Schleswig-Holsteinischer Landtag
Umdruck 17/3879

Ministerium
für Bildung und Kultur
des Landes Schleswig-Holstein

Vorsitzende des Bildungsausschusses
Frau Susanne Herold, MdL
Landeshaus
24105 Kiel

Kiel, 20.03.2012

***Staatssekretär***

**Informationen über den IT-Einsatz in der Schulverwaltung in Schleswig-Holstein**

Sehr geehrte Frau Vorsitzende,

der IT-Einsatz in der Schulverwaltung in Schleswig-Holstein ist für mich Anlass, auch wegen der dafür aufgewendeten Finanzmittel des Landes, Sie über das gegenwärtig Erreichte zu unterrichten.

Das Landesnetz Bildung (LanBSH) ist ein Gemeinschaftsprojekt des Ministeriums für Bildung und Kultur, des Finanzministeriums, der kommunalen Schulträger, des Instituts für Qualitätsentwicklung an Schulen (IQSH) und Dataports.

Das Projekt zielt auf den Auf- und Ausbau einer mit dem Landesnetz in Verbindung stehenden Servicelandschaft (Verzeichnisdienst, eMail, Internet etc.) mit standardisierten und zentral administrierbaren Arbeitsplatzrechnern in den Verwaltungen der Schulen und der Schulämter, um die Kommunikationsmöglichkeiten zwischen Schulen, Schulämtern, Schulträgern und Ministerium zu verbessern und so die tägliche Arbeit durch standardisierte und vernetzte IT-Arbeitsplätze zu erleichtern.

Brunswiker Straße 16 - 22, 24105 Kiel | Telefon (04 31) 9 88 - 57 01 | Telefax (04 31) 9 88 - 58 14
e-mail: Pressestelle@mbk.landsh.de | Internet: www.mbk.schleswig-holstein.de | Bus: Linie 32, 33, 61, 62

Die IT-Ausstattung entspricht den von den Kommunalen Landesverbänden und vom Ministerium für Bildung und Kultur gemeinsam erarbeiteten IT-Ausstattungs-empfehlungen für Schulen und ermöglicht

- sicher über ein landesinternes, vom Unabhängigen Landeszentrum für Daten-schutz zertifiziertes Netz zu kommunizieren und Dokumente auszutauschen,
- auf zentral abgelegte Informationen im schleswig-holsteinischen Informations-Pool (SHIP) zuzugreifen,
- über eine zentrale Plattform (Sharepoint) auf gemeinsame Dokumente zuzugreifen und diese zu bearbeiten,
- eine vereinfachte und beschleunigte Onlinewartung und -aktualisierung der ange-schlossenen Rechner,
- den sichereren Zugriff auf das Internet und
- den Zugriff auf Haushaltsanwendungen beim Schulträger.

Auch viele neue Verfahren basieren inzwischen auf dem vom Unabhängigen Lan-deszentrum für Datenschutz (ULD) zertifizierten Landesnetz Bildung:

- die Kommunikation der Schulen mit ihren Außenstellen,
- die Übermittlung der Aufgaben für die Zentralen Abschlüsse,
- die Übermittlung der Schulstatistikdaten,
- das Personal-Bewerbungsverfahren Online für Lehrkräfte (pbOn),
- die Übermittlung von Schülerdaten gemäß § 30 Abs. 7 SchulG (Pilotbetrieb) und
- KoPers (im Aufbau).

Inzwischen ist das Landesnetz Bildung zu einer unverzichtbaren Infrastruktur für die Schulen, die Schulämter und das Ministerium geworden.
Von 852 öffentlichen Schulen nutzen es bereits über 710 Schulen sowie über 90 Außenstellen von Schulen mit 12.500 Anwenderinnen und Anwendern an 3.400 PCs.
Einen wichtigen Beitrag zur Akzeptanz des LanBSH leistet das IQSH durch seine Beratung und Unterstützung beim Anschluss der Schulen an das LanBSH sowie beim Betrieb des für die Schulen eingerichteten User Help Desk.

Bis Ende des Jahres 2012 sollen alle interessierten Schulen an das Landesnetz Bildung angeschlossen sein. Zur Frage, bei wie vielen Schulen zwar der Landesnetzanschluss hergestellt, aber die Installation durch das IQSH bzw. dataport noch nicht abgeschlossen werden konnte, zeigt sich folgender Zwischenstand: 13 Schulen verfügen bereits über einen Landesnetz-Anschluss, sind aber noch nicht angebunden. Die Liste ist als Anlage 1 beigefügt. Die Anbindung ist für 2012 geplant.
13 Schulen haben noch keinen Antrag auf Anschluss an das „Landesnetz Bildung“ gestellt. Eine Auflistung ist als Anlage 2 beigefügt.
Eine Auflistung derjenigen Schulen, die aus wirtschaftlichen Erwägungen Gründen nicht an das „Landesnetz Bildung“ angeschlossen werden sollen, ist als Anlage 3 beigefügt. Es handelt sich um 5 Halligschulen.
Die einzige Schule, die einen Anschluss ablehnt, ist die Grundschule Mittelschwansen im Kreis Rendsburg-Eckernförde.
Für die Anbindung von Schulen an das Landesnetz Bildung durch den externen Dienstleister sind im Jahr 2011 Kosten in Höhe von 87.456,43 € entstanden. Für das Jahr 2012 ist mit Kosten von ca. 55.000 € zu rechnen.
Das Datensicherungskonzept ist als Anlage 4 beigefügt. Die Schulen und Schulträger werden vor Ort durch das IQSH informiert. Seit dem 01.12.2011 werden neue Schulverwaltungsserver mit installierter Datensicherung ausgeliefert. Bei ca. 655 Schulen muss die Datensicherung nachinstalliert werden. Vorgesehen ist der Einsatz eines externen Dienstleisters. Hierfür sind Mittel in Höhe von ca. 65.000 € veranschlagt.
Zu den Schulverwaltungsprogrammen ergibt sich folgendes Bild:
Von 857 Schulen haben 453 gegenwärtig ein Schulverwaltungsprogramm, das der Empfehlung des Landes (fernadministrierbar, ferninstallierbar, datenschutzzertifiziert, ein Programm für alle Aufgaben, standardisierte Schnittstelle zur Datenübermittlung, Netzwerkfähigkeit) und der kommunalen Verbände (AG-IT-Bildung) entspricht.
Weitere 102 Schulen haben eine Umstellung auf ein solches Programm beim IQSH-Helpdesk beantragt.
49 Schulen, darunter alle 35 Berufsschulen, benutzen das berufsschulspezifische Programm WinSchool, bei dem der Anbieter sich zurzeit bemüht, die Vorgaben der AG-IT-Bildung zu erfüllen. Die verbleibenden 253 Schulen, darunter noch 94 Gymnasien, verwenden pro Schule mehrere verschiedene, teilweise selbst erstellte Pro-

gramme zur Erledigung der Schulverwaltungsaufgaben. Die vom Land empfohlenen Programme haben eine gemeinsame Datenbank mit dem Unterrichtsverteilungs- und Vertretungsplanprogramm Untis sowie eine Schnittstelle zum standardisierten Datenaustausch mit anderen Dienststellen (Vorgaben Datenschutz werden berücksichtigt). Für die Einführung eines einheitlichen Schulverwaltungsprogramms mit den vom Land empfohlenen Eigenschaften für Schulen mit gymnasialer Oberstufe liegt ein Vorschlag des IQSH im MBK vor.
Die Annahme der Landesempfehlung durch bisher 71% der Schulen beruht analog zum erfolgreichen Anschluss an das Landesnetz Bildung Schleswig-Holstein auf freiwilliger Einsicht und auf dem Wunsch der Schulen.
Es gibt zurzeit Vorgespräche über die Kosten für die Beschaffung eines Stunden- und Vertretungsplanprogramms (Untis), das in allen Bundesländern von vielen - in Schleswig-Holstein bisher ca. 240 - großen Schulen genutzt wird. Das Programm Untis hat eine Datenschnittstelle zu den von den kommunalen Verbänden und dem Land Schleswig-Holstein empfohlenen Schüler- und Lehrerverwaltungsprogrammen und befindet sich in der Zertifizierung durch das ULD. Das Ergebnis liegt bis Ende Februar 2012 vor. Nach Bewertung dieses Ergebnisses können gegebenenfalls Verhandlungen mit dem Anbieter aufgenommen werden.

