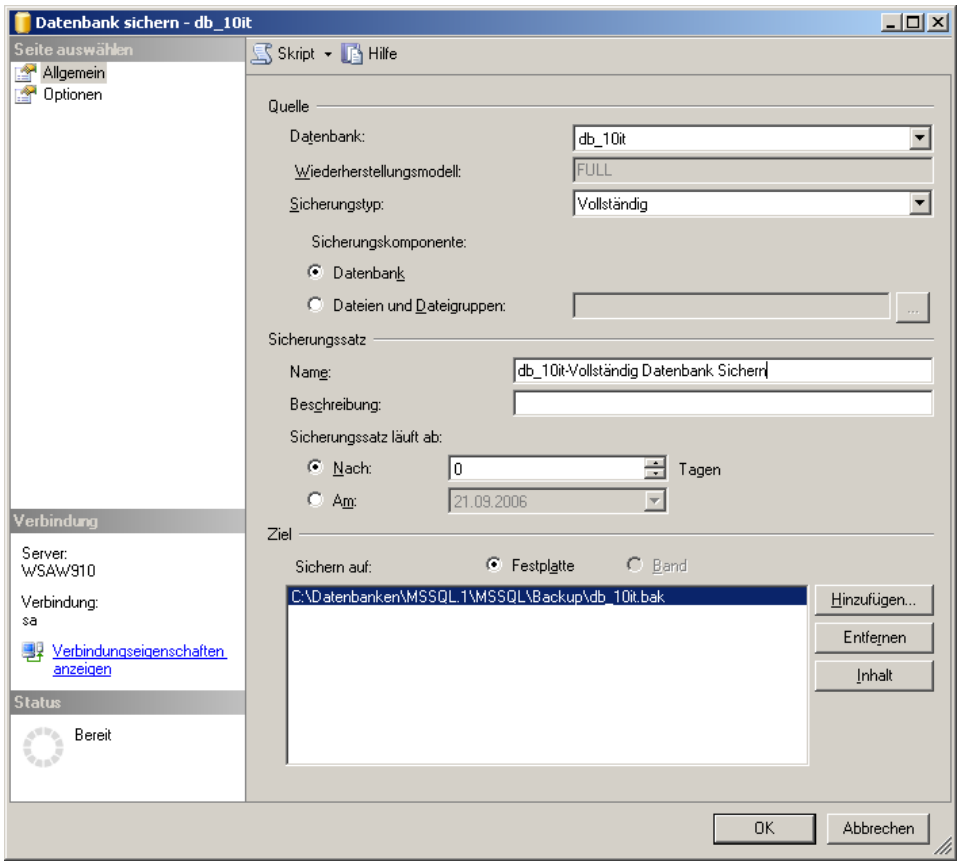
In diesem Abschnitt schildern wir, wie Sie mit Hilfe des SQL Servers Sicherungen durchführen können. Dabei stellen wir ein sehr einfaches Verfahren vor, um die Datenbank zu sichern. Anschließend erläutern wir eine mögliche Erweiterung durch einen Zeitplan und schließlich die Einrichtung eines Wartungsplanes.

#### Manuelle Sicherung mit dem Microsoft SQL Server Management Studio

Dieses Verfahren bietet die Möglichkeit, einfach und schnell eine Sicherung der Datenbank mit Hilfe des SQL Server Management Studios auszuführen. Diese Vorgehensweise empfiehlt sich vor einem Update oder vor programminternen Anpassungen, die nur über ein Rücksichern rückgängig gemacht werden können.

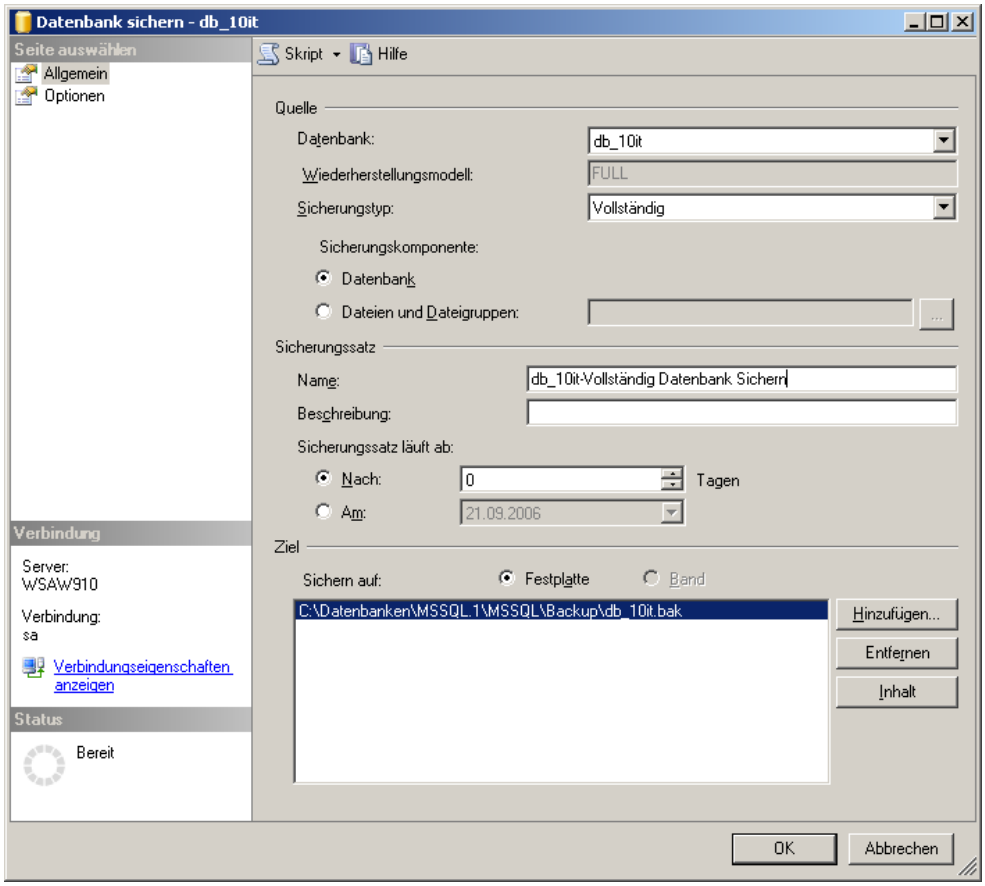
Ziel der Sicherung kann entweder eine Datei, die auf der Festplatte abgelegt wird, oder ein Bandlaufwerk sein. Es wird empfohlen, ein anderes Laufwerk (nicht nur eine andere Partition) als das Laufwerk mit den Originaldaten für diese Datei zu verwenden.

Da der SQL Server das Band in einem eigenen Format beschreibt, wird eine direkte Bandsicherung mit dem SQL Server in den wenigsten Fällen sinnvoll sein. Stattdessen kann die bei der Sicherung entstandene Datei dann wie die anderen zu sichernden Dateien auch im Rahmen der normalen (im Allgemeinen Band-)Sicherung gesichert werden.



Vorgehensweise:

- Starten Sie das Microsoft SQL Server Management Studio.
- Auswahl der Datenbank **db_10it | db_rewe** aus dem Ordner „Datenbanken“.
- Aktivieren des Kontextmenüs mit der rechten Maustaste und Starten des Dialogs „Sichern ...“ unter „Tasks“.
- Ggf. Eingabe eines Namens für die Sicherung.
- Optionale Eingabe einer Beschreibung für die Sicherung.
- Auswahl der Sicherungsmethode „vollständig“.
- Auswahl oder Hinzufügen des Sicherungsziels.
- Wählen der Option „An vorhandenen Sicherungssatz anfügen“ im Reiter „Optionen“.
- Start des Sicherungsprozesses mit [OK].





Die Option „An vorhandenen Sicherungssatz anfügen“ setzt voraus, dass entsprechender Platz auf der Festplatte vorhanden ist. Auch sollte die erstellte Sicherungsdatei durch eine externe Sicherungssoftware zum Beispiel auf ein Sicherungsband gesichert werden, wenn die Sicherungsdatei aufbewahrt werden soll.

## Automatisches Sicherungsverfahren

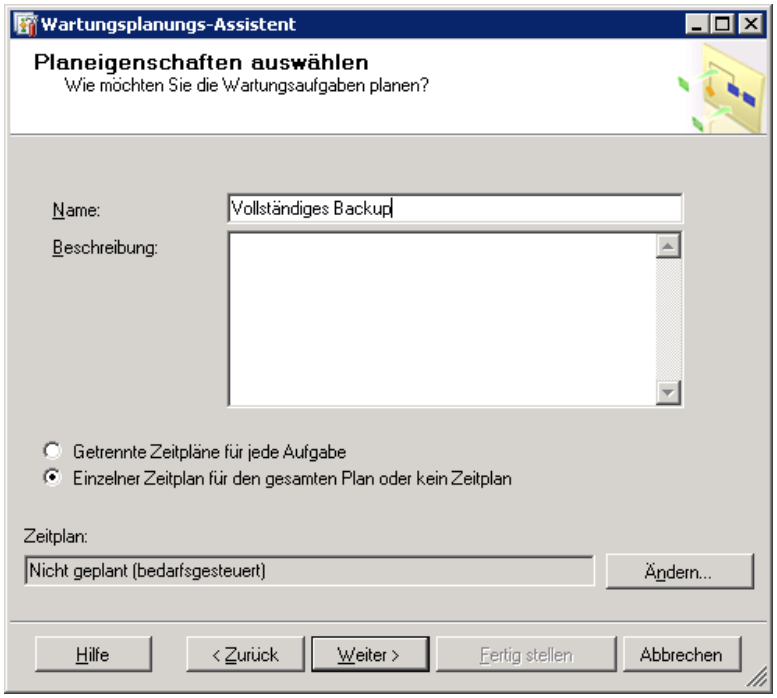
Die Einrichtung eines Wartungsplanes erlaubt Ihnen die Einrichtung eines automatischen Sicherungsverfahrens. Der Vorteil besteht darin, dass Sie eine fortlaufende Sicherung erhalten, ohne diese immer wieder manuell starten zu müssen.

Der Nachteil dieser Methode ist, dass bei der Einstellung „An vorhandenen Sicherungssatz anfügen“ ein entsprechend großer Datenträger vorhanden sein muss. Die Einstellung „Alle vorhandenen Sicherungssätze überschreiben“ hat den Nachteil, dass die vorhergehende Sicherung nicht mehr vorhanden ist.

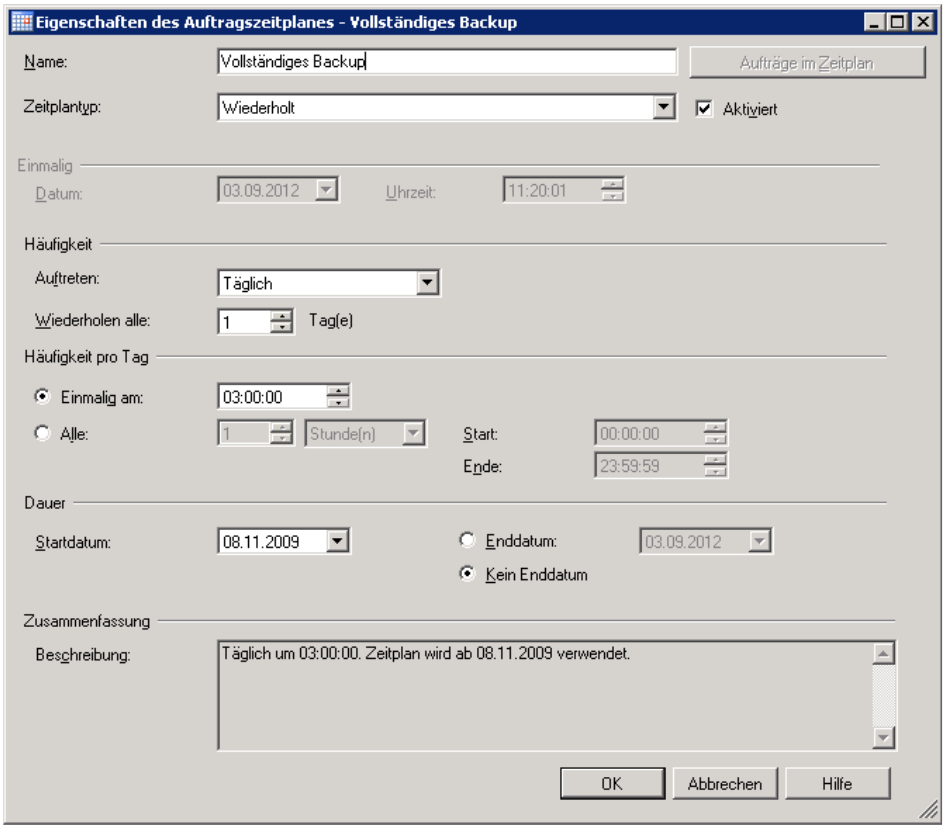
Eine empfehlenswerte Vorgehensweise ist es, eine regelmäßige Sicherung mit der Option „Alle vorhandenen Sicherungssätze überschreiben“ nach einem bestimmten Zeitplan zu erstellen und dann die erzeugte Sicherungsdatei mit einer speziellen Sicherungssoftware zum Beispiel auf ein Band zu sichern.

Vorgehensweise:

- Starten Sie das Microsoft SQL Server Management Studio.
- Erweitern Sie im Objekt-Explorer einen SQL Server und erweitern dann „Verwaltung“.
- Klicken Sie mit der rechten Maustaste auf „Wartungspläne“ und dann auf „Wartungsplan-Assistent“.
- Führen Sie die Schritte des Assistenten aus, um Ihren Wartungsplan zu erstellen.
- Beschreiben Sie zunächst Ihre Wartungstask.



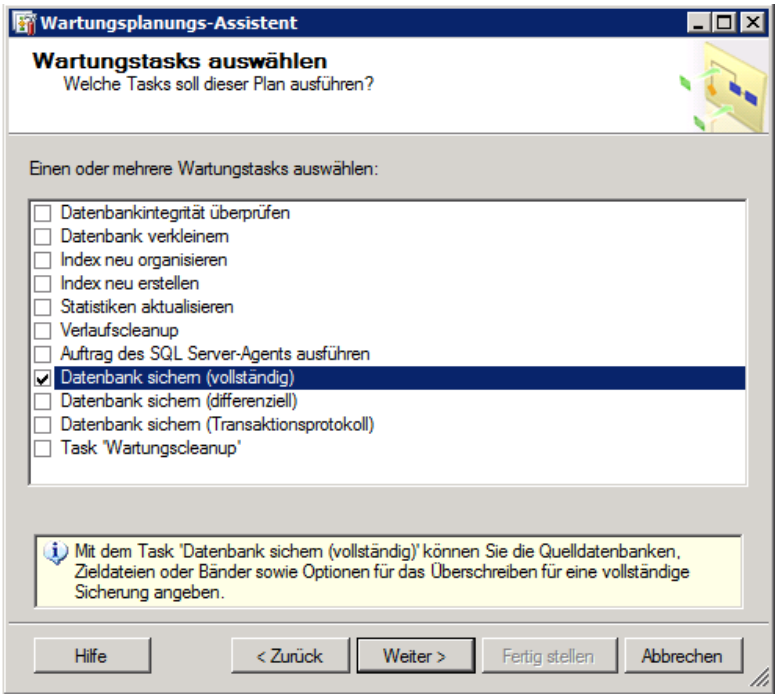
- Stellen Sie nun den Zeitplan und das Wiederholungsintervall ein. Öffnen Sie dazu durch Klick auf die Schaltfläche [Ändern ...] die Eigenschaften des Auftragszeitplanes.



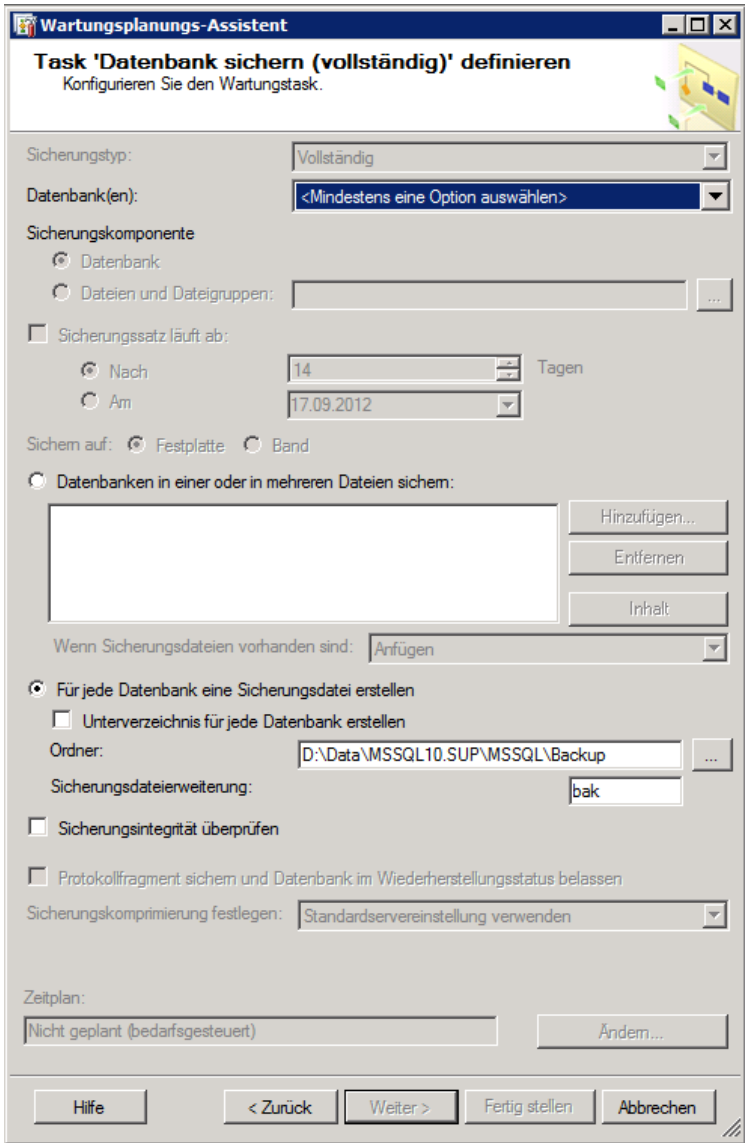

Empfohlen wird bei dieser Methode die Durchführung mindestens einer einmal täglichen vollständigen Datenbanksicherung. Bei starker Beanspruchung der Datenbank sollten zusätzlich zu der vollständigen Sicherung über den Tag verteilt Transaktionsprotokoll-sicherungen eingeplant werden (siehe „Transaktionsprotokollsicherung - Abschneiden des Transaktionsprotokolls“ ). Auch diese können mit Hilfe des Wartungsplan-Assistenten erstellt werden.