Mit freundlichem Gruß
gez.
Eckhard Zirkmann

Anlagen

**Anlage 1**

## Schulen, die einen Anschluss haben, aber noch nicht angebunden sind

| Schulname | Ort | Schulart | Kreis | Bemerkung |
|---|---|---|---|---|
| Regionales Berufsbildungszentrum Plön | Plön | Berufschule | Plön | Plön versucht einen eigenen Weg (Genehmigung fehlt) über das Kreisnetz |
| Gemeinschaftsschule Ratzeburg | Ratzeburg | Gemeinschaftsschule | Herzogtum Lauenburg | Schulen werden Um/Neugebaut. Neue Begehung mit Schulträger und Dataort im 2. Quartal 2012. |
| Grundschule Ratzeburg | Ratzeburg | Grundschule | Herzogtum Lauenburg | |
| Wolfgang-Radtke-Schule | Wilster | Grundschule | Steinburg | Zukunft der Schule noch ungeklärt. |
| Grundschule Bokholt-Hanredder | Bokholt-Hanredder | Grundschule | Pinneberg | Wird angeschlossen sobalt Haushalt freigegeben ist. |
| Sventana-Schule | Bornhöved | Gemeinschaftsschule | Segeberg | Schulinterne Verkabelung fürs Landesnetz noch nicht fertig. Noch keine Haushaltsmittel vom Schulträger für 2012 freigegeben. |
| Stapelholm-Schule | Erfde | Regionalschule | Schleswig-Flensburg | Termin so bald wie möglich, sobalt Schulträger Haushaltsmittel für 2012 freigegeben hat. |
| Grundschule Bergenhusen | Bergenhusen | Grundschule | Schleswig-Flensburg | |
| Grundschule Norderstapel | Norderstapel | Grundschule | Schleswig-Flensburg | |
| Grundschule Morsum | Sylt-Ost | Grundschule | Nordfriesland | Umbau und Hauptstelle ist noch nicht angeschlossen. |
| Grundschule Oster-Ohrstedt | Oster-Ohrstedt | Grundschule | Nordfriesland | Wird angeschlossen sobalt Haushalt freigegeben ist. |
| Grundschule Haselund | Haselund | Grundschule | Nordfriesland | |
| Grundschule Jörl | Kleinjörl (Jörl) | Grundschule | Schleswig-Flensburg | |

**Anlage 2**

## Schulen, die noch keinen Antrag abgegeben haben

| Schulname | Ort | Schulart | Kreis | Bemerkung |
|---|---|---|---|---|
| Grund- und Regionalschule Wankendorf | Wankendorf | Regionalschule | Plön | Antrag angemahnt und zugesagt |
| Grundschule Bünningstedt | Ammersbek | Grundschule | Stormarn | Antrag angemahnt und zugesagt |
| Grundschule mit Förderschulteil Heiligenhafen | Heiligenhafen | Grundschule | Ostholstein | Antrag für Februar zugesagt |
| Grundschule Klixbüll | Klixbüll | Grundschule | Nordfriesland | Antrag angemahnt und zugesagt |
| Grundschule Laboe | Laboe | Grundschule | Plön | Antrag angemahnt und zugesagt |
| Grundschule Münsterdorf | Münsterdorf | Grundschule | Steinburg | Antrag für Februar zugesagt |
| Otto-Thiesen-Schule | Ostenfeld (Husum) | Grundschule | Nordfriesland | Antrag für Februar zugesagt |
| Grundschule mit Regionalschulteil in Ratekau | Ratekau | Grundschule | Ostholstein | Antrag angemahnt und zugesagt |
| Grundschule Wesseln | Wesseln | Grundschule | Dithmarschen | Antrag angemahnt und zugesagt |
| Grundschule Landkirchen auf Fehmarn | Westfehmarn | Grundschule | Ostholstein | Antrag für Februar zugesagt |
| Gustav-Heinemann-Schule | Hohenlockstedt | Förderschule | Steinburg | Schulen werden zusammengelegt. Endgültiger Standort bis April 2012 geklärt, dann folgt Antrag. |
| Ulmenhofschule | Kellinghusen | Förderschule | Steinburg | |

| | | | | |
|---|---|---|---|---|
| Grundschule Mittelschwansen | Waabs | Grundschule | Rendsburg-Eckernförde | Schule will nicht ans Landesnetz angeschlossen werden. |

**Anlage 3**

## Schulen, die nicht angeschlossen werden sollen

| Schulname | Ort | Schulart | Kreis | Bemerkung |
|---|---|---|---|---|
| Grund- und Hauptschule Gröde | Hallig Gröde | Halligschule | Nordfriesland | soll nicht, keine eigene Verwaltung |
| Grund- und Hauptschule Hallig Hooge | Hallig Hooge | Halligschule | Nordfriesland | soll nicht, keine eigene Verwaltung |
| Grund- und Hauptschule Hallig Oland | Hallig Oland | Halligschule | Nordfriesland | soll nicht, keine eigene Verwaltung |
| Grund- und Hauptschule Nordstrandischmoor | Nordstrand | Halligschule | Nordfriesland | soll nicht, keine eigene Verwaltung |
| Eugen-Träger-Schule | Langeness | Halligschule | Nordfriesland | soll nicht, keine eigene Verwaltung |

Institut für
Qualitätsentwicklung
an Schulen
Schleswig-Holstein

# Datensicherungskonzept für Schulen in Schleswig Holstein

**Institut für Qualitätsentwicklung**
**an Schulen in Schleswig-Holstein**
**Schreberweg 5**
**24119 Kronshagen**


Sven Fettweis
17.02.2012
Version 1.0

## Inhaltsverzeichnis

# 1. Einführung

## 1.1 Allgemein

Die Abteilung „IT Dienste“ des Institut für Qualitätssicherung an Schulen in Schleswig Holstein, plant und betreut u.a. die Standortserver der Schulen in Schleswig Holstein.
Durch technisches Versagen, versehentliches Löschen, Diebstahl oder durch Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen. Die regelmäßige Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.
Die Konzeption einer angemessenen und funktionstüchtigen Datensicherung ist daher angemessen.

### 1.1.1 Einsatz an den Schulen

Die Informations- und Datenverarbeitung sowie die dafür benötigte Hard- und Software ist ein fester Bestandteil des heutigen Schulalltags in Unterricht und Verwaltung.
Kommunale Schulträger wie auch das Land Schleswig- Holstein haben in den letzten Jahren erfolgreiche Anstrengungen unternommen, um die Schulen mit funktional sinnvoller IT-Ausstattung auszurüsten und deren Betreuung sicherzustellen.
Dabei hat sich gezeigt, dass die im Jahre 2003 erstmals veröffentlichten gemeinsamen Ausstattungsempfehlungen für Schulträger und Schulen eine hilfreiche Leitlinie für die Investitionen in eine verlässliche und effiziente IT-Ausstattung in Unterricht und Verwaltung der Schulen waren.
Der voraussichtlich Ende 2010 abgeschlossene Anschluss aller Schulen und Schulämter an das Verwaltungsnetz des Landes (LanBSH) sowie der Aufbau einer zentralen Serviceinfrastruktur (Helpdesk) mit dem Ziel, die Schulen von unterrichtsfernen Tätigkeiten zu entlasten, kann seine volle Wirksamkeit nur vor dem Hintergrund einer Vereinheitlichung der IT-Ausstattung erreichen. Die individuelle Beratung der Schulen und Schulträger zur IT-Ausstattung und landesweiten schulbezogenen IT-Verfahren sowie der Betrieb des Helpdesk werden durch das IQSH sichergestellt.

### 1.1.2 Zusammenschluss und Vereinheitlichung (Landesnetz Bildung)

Das Landesnetz Bildung ist ein Gemeinschaftsprojekt des Ministeriums für Bildung und Kultur, des Finanzministeriums, des Instituts für Qualitätsentwicklung
an Schulen und den kommunalen Schulträgern. Das Projekt beinhaltet den Auf- und Ausbau einer mit dem Landesnetz verbundenen Servicelandschaft für Schulen
mit standardisierten und zentral administrierten Verwaltungsrechnern.
Dadurch soll die tägliche Arbeit der Schulen vereinfacht und die Kommunikationsmöglichkeit mit Schulämtern, Schulträgern und Ministerien technisch verbessert werden.

## 1.2 Zieldefinition

Für die Schulen sollen verschiedene Möglichkeiten der Datensicherung aufgezeigt werden.

### 1.2.1 Lokale Sicherung

- Sicherung auf externe Festplatten
- Sicherung auf Netzwerkspeicher (NAS)

### 1.2.2 Zentrale Sicherung

- Zentralisierte Sicherung über Wan Leitungen.
  (Weitverkehrs-Speicherort, Beispiel Dataport)

Anmerkung: Die zentrale Sicherung kann in Betracht gezogen werden, bedarf jedoch eines separaten Konzeptes.
Als Technologie für die Sicherung über die WAN Strecke ist mit dem Dienstleister abzustimmen.

## 1.3 Testumgebung Domäne IQSH.INTERN

Zur Simulation der eingesetzten Technologie und aufzeigen der Verfahrensweisen wurde eine Testumgebung bereitgestellt.

| Server | IP Adresse | Funktion | Betriebssystem |
|---|---|---|---|
| VM Ware ESXI | 192.168.3.252 | ESX Host | VMWare Hypervisor |
| iqshdc01 | 192.168.3.220 | Domänencontroller (VM) | Server 2008 R2 |
| iqshws01 | 192.168.3.221 | Windows7 Client (VM) | Windows7 Enterprise |
| iqshnas01 | 192.168.3.222 | NAS Laufwerk (NAS) | Iomega Nas StorCenter ix2-200 |
| iqshbu01 | 192.168.3.223 | Alpha 2000<br>Schul-Mitgliedsserver (Physik) | Server 2008 R2 |

# 2. Datenschutz

## 2.1 Einhaltung der Datenschutzmaßnahmen

Als Grundsatz gelten die Regeln der Datenschutzverordnung Schule.

## 2.2 Anforderung an die Datensicherung

Die Anforderungen gliedern sich in folgende Punkte:

- Benachrichtigung der erledigten Backupjobs.
- Verschlüsselung der Datensicherung
- Einhaltung der Datenschutzverordnung Schule
- Sicherung auf NAS System
- Sicherung auf externe Festplatten
- Zentrale Überwachungsfunktion

## 2.3 Umgang und Handhabung der Datensicherung

### 2.3.1 Auszüge aus dem LDSG (Landesdatenschutzgesetz)

Als weitere Grundlage dieses Konzeptes gelten die Paragraphen 5 und 6 des LDSG.

#### 2.3.1.1 § 5 Maßnahmen zur Datensicherheit

(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen. Dabei ist insbesondere
1. Unbefugten der Zugang zu Datenträgern, auf denen personenbezogene Daten gespeichert sind, zu verwehren,
2. zu verhindern, dass personenbezogene Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können,
3. zu gewährleisten, dass die datenverarbeitende Person, der Zeitpunkt und Umfang der Datenverarbeitung festgestellt werden kann.

(2) Es sind die technischen und organisatorischen Maßnahmen zu treffen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. Automatisierte Verfahren sind vor ihrem erstmaligen Einsatz und nach Änderungen durch die Leiterin oder den Leiter der datenverarbeitenden Stelle oder eine befugte Person freizugeben.

(3) Die Landesregierung regelt durch Verordnung die Anforderungen an das Sicherheitskonzept sowie die Freigabe automatisierter Verfahren und weitere Einzelheiten einer ordnungsgemäßen Datenverarbeitung der öffentlichen Stellen. Das Unabhängige Landeszentrum für Datenschutz ist anzuhören.

#### 2.3.1.2 § 6 Maßnahmen zur Datensicherheit bei Einsatz automatisierter Verfahren

(1) Automatisierte Verfahren sind so zu gestalten, dass eine Verarbeitung personenbezogener Daten erst möglich ist, nachdem die Berechtigung der Benutzerin oder des Benutzers festgestellt worden ist.
(2) Zugriffe, mit denen Änderungen an automatisierten Verfahren bewirkt werden können, dürfen nur den dazu ausdrücklich berechtigten Personen möglich sein. Die Zugriffe dieser Personen sind zu protokollieren und zu kontrollieren.
(3) Werden personenbezogene Daten mit Hilfe informationstechnischer Geräte von der datenverarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet, sind die Datenbestände zu verschlüsseln. Die datenverarbeitende Stelle hat sicherzustellen, daß sie die Daten entschlüsseln kann.
(4) Sollen personenbezogene Daten ausschließlich automatisiert gespeichert werden, ist zu protokollieren, wann, durch wen und in welcher Weise die Daten gespeichert wurden. Entsprechendes gilt für die Veränderung und Übermittlung der Daten. Die Protokolldatenbestände sind ein Jahr zu speichern. Es ist sicherzustellen, daß die Verfahren und Geräte, mit denen die gespeicherten Daten lesbar gemacht werden können, verfügbar sind.
(5) Die datenverarbeitenden Stellen haben die ordnungsgemäße Anwendung der automatisierten Verfahren zu überwachen.

## 2.4 Kennwortsicherheit

### 2.4.1 Verwendete Kennwörter und Verfahrensweisen

1. Das Dienstkennwort für die Datensicherung wird zentral verwaltet. Dies bedeutet, dass die IQSH das Kennwort für die Datensicherung festlegt und verwahrt.
   Das Benutzer Konto wird 1x jährlich per Script geändert. Die Länge des Kennwortes beträgt 8 Zeichen.
   Ob eine regelmäßige Änderung der Backup-Kennwörter erfolgt, wird stichprobenartig von der IQSH geprüft. Der Dienstleister stellt eine Änderung der Kennwörter per Script sicher.

2. Das Sitzungs-und Widerherstellungskennwort, sowie das Datenverschlüsselungskennwort wird während der Installation festgelegt. Nach einer eventuellen Rücksicherung von Daten oder dem System werden die Kennwörter geändert. Die Kennwörter verbleiben in der jeweiligen Schule zur sicheren Verwahrung.