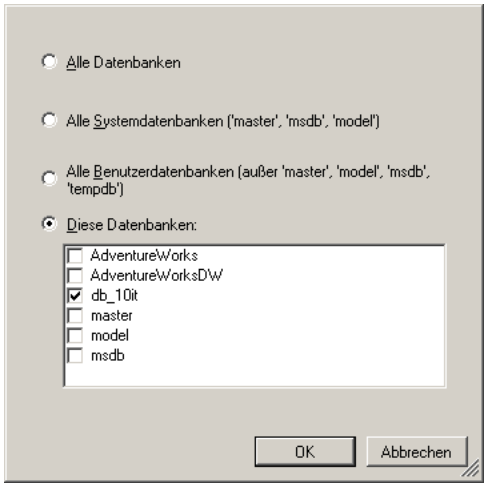
Damit die angegebenen Termine auch ausgeführt werden, ist der SQL Server Agent Dienst zu starten. Diesen konfigurieren Sie mit dem SQL Server Konfiguration Manager.

- Im nächsten Schritt wählen Sie die Aufgabe „Datenbank sichern (vollständig)“ aus und klicken auf [Weiter].




- Bestätigen Sie mit [Weiter] den Dialog „Wartungstaskreihenfolge“.
- Im darauf folgenden Dialog „Task 'Datenbank sichern (vollständig)'“ markieren Sie unter „Datenbanken“ Ihre tse:nit | cs:Plus Datenbank.


Wartungsplanungs-Assistent
Task 'Datenbank sichern (vollständig)' definieren
Konfigurieren Sie den Wartungstask.
Sicherungstyp:
Vollständig
Datenbank(en):
<Mindestens eine Option auswählen>
Sicherungskomponente
Datenbank
Dateien und Dateigruppen:
Sicherungssatz läuft ab:
Nach
14
Tagen
Am
17.09.2012
Sichern auf:
Festplatte
Band
Datenbanken in einer oder in mehreren Dateien sichern:
Hinzufügen...
Entfernen
Inhalt
Wenn Sicherungsdateien vorhanden sind:
Anfügen
Für jede Datenbank eine Sicherungsdatei erstellen
Unterverzeichnis für jede Datenbank erstellen
Ordner:
D:\Data\MSSQL10.SUP\MSSQL\Backup
Sicherungsdateierweiterung:
bak
Sicherungsintegrität überprüfen
Protokollfragment sichern und Datenbank im Wiederherstellungsstatus belassen
Sicherungskomprimierung festlegen:
Standardservereinstellung verwenden
Zeitplan:
Nicht geplant (bedarfsgesteuert)
Ändern...
Hilfe
< Zurück
Weiter >
Fertig stellen
Abbrechen


Alle Datenbanken
Alle Systemdatenbanken ('master', 'msdb', 'model')
Alle Benutzerdatenbanken (außer 'master', 'model', 'msdb', 'tempdb')
Diese Datenbanken:
AdventureWorks
AdventureWorksDW
db_10it
master
model
msdb
OK
Abbrechen

- Anschließend kann ein Ablageverzeichnis für die bei den Sicherungen erstellten Log-Dateien angegeben werden. Wahlweise besteht auch die Möglichkeit, die Log-Datei nach Abschluss des Sicherungsauftrages per E-Mail versenden zu lassen.
- Abschließend bestätigen Sie das Erstellen des Sicherungsauftrages mit Klick auf [Fertig stellen].

### Datenbank-Wartungsplan

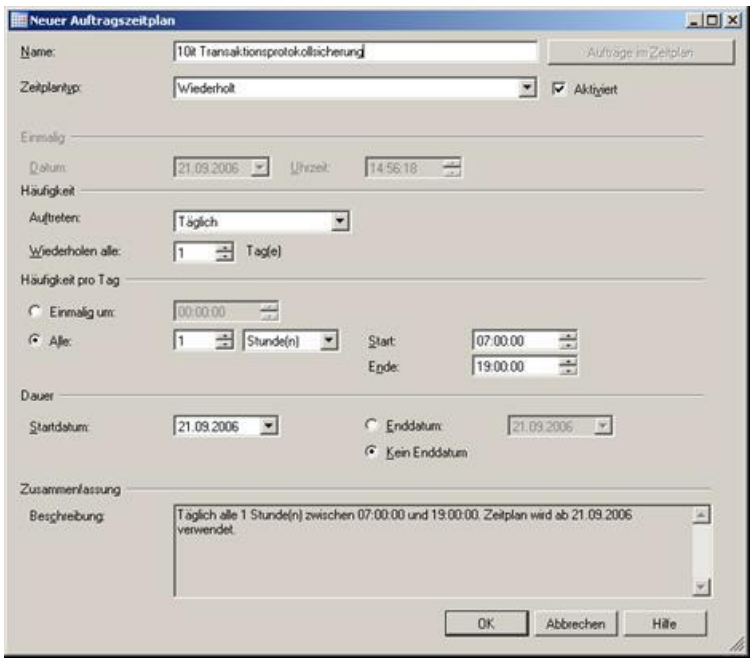
Voraussetzungen:


Um Aufgaben im Rahmen des Wartungsplans auszuführen, ist es erforderlich, dass der SQL Server Agent Dienst gestartet ist. Dieser Dienst implementiert den Agenten, der auf der Basis eines Zeitplans Tasks im Rahmen der SQL Server Administration ausführt. Für jede Instanz von SQL Server, die auf einem Computer ausgeführt wird, gibt es einen eigenen SQL Server Agent Dienst.

Bitte konfigurieren Sie den Dienst so, dass der SQL Server den Dienst automatisch startet. Der Status der ausgeführten Wartungspläne muss regelmäßig kontrolliert werden. Der SQL Server bietet hierzu diverse Unterstützungsdienste an, z.B. das automatisierte Versenden von E-Mails.

#### *Transaktionsprotokollsicherung - Abschneiden des Transaktionsprotokolls*

Durch Transaktionsprotokollsicherungen werden Sie in die Lage versetzt, den Status der Datenbank zu einem bestimmten Zeitpunkt (z.B. bis zu dem Zeitpunkt, bevor unerwünschte Daten eingegeben wurden) oder bis zu dem Punkt, an dem ein Fehler aufgetreten ist, wiederherzustellen.



Würde keine Löschung der Protokolleinträge aus dem Transaktionsprotokoll erfolgen, würde das logische Protokoll so lange wachsen, bis es den gesamten verfügbaren Speicherplatz auf dem Datenträger einnähme, auf dem sich die physischen Protokolldateien befinden. Von Zeit zu Zeit müssen alte Protokolleinträge, die zum Wiederherstellen einer Datenbank nicht mehr benötigt werden, gelöscht werden, um Speicherplatz für neue Protokolleinträge freizugeben. Der Vorgang, durch den diese Protokolleinträge gelöscht werden, um die Größe des logischen Protokolls zu verringern, wird als „Abschneiden des Protokolls“ oder „Protokollkürzung“ bezeichnet.

## Vorgehensweise:

Zur Erstellung eines Wartungsplanes müssen Sie ein Mitglied der festen Serverrolle sysadmin sein!

- Starten Sie das Microsoft SQL Server Management Studio.
- Erweitern Sie im Objekt-Explorer einen SQL Server und erweitern dann „Verwaltung“.
- Klicken Sie mit der rechten Maustaste auf „Wartungspläne“ und anschließend auf „Wartungsplan-Assistent“.
- Führen Sie die Schritte des Assistenten aus, um Ihren Wartungsplan zu erstellen.
- Stellen Sie nun den Zeitplan und das Wiederholungsintervall ein. Öffnen Sie dazu durch Klick auf die Schaltfläche [Ändern ...] die Eigenschaften des Auftragszeitplanes.
- Im nächsten Schritt wählen Sie die Aufgabe „Datenbank sichern (Transaktionsprotokoll)“ aus und klicken auf [Weiter].
- Bestätigen Sie mit [Weiter] den Dialog Wartungstaskreihenfolge.
- Im darauf folgenden Dialog „Task 'Datenbank sichern (Transaktionsprotokoll)'“ markieren Sie unter „Datenbanken“ Ihre tse:nit | cs:Plus Datenbank und bestätigen Sie den Dialog mit Klick auf [Weiter].
- Anschließend kann ein Ablageverzeichnis für die bei den Sicherungen erstellten Log-Dateien angegeben werden. Wahlweise besteht auch die Möglichkeit, eine Log-Datei nach Abschluss des Sicherungsauftrages per E-Mail versenden zu lassen.
- Abschließend bestätigen Sie das Erstellen des Sicherungsauftrages mit Klick auf [Fertig stellen].

Transaktionsprotokollsicherungen werden nur mit dem Modell der vollständigen Wiederherstellung bzw. dem Modell der massenprotokollierten Wiederherstellung verwendet. Es kommt vor, dass eine Transaktionsprotokollsicherung umfangreicher ist als eine Datenbanksicherung, beispielsweise dann, wenn eine Datenbank eine hohe Transaktionsrate aufweist, wodurch sich das Transaktionsprotokoll schnell vergrößert. In dieser Situation sollten Sie häufiger Sicherungen des Transaktionsprotokolls erstellen.

Das Wiederherstellen einer Datenbank mit Hilfe von Datenbank- und Transaktionsprotokollsicherungen funktioniert nur bei der Verwendung einer ununterbrochenen Sequenz von Transaktionsprotokollsicherungen nach der letzten Datenbanksicherung oder der letzten differenziellen Datenbanksicherung.

Führen Sie deshalb regelmäßig vollständige Datensicherungen durch. Empfohlen wird die tägliche vollständige Datensicherung.

Wenn der SQL Server das Sichern des Transaktionsprotokolls beendet, wird der inaktive Abschnitt des Transaktionsprotokolls automatisch abgeschnitten.

### Datenbankintegrität prüfen

Erstellen Sie mit Hilfe des Wartungsplan-Assistenten einen Wartungsplan zur Überprüfung der Datenbankintegrität.

Die Datenbankintegritätsprüfung sollten Sie mindestens einmal pro Woche durchführen lassen.

### Textberichte / Verlauf

Verwenden Sie Textberichte und/oder Verlaufsinformationen, um einen Bericht zu den von Microsoft® SQL Server™ ausgeführten Wartungsaktivitäten in einer Datei zu speichern bzw. in eine Tabelle zu schreiben.

### Wartungsplan und Systemdatenbanken

Wenn Sie einen Wartungsplan für die tse:nit | cs:Plus Datenbank einrichten, müssen Sie darauf achten, dass die Systemdatenbanken MASTER und MSDB folgende Voraussetzungen erfüllen:

- Stellen Sie für die Systemdatenbanken MASTER und MSDB grundsätzlich das einfache Wiederherstellungsmodell ein.
- Richten Sie für die Systemdatenbanken einen eigenen Wartungsplan ein.
- Führen Sie für die Systemdatenbanken keine Transaktionsprotokollsicherung durch. Dies ist beim einfachen Wiederherstellungsmodell nicht möglich.

Wenn diese Voraussetzungen nicht eingehalten werden, kann dies zu nicht vollständig ausgeführten Wartungsplänen führen. Auch Ihre - im Rahmen eines Wartungsplanes - eingerichtete Sicherung des Transaktionsprotokolls der tse:nit | cs:Plus Datenbank wird dann nicht ordnungsgemäß ausgeführt. In der Folge wird Ihr Transaktionsprotokoll nicht mehr verkleinert und wächst überproportional an.

## 6.3.7. Vorgehensweise zur Rücksicherung der Datenbank

Haben Sie eine Datenbanksicherung mit dem Microsoft SQL Server Management Studio Ihres SQL Servers erstellt, führen Sie eine Rücksicherung durch, wie in diesem Kapitel beschrieben.

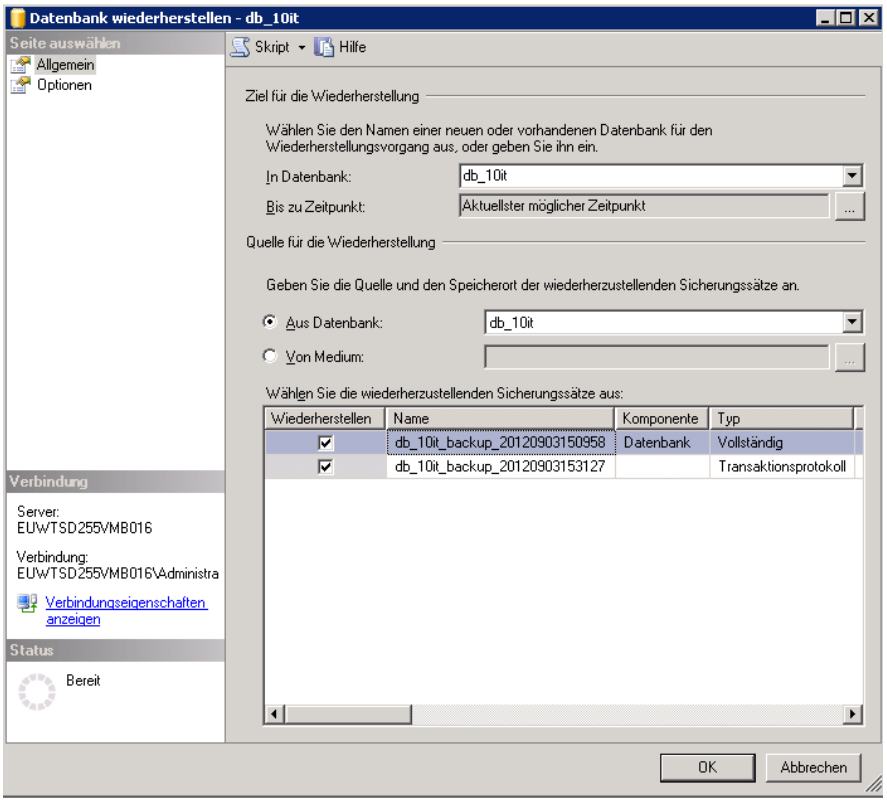
Achten Sie bitte darauf, Ihre Bewegungsdaten und die FastObjects Server Datenbank auf dem entsprechenden Stand der Datenbank zu halten. Kopieren Sie die gesicherten Bewegungsdaten in das Verzeichnis **10it_Daten** bzw. **csPlus_Daten** (Standardname) bzw. in Ihr Programmverzeichnis (bei älteren Einzelplatzinstallationen), aber nicht ohne vorher vom letzten Stand ebenfalls eine Sicherung erstellt zu haben.

Zur Wiederherstellung der FastObjects Server Datenbank ist es ebenfalls notwendig, den FastObjects Dienst zu beenden und nach Kopieren der FastObjects-Datenbankdateien bzw. des tse:nit | cs:Plus-Bewegungsdaten-verzeichnisses den Dienst wieder zu starten. Die Befehle finden Sie im Abschnitt ***FastObjects Server Datenbank***.

Ist die Datenbank im Microsoft SQL Server Management Studio als Objekt vorhanden, rufen Sie das Kontextmenü auf und wählen **Tasks | Wiederherstellen ...** aus. In dem folgenden Dialog können Sie aus allen Ihren Sicherungen die richtige auswählen.

Vorgehensweise:

1. Im Feld „In Datenbank“ wählen Sie die Datenbank aus. Da Sie von der vorhandenen tse:nit | cs:Plus Datenbank aus den Befehl aufgerufen haben, ist dies Ihr Standardvorschlag. Wenn Sie eine Sicherung testen wollen, könnten Sie hier einen abweichenden Namen eingeben.



2. Wählen Sie bei „Quelle für die Wiederherstellung“ den Punkt „Aus Datenbank“ aus.

3. Es werden alle vorhandenen Sicherungen innerhalb des ausgewählten Mediums aufgelistet.

4. Durch Ankreuzen wählen Sie die Sicherung aus. In unserem Beispiel handelt es sich um ein Transaktionsprotokoll. Automatisch ist die letzte vollständige Sicherung mit angekreuzt.

5. Mit [OK] startet die Rücksicherung.

Wenn Sie über eine Sicherung verfügen, aber die Datenbank **db_10it | db_rewe** selbst im Microsoft SQL Server Management Studio nicht mehr angezeigt wird, dann haben Sie die Möglichkeit, die Sicherung einzuspielen, indem Sie das Kontextmenü des Objektes „Datenbanken“ aufrufen und über **Tasks | Wiederherstellen | Datenbank ...** diesen Dialog öffnen. Voraussetzung ist, dass die Systemdatenbanken MASTER und MSDB über die entsprechenden Informationen verfügen.

Ist dies nicht der Fall, weil Sie diese Systemdatenbanken nicht gesichert haben und Sie nur über die tse:nit | cs:Plus Datenbanksicherung verfügen, müssen Sie folgendermaßen vorgehen:

1. Sicherung auf Festpatte kopieren.

2. Schreibschutz entfernen, falls die Sicherung von einer CD stammt.

3. Starten Sie das Microsoft SQL Server Management Studio.

4. Erweitern Sie im Objekt-Explorer einen SQL Server und erweitern dann „Datenbanken“.

5. Klicken Sie mit der rechten Maustaste auf „Datenbanken“ und dann auf „Datenbank wiederherstellen ...“

6. Geben Sie als Ziel für die Wiederherstellung im Feld „In Datenbank“ einen Datenbanknamen an, z.B. **db_10it** oder **db_rewe**.

7. Als Quelle für die Wiederherstellung wählen Sie „Von Medien“ aus, im darauf folgenden Dialog belassen Sie das Sicherungsmedium „Datei“ und fügen den Sicherungsspeicherort Ihrer Backupdatei hinzu.

8. Wählen Sie anschließend den wiederherzustellenden Sicherungssatz aus und klicken auf [OK]; die Rücksicherung wird gestartet.

## Rücksicherung der Datenbanksicherungsdatei in einen neuen SQL Server

Stammt die Sicherung nicht aus der gleichen SQL-Server-Installation (also anderer Rechner oder neue SQL-Server-Installation auf gleichem Rechner), muss der für tse:nit | cs:Plus benötigte Benutzer 10ITSQLDBSERVER der Datenbank dem Benutzer 10ITSQLDBSERVER des SQL Servers wieder zugeordnet werden.

Handelt es sich um eine SQL Server-Neuinstallation, muss zuvor der Benutzer 10ITSQLDBSERVER noch im SQL Server selbst angelegt werden. Führen Sie dazu in den tse:nit | cs:Plus administration tools unter „Allgemeine Aufgaben“ die Aufgabe „SQL Server-Ersteinrichtungsdatenbank anlegen“ aus und benennen die Datenbank mit DB_10IT_ERST. Öffnen Sie im Anschluss das SQL Server Management Studio und starten Sie auf dem entsprechenden neuen SQL Server eine Abfrage, indem Sie das Kontextmenü des SQL Servers öffnen und „Neue Abfrage“ wählen.