## 2.5 Verantwortlichkeit und Vorgehensweise

Die Verantwortung für die Datensicherung trägt die jeweilige Schulleiterin bzw. der jeweilige Schulleiter. Sollte eine Lehrkraft mit den Aufgaben des Austauschens von Datenträgern und oder der Durchführung der Datensicherung beauftragt werden, hat diese schriftlich zuzusichern das ausreichende Kenntnisse auf dem Gebiet der Datensicherung vorhanden sind. (Siehe DSVO **[Datenschutzverordnung Schule]** §10 Abs.5)
Wenn eine zentrale Speicherung der Daten erfolgen soll, ist dies vertraglich mit dem jeweiligen Dienstleister (Dataport, o.ä.) zu vereinbaren. (Auftragsdatenverarbeitung)

## 2.6 Aufbewahrungsfristen der Datensicherung

Die erstellten Backupdateien werden für einen Zeitraum von 2- 8 Wochen auf den Datenträgern aufbewahrt und danach durch die Datensicherungssoftware überschrieben. Der Zeitraum ist Abhängig von den Gegebenheiten an den Schulen.
(Speicherplatz-Voraussetzungen)

# 3. Durchführungsanleitung und Dokumentation

## 3.1 Testbetrieb und Evaluierung

Alle hier in diesem Konzept aufgeführten Schritte zur Installation und Konfiguration und Ausführung der Sicherung sind ausführlich in einer Testumgebung evaluiert worden, so dass eine reibungslose Durchführung an den Schulen gewährleistet ist.

## 3.2 Standortspezifische Dokumentation

Für jeden Standort wird eine Kurzdokumentation / Anleitung auf Grundlage dieses Konzeptes erstellt und um entsprechende Eckdaten, wie IP Adressen, Rechnernamen und Benutzerkonten ergänzt. Die IQSH erstellt Vorgaben für die Anpassung der Installationsdokumentation für die jeweilige Schule / Standort.

## 3.3 Erweiterung des Netzplanes durch Datensicherungsanteil

Aufnahme der Geräte in die Darstellung der informationstechnischen Vernetzung (Netzplan) gemäß §3 Abs 2 Punkt 4 DSVO. Der Anteil Datensicherung wird in der bereits bestehenden Dokumentation erweitert.

## 3.4 Inventarisierung der Geräte und der eingesetzten Software

Die Erweiterung der Dokumentation um den Datensicherungsanteil wird seitens der IQSH ergänzt und ständig weiter gepflegt. Entsprechende Vorlagen existieren bereits.

# 4. Sicherungstechnologien

Folgende Geräte und Technologien sollen zum Einsatz kommen:

## 4.1 Hardware

Als Sicherungsgerät dient ein NAS* Laufwerk der Firma Iomega.
(StorCenter ix2-200 Network)
Die Entscheidung für das Gerät hatte folgende Aspekte:

- Integriertes Raid System (Raid1, Spiegelung)
- Austauschbare Festplatten
- Erfahrungswerte im Bereich Schulnetze
- Möglichkeit der Active Directory Integrierung
- Gigabit Netzwerk Anbindung
- Möglichkeit des weiteren Anschlusses von Festplatten und Druckern.

* „Network Attached Storage“ (NAS) bezeichnet einfach zu verwaltende Dateiserver. Allgemein wird NAS eingesetzt, um ohne hohen Aufwand unabhängige Speicherkapazität in einem Rechnernetz bereitzustellen.

### 4.1.1 Eckdaten zum Datensicherungsmedium (NAS)

Iomega Storcenter ix2-200 (NAS-System)
CPU Marvel 6281 1,0 GHz
Speicher 256 MB
Raid-System 1, JBOD
Festplatten 2 x S-ATA, 500 GB, 1TB, 2TB
Dateisystem EXT3
Netzwerk 1 x Gigabit
Anschlüsse 3 x USB
Netzwerk-Protokolle AFP, NFS, CIFS, FTP HTTP, HTTPS, SNMP, Bonjour, Rally
Media Server UPnP
Abmessungen (B X T X H) 200 x 196 x 168 mm
Gewicht 5,8 kg

Stromverbrauch Betrieb 19 Watt
Stromverbrauch Standby 12 Watt
Geräuschpegel Betrieb 25 dB(a)
Geräuschpegel Standby 22 dB(a)
Datenrate Lesen 30 MB/s
Datenrate Schreiben 20 MB/s

### 4.1.2 Sicherungsfestplatten

Als Basis wird angenommen, das zwei externe USB Festplatten, nach Möglichkeit gleicher Bauart und Kapazität zum Einsatz kommen.

(Beispielabbildung)

### 4.1.3 Backup-Server

Als Standortserver der Schulen wird ein alpha 2000 Rechner (Server) eingesetzt.
Die Alpha 2000 Rechner / Server unterliegen keinen einheitlichen Standards seitens der Hardware-Konfiguration. Die Server dienen als Daten und Anwendungsserver.
Die Datensicherungssoftware wird auf dem bereits konfigurierten System aktiviert bzw. installiert.

## 4.2 Software

### 4.2.1 Betriebssysteme

Konzeptionell aufgezeigt wird die Server-Datensicherung auf den Plattformen Server 2008 / R2 sowie dem Server 2003 / R2 durchgeführt.



### 4.2.2 CA ARCserve Backup r15


CA ARCserve Backup ist eine hochleistungsfähige Lösung für die Datenschutzanforderungen von Unternehmen und öffentlichen Einrichtungen mit heterogenen Umgebungen. Sie bietet flexible Leistungsfähigkeit bei der Sicherung und Wiederherstellung, unkomplizierte Verwaltung, breite Geräteunterstützung und unübertroffene Zuverlässigkeit. Mit dieser Lösung kann die Datenspeicherungsfähigkeiten optimiert werden, indem die Datenschutzstrategien an die individuellen Speicheranforderungen anpasst werden. Darüber hinaus ermöglicht die flexible Benutzeroberfläche erweiterte Konfigurationen und bietet unabhängig von den technischen Vorkenntnissen der Benutzer ein kostengünstiges Mittel zur Implementierung und Verwaltung einer Vielzahl von Agenten und Optionen. Diese Version von CA ARCserve Backup für Windows ist die nächste Generation in der Produktfamilie von CA ARCserve Backup. Sie baut auf den Funktionen der vorhergehenden Versionen auf und bietet gleichzeitig neue Funktionalität, um bei der Optimierung der Sicherungs- und Wiederherstellungsvorgänge zu helfen. CA ARCserve Backup gewährleistet einen umfassenden Datenschutz für verteilte Umgebungen und bietet virenfreie Sicherungs- und Wiederherstellungsvorgänge. Mit einer umfangreichen Palette an Optionen und Agenten bietet es besseren Datenschutz in der gesamten Organisation.
Zu den erweiterten Funktionen zählen Online-Sicherung und -Wiederherstellung bei laufendem Betrieb von Anwendungen und Datendateien, optimierte Geräte- und Datenträgerverwaltung sowie Systemwiederherstellung.

#### 4.2.2.1 Leistungsmerkmale CA ARCserve Backup R15

Visualisierung der Infrastruktur zur schnellen Verwaltung der gesamten Umgebung.
Erstellung von SRM-Berichten, um Problemen vorzubeugen, bevor sie unvorhergesehene Ausfälle verursachen.
Datenschutz für physische und virtuelle Server in einem einzigen, kosteneffizienten Tool.
Integrierte Datendeduplizierung — verbessert die Effizienz von Backup und Recovery: längere Aufbewahrungszeiträume, kostengünstiges Verfahren zur Speicherreduzierung, Schutz kritischer Daten sowie Integration, Konfiguration und Verwaltung der Datendeduplizierung in der vorhandenen Backupumgebung.

Dashboard mit SRM-Reporting — stellt Ihre Backupumgebung in einer grafischen Ansicht dar. Status aller Backupaktivitäten überwachen, Knoten aufspüren, die die meiste Zeit beanspruchen; gesicherte Daten lokalisieren; feststellen, ob die Daten verschlüsselt und für die Disaster-Recovery bereit sind, und die Datenträger-, Platten- und Speichernutzung auf jedem Ihrer Produktionsserver verfolgen.
Zentrale Verwaltung und Administration — verwendet eine dreistufige Architektur, die es Administratoren ermöglicht, Backup- und Wiederherstellungsjobs, Mediengeräte, Aktivitätsprotokolle, Warnungen, Kataloge, Produktlizenzen und Berichte über einen zentralen Punkt, der lokale und dezentrale Server und Standorte einbezieht, zu verwalten, zu ändern und zu kontrollieren.