Geben Sie folgende Befehle ein und führen diese jeweils aus:

1. Befehl eingeben:
   ```
   use db_10it
   ```
   Führen Sie im Menü **Abfrage | Ausführen** aus.

2. Befehl eingeben:
   ```
   EXEC sp_change_users_login Update_One, '10itSQLDBServer', '10itSQLDBServer'
   ```
   Führen Sie im Menü **Abfrage | Ausführen** aus.

Danach können Sie auf die zurückgesicherte Datenbank mit den tse:nit | cs:Plus Clients bzw. Arbeitsplätzen zugreifen.

# 7. Besondere Hinweise für die ADDISON Software und Aktenlösungen

## 7.1. FastObjects Server Datenbank

Dieser Abschnitt gilt nur für die ADDISON Software und tse:nit.

Die ADDISON-Datenbank basiert auf dem FastObjects Datenbankserver der Versant Corporation.

Zur korrekten Sicherung der Datenbank darf niemand mit den ADDISON-Anwendungen arbeiten. Es muss das komplette Verzeichnis „db\dbkanz“ inkl. aller Unterverzeichnisse gesichert werden.

Für die Rücksicherung der Datenbank muss ebenfalls das komplette Verzeichnis „db\dbkanz“ inkl. aller Unterverzeichnisse zurückgesichert werden. Nur die Datei objects.dat allein genügt nicht.

Zum Zeitpunkt der Datensicherung muss der FastObjects Server Dienst nicht zwangsweise beendet werden. Es darf jedoch zum Zeitpunkt der Datensicherung niemand mit der ADDISON Software arbeiten. Um sicherzustellen, dass während der Sicherung keine Änderungen vorgenommen werden, empfehlen wir den FastObjects Server Dienst sicherheitshalber zu beenden.
Wenn Anwender per Remote-Verbindung auf die ADDISON Software zugreifen (Terminalserver-Umgebung), empfehlen wir jedoch die Sessions zu schließen und den FastObjects Server Dienst zu beenden, bevor die Datensicherung gestartet wird.

### 7.1.1. Methoden der Sicherung

Die FastObjects Server Datenbank besteht aus zwei Dateien, die sich in den Verzeichnissen „...\db\dbkanz“ (ADDISON Software) bzw. „...\Daten\NGDB\dbkanz“ (tse:nit) befinden. Diese Dateien heißen objects.dat und objects.idx.

Vor der Sicherung sollte der entsprechende FastObjects Server Dienst beendet werden.

Falls auf Ihrem System mehrere Konfigurationen/ Softwarestände existieren, bedenken Sie bitte, dass jeder seine eigene FastObjects Server Datenbank und somit einen eigenen FastObjects Server Dienst besitzt.

Die Sicherung der FastObjects Server Datenbank kann im Zuge des Sicherns des

Datenverzeichnisses erfolgen.

Vorgehensweise:

Beenden des FastObjects Server Dienstes vor dem Start der Sicherung und erneutes Starten nach dem Beenden der Sicherung, um die Datenbankdateien objects.dat und objects.idx bzw. das gesamte Datenbankverzeichnis direkt zu sichern.

Falls auf Ihrem System ein separater FastObjects Server installiert ist, können die Pfade zur FastObjects Datenbank ggf. abweichen.

Geben Sie in **Start | Ausführen** folgende Befehle ein.

vor der Sicherung:
`NET STOP „FastObjects Server 12.0“`
oder
`NET STOP „FastObjects Server 12.0 an xxxx“`

nach der Sicherung:
`NET START „FastObjects Server 12.0“`
oder
`NET START „FastObjects Server 12.0 an xxxx“`

„xxxx“ steht dabei für den entsprechenden Port, an dem der FastObjects Server läuft, falls dieser vom Standard 6001 abweicht (z.B. 6010).
Dies ist i.d.R. in der ADDISON Aktenlösung der Fall.

Werden diese Befehle eingegeben, dann kann direkt kopiert oder durch eine Sicherungssoftware ein Backup erstellt werden. Sollen diese Befehle automatisch ausgeführt werden, so besteht die Möglichkeit, die Befehlsfolge als entsprechende Aufgabe in **Systemsteuerung | Geplante Tasks** einzurichten.

Vergleichbar ist dies mit dem Ausführen des Befehls „Beenden“ bzw. „Starten“ in der Windows-Dienste-Verwaltung.

## 7.2. ADDISON OneClick

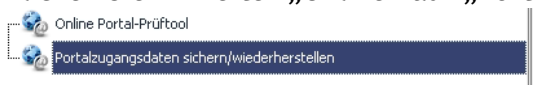
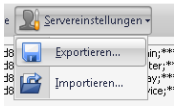
### 7.2.1. Allgemein

#### ADDISON Service - Benutzerprofil

Wenn Sie Nutzer des ADDISON Online-Portals sind, so sichern Sie bitte das **Benutzerprofil** des Windows-Users **„ADDISON Service“**. Dort ist u.a. gespeichert, mit welcher ID die Portal-Anmeldung erfolgt und auch, ob das Portal aktiviert ist oder nicht.
Für die Sicherung sind alle Dateien und Unterordner des Verzeichnisses:

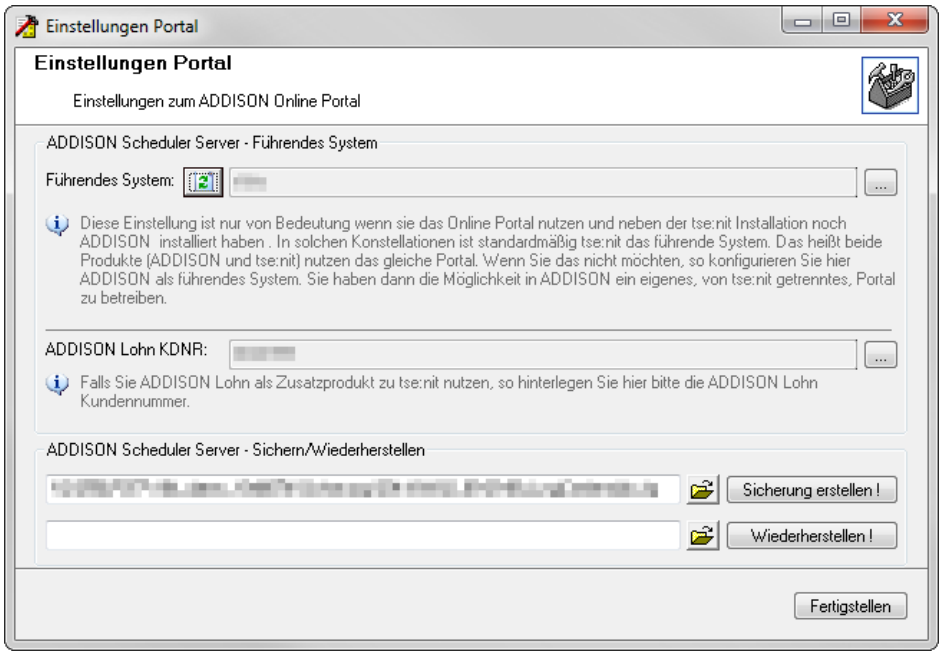
**C:\Users\ADDISON Service\AppData\Local\ADDISON_Software_und_Serv** relevant.

### 7.2.2. ADDISON Software

- Starten Sie das Enterprise Management Tool und aktivieren Sie den Erweiterten Modus 
- Klicken Sie im Reiter „Online“ auf „Portalzugangsdaten sichern/wiederherstellen“
  
  
- Wählen Sie **Servereinstellungen | Exportieren**.
  
  
  Es wird eine ZIP-Datei mit den Zugangsdaten erstellt, die mit Hilfe der Datensicherung als herkömmliche Datei gesichert werden kann.
- Zum Wiederherstellen wählen Sie **Servereinstellungen | Exportieren** und geben Sie im Dateiauswahldialog eine entsprechende ZIP-Datei mit Portalzugangsdaten an.

### 7.2.3. ADDISON Aktenlösung

- Öffnen Sie die tse:nit | cs:Plus administration tools und starten Sie in Ihrer Konfiguration die Erweiterte Aufgabe „Einstellungen Portal“.



- Klicken Sie dort auf [Sicherung erstellen!] und nehmen Sie die dabei erstellte ZIP-Datei in Ihre Sicherung auf.

## 7.3. ADDISON Kanzlei Cockpit – ADDISON WIKI-Hilfe

Zu (Rück-)Sicherungen im Umfeld des **ADDISON Kanzlei Cockpit** verweisen wir auf die Notwendigkeit den **ADDISON Scheduler Server-Dienst** zu **beenden**. Dadurch wird der PostgreSQL Server beendet und die Dateien der Kanzlei Cockpit-Umgebung können ohne Zusatzmodul (SQL-Agent) zur Sicherungssoftware (zurück-)gesichert werden.

Die Daten einer Kanzlei Cockpit-Umgebung befinden sich ebenfalls unterhalb des o.g. Datenverzeichnisses der ADDISON Software: „DATEN\SDN…“, wobei

- „…\Daten\SDN\Daten“ Zertifikate enthält und unter
- „…\Daten\SDN\Databases: die eigentlichen PostgreSQL-Datenbanken gespeichert sind. Der PostgreSQL Server greift ausschließlich auf dieses Verzeichnis zu.

Auf beide der o.g. Verzeichnisse wird zugegriffen, solange PostgreSQL und Tomcat laufen.

Sollten Sie die **ADDISON WIKI-Hilfe** für die Anzeige der Hilfen bzw. Produktdokumentationen innerhalb der ADDISON Software verwenden, ist es ebenfalls notwendig den **ADDISON Scheduler Server-Dienst** zu **beenden**, da u.U. Dateien unter „…\Daten“ dadurch gelockt sein können.

## 7.4. Belegverarbeitung Scannen-Buchen-Archivieren

### SQL Server Management Studio

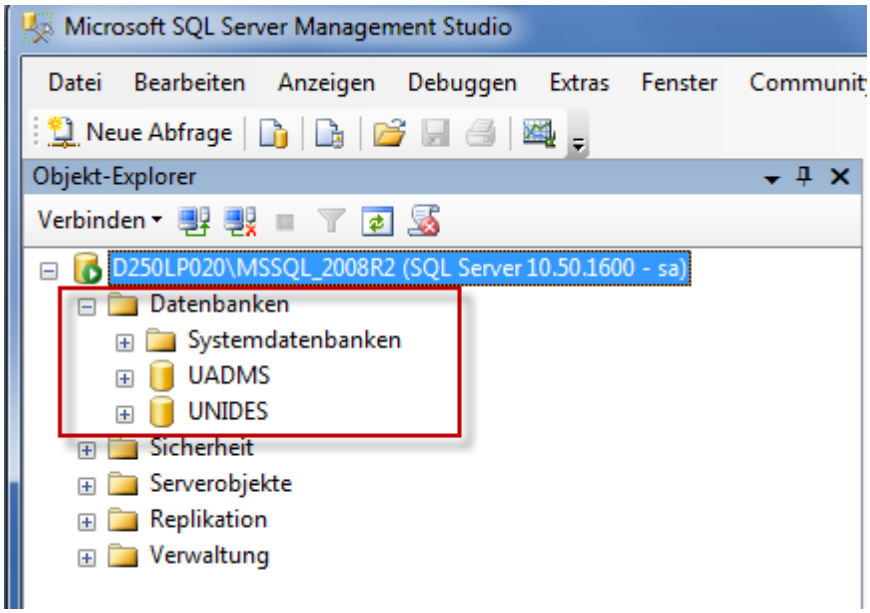
Eine SQL-Datenbank kann im laufenden Betrieb nicht gesichert werden. Da der SQL-Serverdienst aber noch immer läuft, auch wenn gerade keine Anwendung gestartet ist, ist die Datenbank im Zugriff und kann daher nicht gesichert werden.

### Einrichten eines SQL-Skriptes

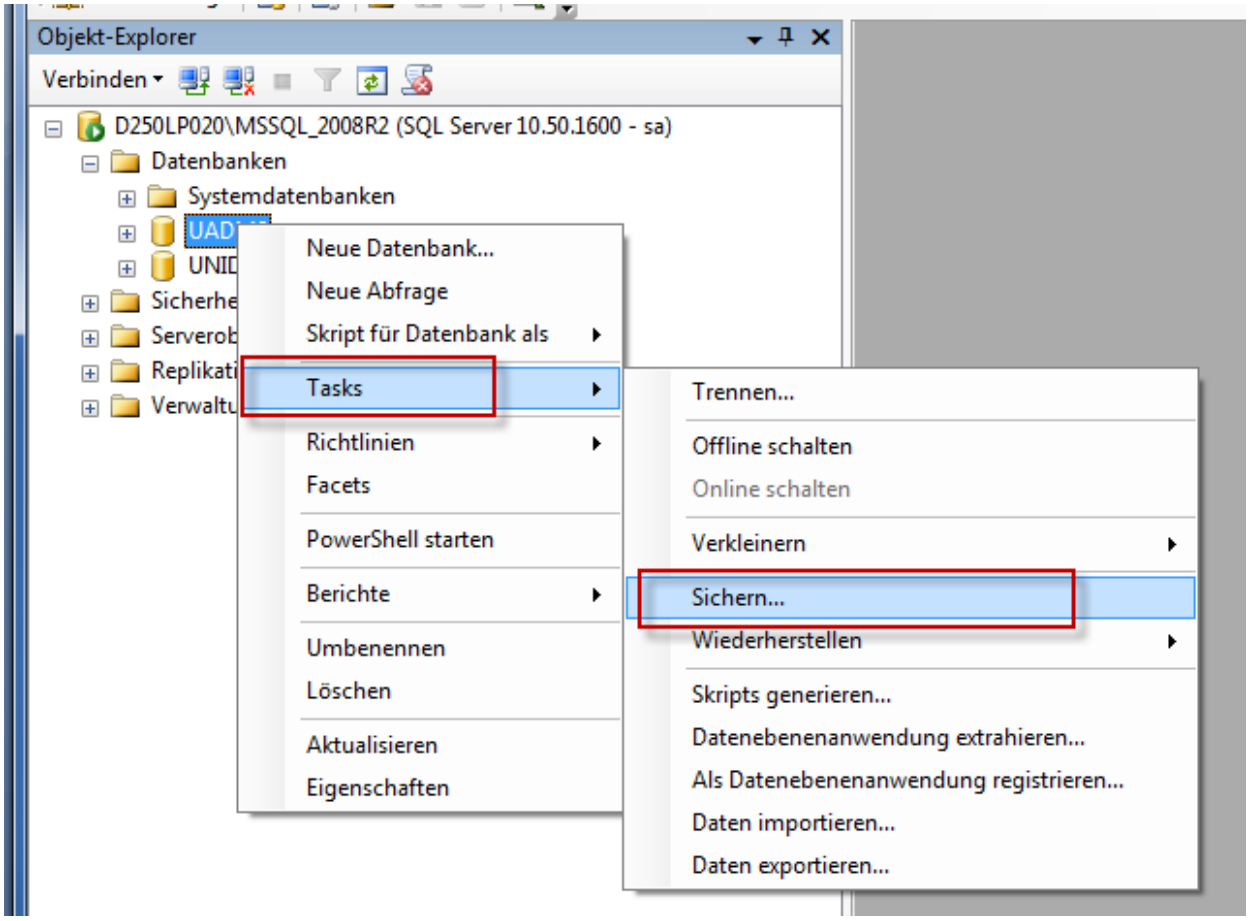
Über das Programm **Microsoft SQL-Server | SQL-Servermanagement** kann solch ein Sicherungsskript einfach eingerichtet werden.


Geben Sie nach dem Start des Programms das Kennwort des „sa“-Nutzers ein und klicken Sie auf [Verbinden].

Auf der linken Seite werden Ihnen in einer Explorer-Leiste alle Datenbanken angezeigt.




Klicken Sie mit der rechten Maustaste auf „UADMS“ und dort auf **Tasks | Sichern.**




In diesem Dialog tragen Sie lediglich noch die Sicherungstage mit 1 ein.

Dieses Skript erstellt in dem angegebenen Verzeichnis eine UADMS.BAK. Diese BAK-Datei wird jede Nacht um 0:00 Uhr erstellt.

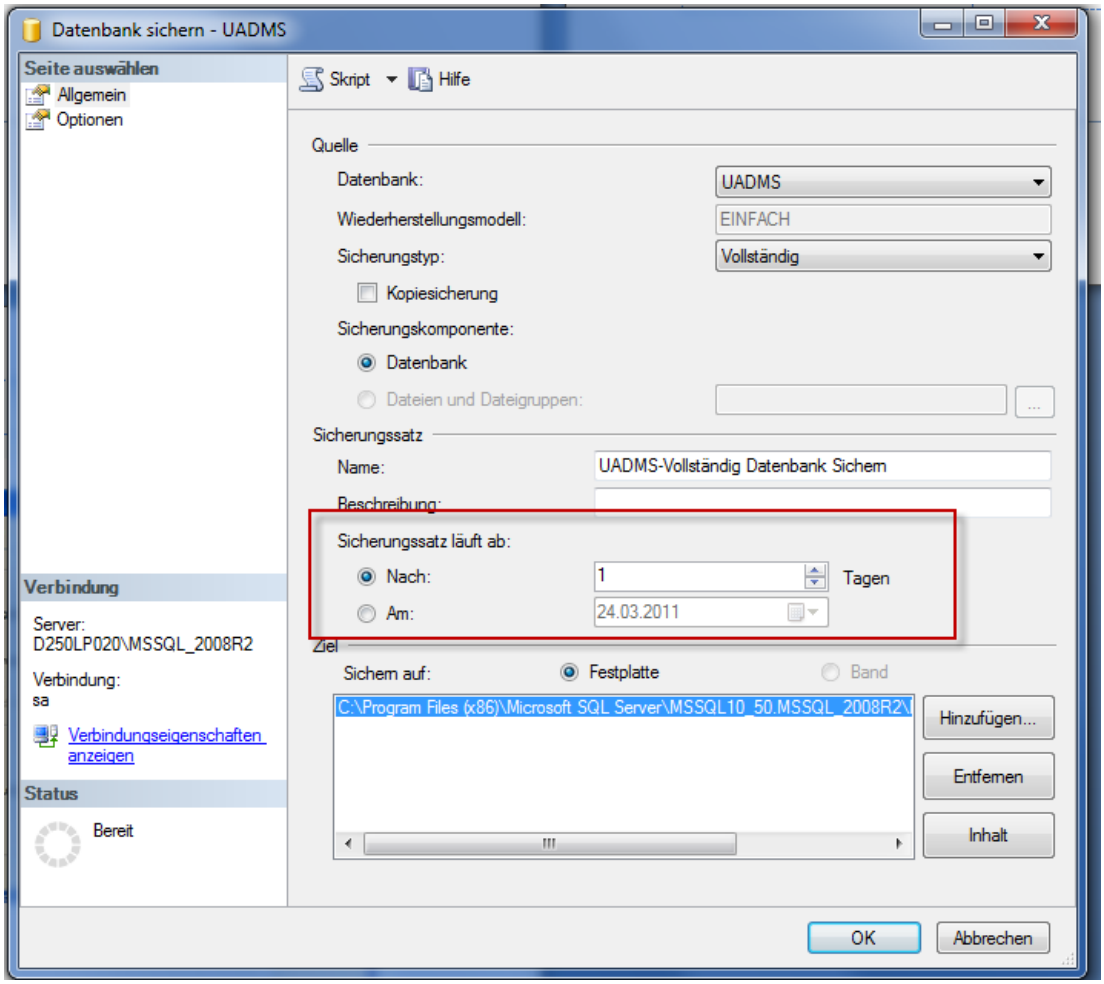
Die UADMS.BAK muss in die Sicherungsprozedur mit aufgenommen werden.