Flexible Backupverfahren — unterstützen Backups auf Platte, Backups auf Band, D2D2T-Backups, VTL- und Microsoft Volume Shadow Copy Service-Snapshots, Hardware-Snapshots, Multiplexing und Multistreaming.

#### 4.2.2.2 Systemvoraussetzungen CA ARCserve Backup R15

Systemvoraussetzungen für das CA ARCserve Backup-Basisprodukt
Für CA ARCserve Backup gelten folgende Mindestsystemvoraussetzungen:

CPU: 600-MHz-Prozessor, Pentium-III-kompatibel oder schneller; 1 GHz oder schneller empfohlen
RAM: 512 MB, 1 GB oder mehr empfohlen
Festplattenspeicher:
Primärserver: 800 MB plus 1,3 GB für Agent-Bereitstellungspakete
Mitgliedsserver: 450 MB plus 1,3 GB für Agent-Bereitstellungspakete
Diese Version von CA ARCserve Backup installiert folgende .NET-Komponenten:
.NET 2.0 SP2, bis zu 500 MB freier Speicherplatz erforderlich
.NET 3.0 SP1, bis zu 500 MB freier Speicherplatz erforderlich
.NET 3.5 SP1, bis zu 500 MB freier Speicherplatz erforderlich
Microsoft .NET Framework

CA ARCserve Backup erfordert folgende Versionen von Microsoft .NET Framework:
Microsoft .NET Framework 3.5 SP1 auf Windows Server 2003- und Windows Server 2008-Systemen
CA ARCserve Backup-Datenbank
CA ARCserve Backup unterstützt die folgenden Anwendungen, die als Host der CA ARCserve Backup-Datenbank (ASDB) dienen sollen:
Microsoft SQL Server 2008 Express Edition
Microsoft SQL Server 2008 Enterprise/Standard Edition
Microsoft Windows Server 2000 mit Service Pack 4
Microsoft SQL Server 2005 mit Service Pack 1, Service Pack 2 oder Service Pack 3
Hinweis: Beachten Sie, dass Sie zusätzlich zu diesen Voraussetzungen über den erforderlichen Speicherplatz für die CA ARCserve Backup-Standarddatenbank verfügen müssen. Je nach Nutzung kann die Datenbank auf eine Größe von bis zu mehreren GB anwachsen.

Adobe Reader:
Adobe Acrobat Reader 8 und höher
Internetbrowser:
Internet Explorer 6.0 SP1
Internet Explorer 7.0
Internet Explorer 8.0 (alle Rendering-Modi)

#### 4.2.2.3 Erforderlicher Festplattenplatz zum Installieren

**Windows-x64-Systeme**

- Primärserver und Standalone-Server: 1 GB bis 2,13 GB freier Speicherplatz.
- Mitgliedsserver: 0,71 GB (727 MB) bis 1,97 GB freier Speicherplatz.

**Windows-x86-Systeme**

- Primärserver und Standalone-Server: 0,77 GB (788 MB) bis 1,34 GB freier Speicherplatz.
- Mitgliedsserver: 0,67 GB (690 MB) bis 0,91 GB (932 MB) freier Speicherplatz.

#### 4.2.2.4 Datensicherungskonto

CA ARCserve Backup verwendet für Verwaltungszwecke einen eigenen Authentifizierungsmechanismus. Dieser erstellt einen Standardbenutzer namens "caroot", wenn Sie CA ARCserve Backup installieren. Mit caroot können Sie sich bei der CA ARCserve Backup-Manager-Konsole anmelden. Das caroot-Standardbenutzerkonto hat Root-Berechtigungen für alle CA ARCserve Backup-Funktionen. Sie können ein Kennwort für das caroot Benutzerprofil während der Konfiguration der Software bzw. im Anschluss daran mit dem Benutzerprofil-Manager einrichten. Der Benutzerprofil-Manager ermöglicht außerdem das Erstellen zusätzlicher Benutzerprofile.
Das caroot-Kennwort kann aus einer Kombination von alphanumerischen Zeichen und Sonderzeichen bestehen, darf jedoch 15 Byte nicht überschreiten. Ein Kennwort mit 15 Byte entspricht etwa 7 bis 15 Zeichen. Hinweis: CA ARCserve Backup-Benutzernamen steuern lediglich den Zugriff auf Funktionen von CA ARCserve Backup und sollten nicht mit den Benutzerinformationen verwechselt werden, die zur Anmeldung beim Betriebssystem erforderlich sind (Anmeldename und Kennwort).

### 4.2.3 CA ARC Serve Replication and High Availability

Für größere Institutionen, wie Schulverbände, Gesamtschulen und Schulen die ein hohes Datenaufkommen haben, kann eine zentrale Sicherung Ihrer Daten in Betracht gezogen werden.

#### 4.2.3.1 Leistungsmerkmale CA ARCServe Replication and High Availabillity

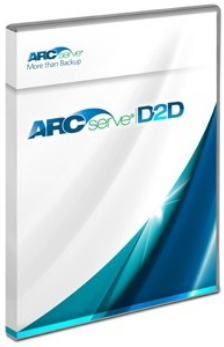
- Hochverfügbarkeit des gesamten Systems schützt das Windows-Betriebssystem, den Systemstatus, die Anwendungen und die Daten durch Replikation "physisch zu virtuell" bzw. "virtuell zu virtuell" und Failover.
- Die LAN- und WAN-optimierte Replikation gewährleistet kontinuierlichen Schutz interner und externer Daten.
- Datenrücklauf für kontinuierlichen Datenschutz (Continuous Data Protection, CDP) zwischen Backups.
- Automatisierte, unterbrechungsfreie Recoverytests mit VSS Snapshot-Management, um anwendungskonsistente Backups zu erzielen.
- Echtzeitüberwachung von Servern und Anwendungen mit automatisiertem und manuellem Failover und manuellem Failback.
- Servergruppenmanagement, das ein gemeinsames Failover mehrerer Server oder von Serverumgebungen ausführt, um die Leistung zu steigern.
- Einheitliche, webgestützte Management- und Reportingkonsole – optional mit Redundanz und Failover, um Bereitstellung und Wartung zu beschleunigen und zu vereinfachen.

#### 4.2.3.2 Systemvoraussetzungen CA ARCServe Replication and High Availabillity

Es gelten die Systemvoraussetzungen vom ARCServe Basisprodukt. (3.2.2.2 und 3.2.2.3)

### 4.2.4 CA ArcServe D2D r15 (Disk to Disk Backup)

Zur Komplettsystemwiederherstellung ist zusätzlich das Produkt D2D beschrieben.




CA ArcServe D2D ist eine festplattenbasierte Backuplösung, die den Schutz und die Widerherstellung von Daten vereinfacht. D2D bietet eine Wiederherstellung auf einer anderen Hardware sowie unbegrenzte, inkrementelle Snapshots auf Blockebene.
Nach einem ersten vollständigen Backup werden die Backups inkrementell durchgeführt, wodurch die Notwendigkeit eines weiteren vollständigen Backups entfällt. Dadurch werden die Zeitfenster für Sicherungen, der Netzwerkverkehr, der Speicherplatzbedarf sowie die Belastung für Anwendungen reduziert.

#### 4.2.4.1 Leistungsmerkmale CA ArcServe D2D R15

- Unbegrenztes, inkrementelles Backup auf Blockebene.

- Single Snapshot Backup mit vier Wiederherstellungsarten bietet die Möglichkeit, Dateien, Volumes, Datenbanken oder auch das gesamte System auf jeden beliebigen Server in physischen wie auch virtuellen Umgebungen von einem einzigen Backupdurchlauf wiederherzustellen.