Den gleichen Vorgang führen Sie für die Datenbank „UNIDES“ durch.

## Sicherungsverzeichnisse für die Datensicherung

Um die Belegverarbeitung komplett zu sichern, müssen folgende Dateien in die Sicherungsprozedur mit aufgenommen werden:

- UNIDES.BAK
- UADMS.BAK
- C:\UNIARCHIV (evtl. anderer Laufwerksbuchstabe)




## 7.5. DocuWare

Zur (Rück-)Sicherungen im Umfeld von DocuWare verweisen wir auf die Informationen des Herstellers selbst: http://help.docuware.com/de/#b57864t59282n56783

## 7.6. tse:nit banking

### 7.6.1. Zu (rück)sichernde Bewegungsdaten

Die tse:nit banking Bewegungsdaten befinden sich in der Regel auf dem Datenserver im Verzeichnis **10it_Banking_Daten.** Dies gilt sowohl für die lokale Ordnerbezeichnung, als auch für eine UNC-Freigabe.

Zu den Bewegungsdaten zählen die Dateien in folgenden Unterverzeichnissen

**..\Backup**

Kopien der DB_zp_10it_Banking (erstellt mit dem tse:nit banking administrations tool)

**..\TEMP**

internes Verzeichnis für die Ablage temporärer Dateien

**..\XMLExport**

Exportpfad der Kontoumsätze für den tse:nit Bankauszug

### 7.6.2. SQL Server Datenbank

Zum Sicheren und Wiederherstellen beachten Sie bitte die Abschnitte ***Empfohlene Vorgehensweisen zur Sicherung von SQL Server*** Datenbanken und *Fehler! Verweisquelle konnte nicht gefunden werden.* aus dem Kapitel der ADDISON Aktenlösung.

## 7.7. tse:nit DMS

Da die Informationen im Archiv selbst, in der Verwaltungsdatenbank für SAPERION (DB_SAPERION) und in der tse:nit Datenbank (standardmäßig: DB_10IT) zueinander passen müssen, muss eine möglichst zeitnahe Sicherung des 10itDMS-Verzeichnisses auf dem Archivserver sowie der Datenbank DB_SAPERION und der tse:nit-Datenbank eingerichtet werden.

## 7.8. Daten außerhalb der Software-Verzeichnisstruktur

Zudem müssen Sie beachten, dass **Daten/Dateien außerhalb der o.g. Verzeichnisstruktur gespeichert werden können**, sofern die Anwendung einen Auswahldialog zur Speicherung der Dateien bietet. Sie müssen selbstverständlich auch diese Verzeichnisse bei der Sicherung berücksichtigen.

# 8. ADDISON Handwerk

## 8.1. Allgemein

### 8.1.1. Allgemeine Informationen zum SQL Server

#### SQL Server

Um große Mengen an Daten zu verwalten, bedarf es einer Datenbank. ADDISON Handwerk verwaltet seine Daten mit dem Microsoft SQL Server (auch kurz MSSQLServer). Dieses ist ein relationales Datenbankmanagementsystem von Microsoft.

#### SQL Dienst

Beim Microsoft SQL Server handelt es sich um eine Software. Diese wird als Systemdienst installiert und läuft in aller Regel, solange der Server eingeschaltet ist.
D.h., eine SQL Datenbank kann man nicht einfach zum Sichern über den Windowsexplorer in einen separaten Ordner kopieren, da der SQL Server Dienst und damit auch die Datenbank ständig im Zugriff sind.

### 8.1.2. Die ADDISON SQL Datensicherung

#### Addison SQL Datensicherung

Um dennoch eine problemlose und automatische Sicherung Ihrer Daten zu gewährleisten, wurde die ADDISON SQL Datensicherung entwickelt.

#### Systemdienst

Die ADDISON Datensicherung wird ausschließlich auf dem Server installiert, auf dem in aller Regel auch der Microsoft SQL Server läuft. Sie richtet sich beim Installieren ebenfalls als Systemdienst unter Windows ein.

#### Sicherung bei geöffnetem Handwerksprogramm

Die ADDISON Datensicherung kann während des laufenden Betriebes erfolgen. Sie sichert genau die Daten, die zum Zeitpunkt der Sicherung gerade nicht in Benutzung sind.

**Beispiel:** Bei einem gerade geöffneten Beleg würde nur der Stand, der in der Datenbank gespeichert ist, gesichert werden.

## 8.2. Beschreibung der ADDISON SQL Datensicherung

### 8.2.1. Programmaufruf

Der Aufruf der Software erfolgt am Server über **Start | Alle Programme | ADDISON | Datenbanktools | ADDISON Datensicherung ab Version 7.4.**

### 8.2.2. Anmeldung

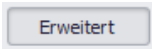
#### Datenbankname keine Pflichtangabe

Für die Einrichtung und Durchführung der Datensicherung ist die Angabe einer Datenbank **nicht** erforderlich. Diese wird ausschließlich dann benötigt, wenn Protokolle innerhalb der ADDISON Datensicherungssoftware gedruckt werden sollen.

#### Server

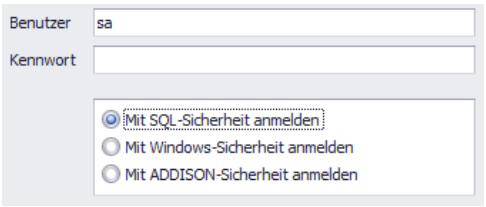

Hier ist der Name des SQL Servers und evtl., gefolgt von einem Backslash, der Name der SQL Instanz einzutragen. Bestehende SQL Server können über das Symbol [...] ausgewählt und übernommen werden.

#### Art der Anmeldung

Über den Button 

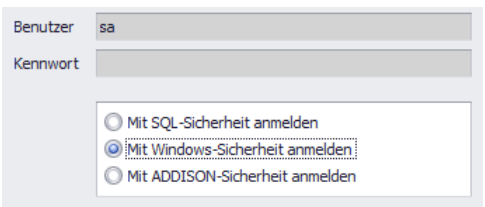
kann die Art der Anmeldung ausgewählt werden.

#### SQL Sicherheit




Für eine korrekte Anmeldung wird das Kennwort für den Benutzer „sa“ (Systemadministrator des SQL Servers) benötigt.

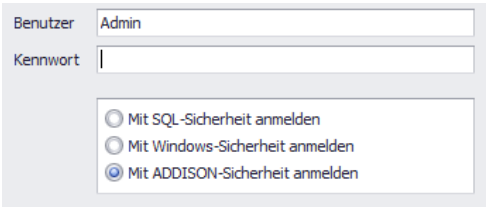
#### Windows-Sicherheit




Für eine korrekte Anmeldung genügt der aktuelle Windows-Benutzer.

Um die vollen Funktionalität der ADDISON Datensicherung nutzen zu können muss der anmeldende Windows-Benutzer Administrator-Rechte besitzen!

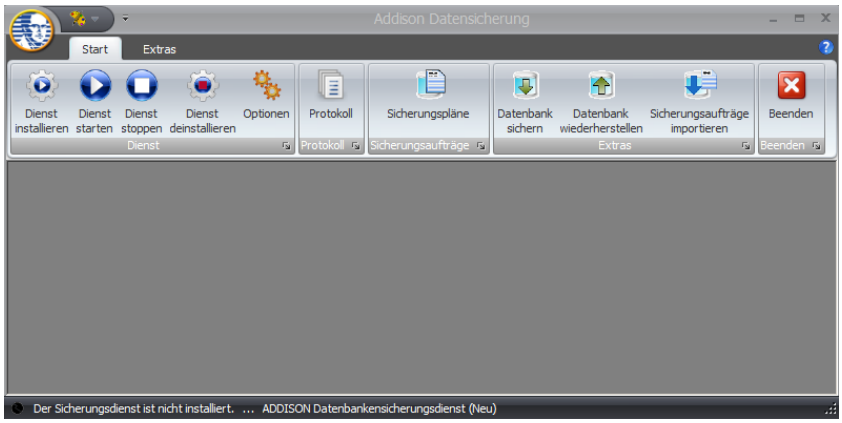
### ADDISON Sicherheit




Für eine korrekte Anmeldung wird das Kennwort für den ADDISON-Benutzer „Admin“ (Administrator von ADDISON Handwerk) benötigt.

Bei korrekten Anmeldedaten wird mit Klick auf den Button OK die ADDISON Datensicherungssoftware gestartet.

## 8.2.3. Oberflächenbeschreibung




### Dienst installieren

Mit dem Button  wird der Windows-Dienst für die ADDISON Datensicherung installiert.
**Hinweis:** Mit dem Installieren des Dienstes wird dieser auch automatisch gestartet.

### Dienst starten

Mit dem Button  kann der Windows-Dienst für die ADDISON Datensicherung manuell gestartet werden.

### Dienst stoppen

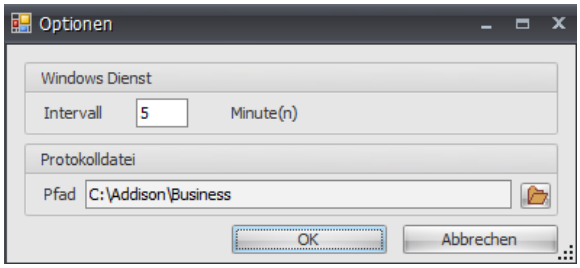
Mit dem Button  kann der Windows-Dienst für die ADDISON Datensicherung gestoppt werden.

### Dienst deinstallieren

Mit dem Button  kann der Windows-Dienst für die ADDISON Datensicherung deinstalliert werden.

### Optionen

Über den Button  öffnen sich die Optionen:




### Intervall

Hier kann festgelegt werden, wie oft der Dienst nach geänderten Einstellungen z.B. in den Sicherungsaufträgen suchen soll.

### Pfad für die Protokolldatei

In die Protokolldatei werden die erfolgten Sicherungen bzw. Sicherungsversuche eingetragen. Hier kann der Speicherpfad zur Protokolldatei hinterlegt werden.

### Protokoll

 Anzeige des Datensicherungsprotokolls.

### Sicherungspläne

 Aufruf der Sicherungspläne.

### Datenbank sichern

 Manuelle Sicherung einer Datenbank.

### Datenbank wiederherstellen

 Rücksicherung einer Datenbank.

### Sicherungsaufträge importieren

 Sicherungsaufträge der vorherigen Version der ADDISON Datensicherung importieren.



*<Hier klicken, um zurück zum Inhaltsverzeichnis zu gelangen>*

### Beenden

 Beenden der Oberfläche der ADDISON Datensicherung.

### 8.2.4. Einrichtung des Dienstes

#### Installation

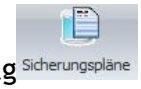
Hierzu klicken Sie auf den Button [Dienst installieren].

 Der Dienst wird nach erfolgter Installation automatisch gestartet.

## 8.3. Datensicherung durchführen

### 8.3.1. Einrichtung einer automatischen Sicherung

#### Aufruf der Sicherungspläne

Über den Menüeintrag 

wird die Einrichtung der Sicherungspläne gestartet.

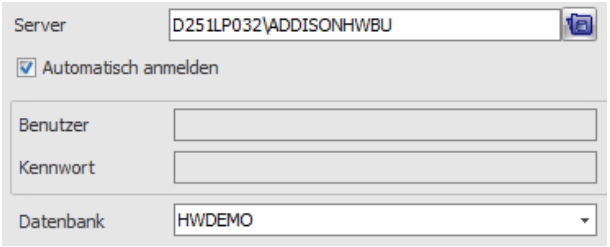
#### Neu ...

Über den Button  wird ein neuer Sicherungsplan geöffnet.

#### Sicherungsauftrag


Hier wird ein Name für den Sicherungsplan vergeben, z.B. „täglich“.

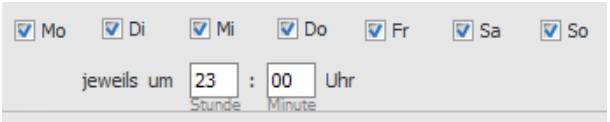
#### Verbindungsdaten




Hier werden die Daten für die Verbindung zum SQL-Server sowie der zu sichernden Datenbank eingegeben.

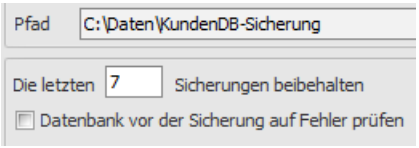
Bestehende Datenbanken können über das Pfeilsymbol ausgewählt werden.

### Sicherungsintervall




Hier werden die Tage sowie die Uhrzeit gesetzt, an denen die Datenbank gesichert werden soll.

### Ziel




Hier wird der Pfad eingetragen, in den die SQL Datensicherung erfolgen soll.

### Beispiel:

Im vorigen Beispiel wird ein „Job“ namens „täglich“ eingerichtet. Er wird von montags bis sonntags um jeweils 23:00 Uhr gestartet. Die Sicherungen erfolgen in Dateien, die unter „C:\Daten\KundenDB-Sicherung“ gespeichert werden. Diese Sicherungsdateien werden maximal 7 Tage aufgehoben, danach werden die ältesten überschrieben.

### Speichern

Über den Button  wird der angelegte Sicherungsauftrag gespeichert.

## 8.3.2. Durchführung einer manuellen Sofortsicherung

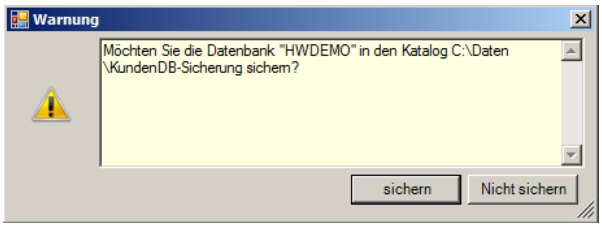
Auch zur Durchführung einer manuellen Datenbanksicherung wird ein Auftrag benötigt. Dieser enthält jedoch keine festen Sicherungstage.

### Starten der Datensicherung

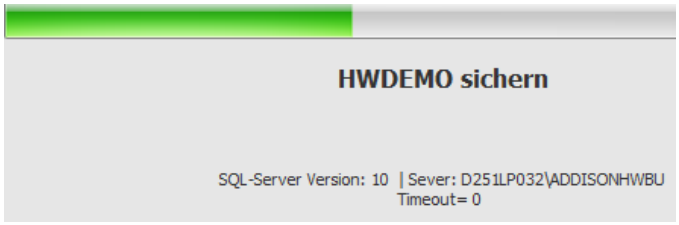
Auftrag markieren und mit dem Symbol 

die Datenbanksicherung starten.

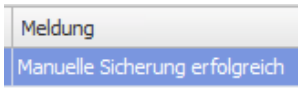
### Sicherheitsabfrage



### Fortschrittsanzeige




### Statusmeldung




In der Auftragstabelle wird der Status der letzten Sicherung angezeigt.

## 8.4. Datenbankrücksicherung

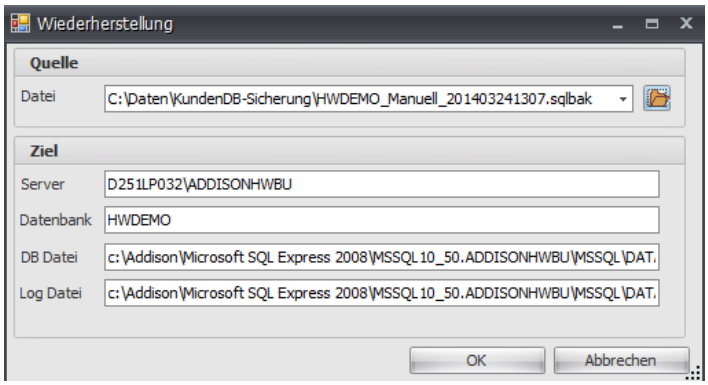
### 8.4.1. Datenbankrücksicherung durchführen


Bei einer Rücksicherung wird der komplette Datenbestand überschrieben!

### Aufruf

Mit dem Symbol 

wird der Dialog zur Datenbankrücksicherung aufgerufen.




Über die Dateiauswahl wird die SQL Backup-Datei ausgewählt. Der Dateiname endet mit *.sqlbak.

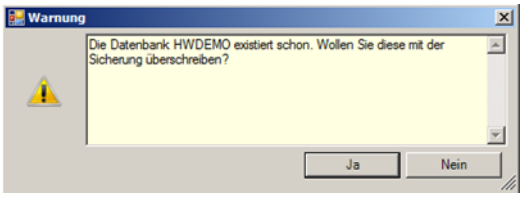
Der SQL-Server, der Datenbankname sowie die Dateipfade werden automatisch ermittelt und vorgeschlagen.

## Ändern der Pfade


Wird der Datenbankname geändert, so sollte zwingend auch der Name der DB-Datei sowie der Log-Datei geändert werden!

Dies ist z.B. dann sinnvoll, wenn die aktuelle Datenbank nicht überschrieben, sondern unter einem neuen Namen angelegt werden soll.

## Warnhinweis



# 9. Symbole/Legende

Im vorliegenden Dokument werden z.T. Symbole für die Hervorhebung von wichtigen/besonderen Abschnitten verwendet, die folgende Bedeutung haben:

| | |
|---|---|
|  | Weiterführende Informationen |
|  | Wichtige Hinweise |
|  | Handlungsanweisungen |
|  | Nützliche Tipps und Tricks |
|  | Beispiele zu den Themen |
|  | Notizen |
|   | Besonders wichtige Hinweise |