- Die Bare Metal-Wiederherstellung auf eine andere Hardware stellt eine äußerst schnelle Methode bereit, einen abgestürzten Server auf dieselbe oder eine andere Hardware wiederherzustellen. Dies verkürzt einen Vorgang, der bis zu 36 Stunden dauern kann, auf nur wenige Minuten.

- Anwendungskonsistente Snapshot-Backups stellen sicher, dass die Anwendung ordnungsgemäß angehalten und in einem fehlerfreien Zustand für eine schnelle Datensicherung gesichert wird.

- Die Backupansicht bietet eine vollständige zeitpunktorientierte Sicht auf die Festplatte, um Dateien, Ordner, Volumes und Datenbanken wiederherzustellen.

# 5. Vorbereiten der Hardware für die Sicherung

## 5.1 Vorbereitung des Datensicherungslaufwerks (Iomega NAS)

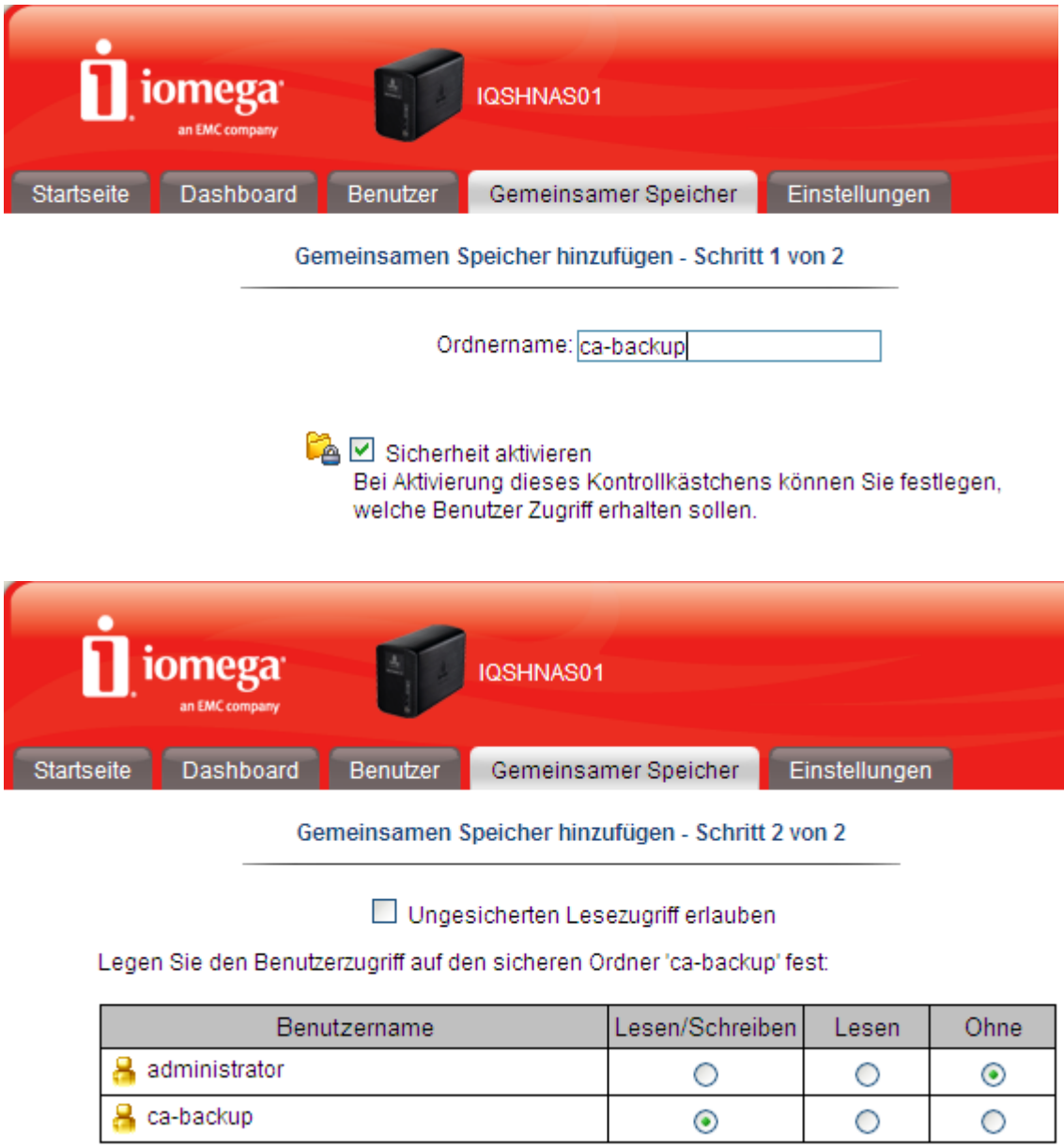
### 5.1.1 Grundeinrichtung als Backuplaufwerk

*Die Grundeinstellungen des Gerätes sind über die mitgelieferte Software CD vorzunehmen. IP im jeweiligen Adressbereiches des Standorts, sowie Benutzername und Kennwort. Anschließend kann die Konfiguration über den Webbrowser erfolgen.*

#### 5.1.1.1 Anlegen eines Backup-Benutzers


Um ein permanentes Backup zu gewährleisten wird ein lokaler Backupuser im Benutzermanagement des NAS Laufwerkes angelegt. Die Authentifizierung wird für den Zugriff auf den später anzulegenden Backup Ordner, sowie den „Backup-Dienst-Benutzer“ von ARCserve benötigt.

#### 5.1.1.2 Anlegen eines Backup-Ordners





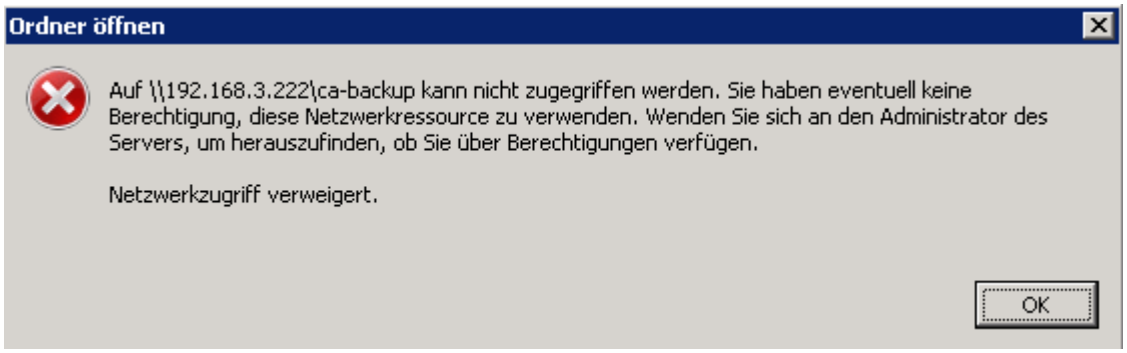


Wichtig ist der Lese und Schreib-Zugriff des Benutzers auf den bereits angelegten Sicherungsordner „ca-backup“


Zusammenfassung

#### 5.1.1.3 Prüfung der Datensicherheit

Seitens des Backupservers ist zu prüfen, ob der Zugriff auf den Ordner gesichert ist. Dies erfolgt durch die Eingabe des UNC Pfades im Windows Explorer.
Beispiel: \\192.168.3.222\ca-backup

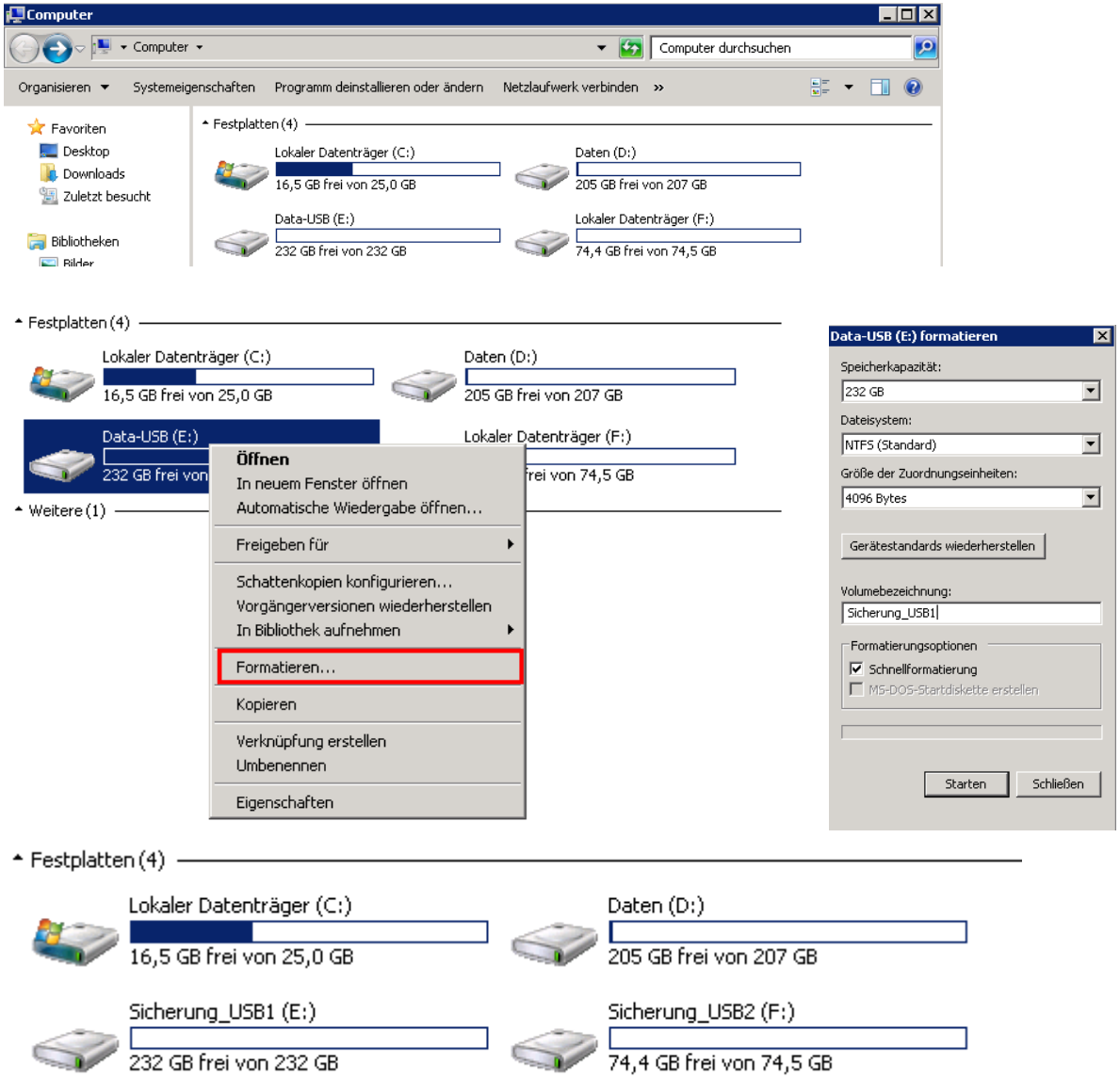



Durch den Zugriff eines nicht authentifizierten Benutzers erfolgt eine Verweigerung.

#### 5.1.1.4 Kennwort für Benutzer und Backup-Ordner

Für jeden einzelnen Standort ist das Kennwort für Benutzer und Ordner individuell festzulegen, administrativ zu dokumentieren und unter Verschluss zu halten.

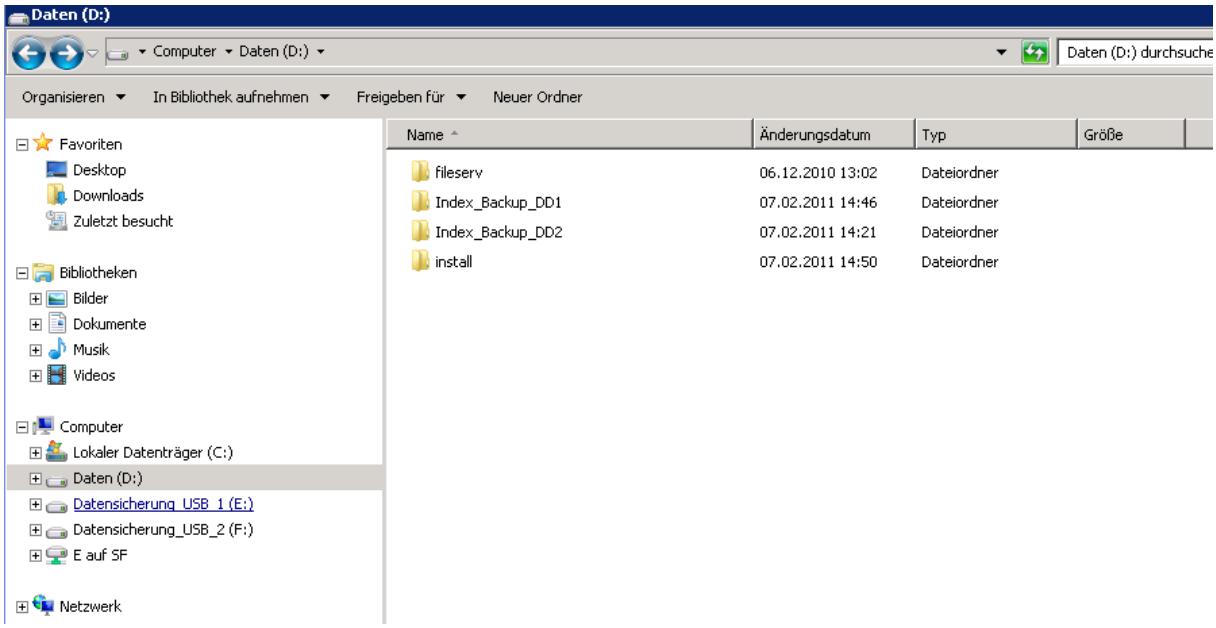
## 5.2 Vorbereitung des Datensicherungslaufwerks (Externes USB Laufwerk)



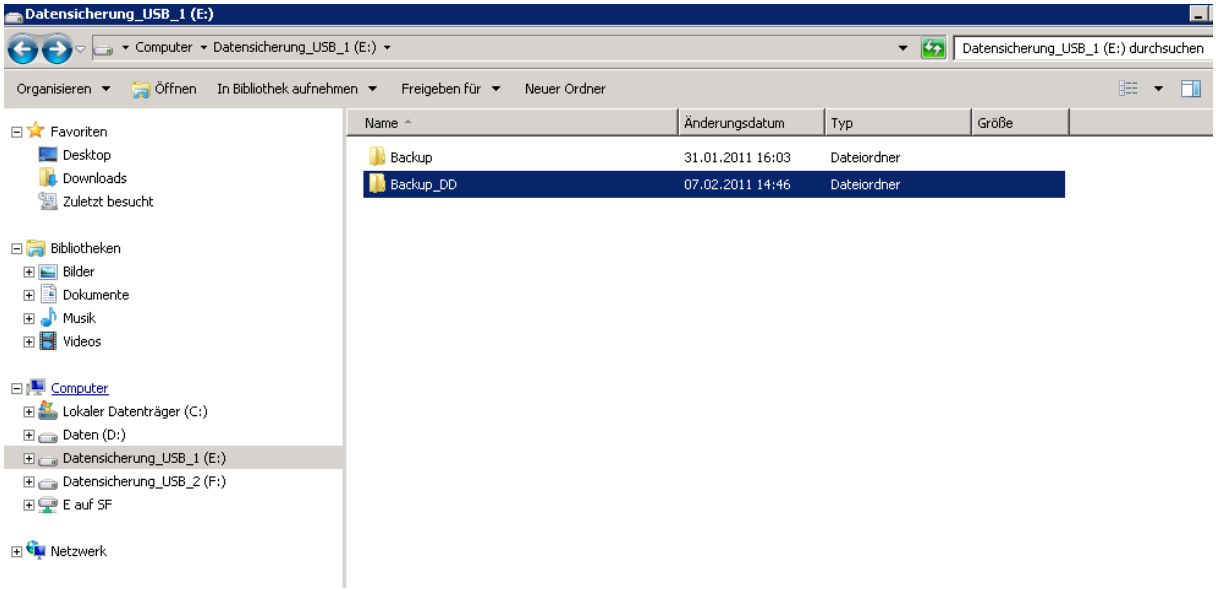

Nachdem die externen USB Laufwerke an den Server angeschlossen wurden, sollten diese im Vorwege formatiert und namentlich benannt werden.

### 5.2.1 Anlage der Sicherungs- und Index Dateiordner

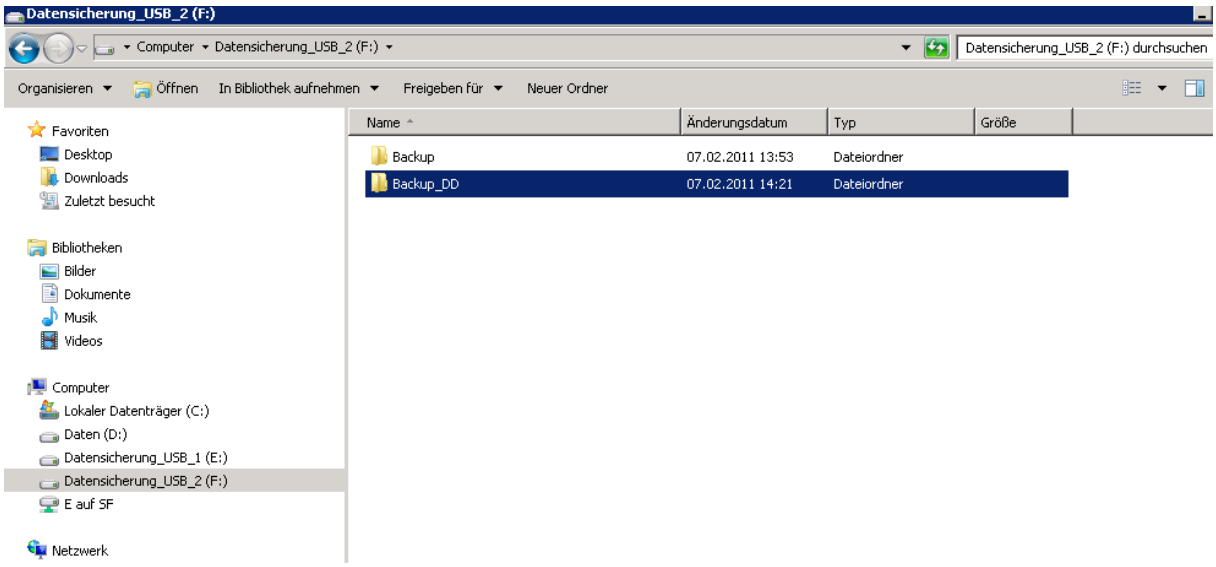
Vor Anlage der Sicherungsjobs ist es erforderlich entsprechende Ordner auf den Sicherungsdatenträgern zu erstellen.




Anlage der Index-Ordner für die Deduplizierungssicherung.
Dies erfolgt auf dem lokalen Laufwerk D:\ des zu sichernden Servers.



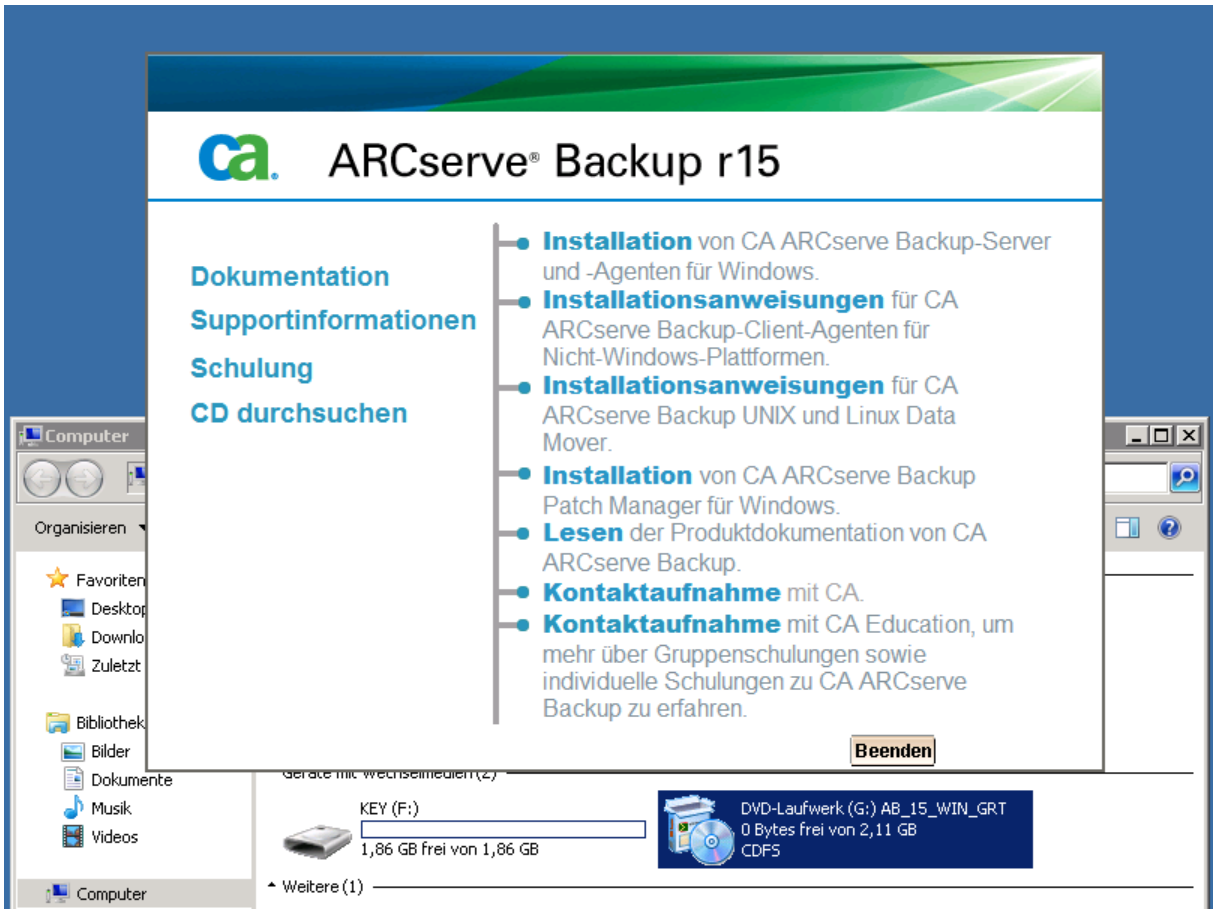

Anlage des Sicherungsordners für die Deduplizierungssicherung (Auf USB1 HDD)



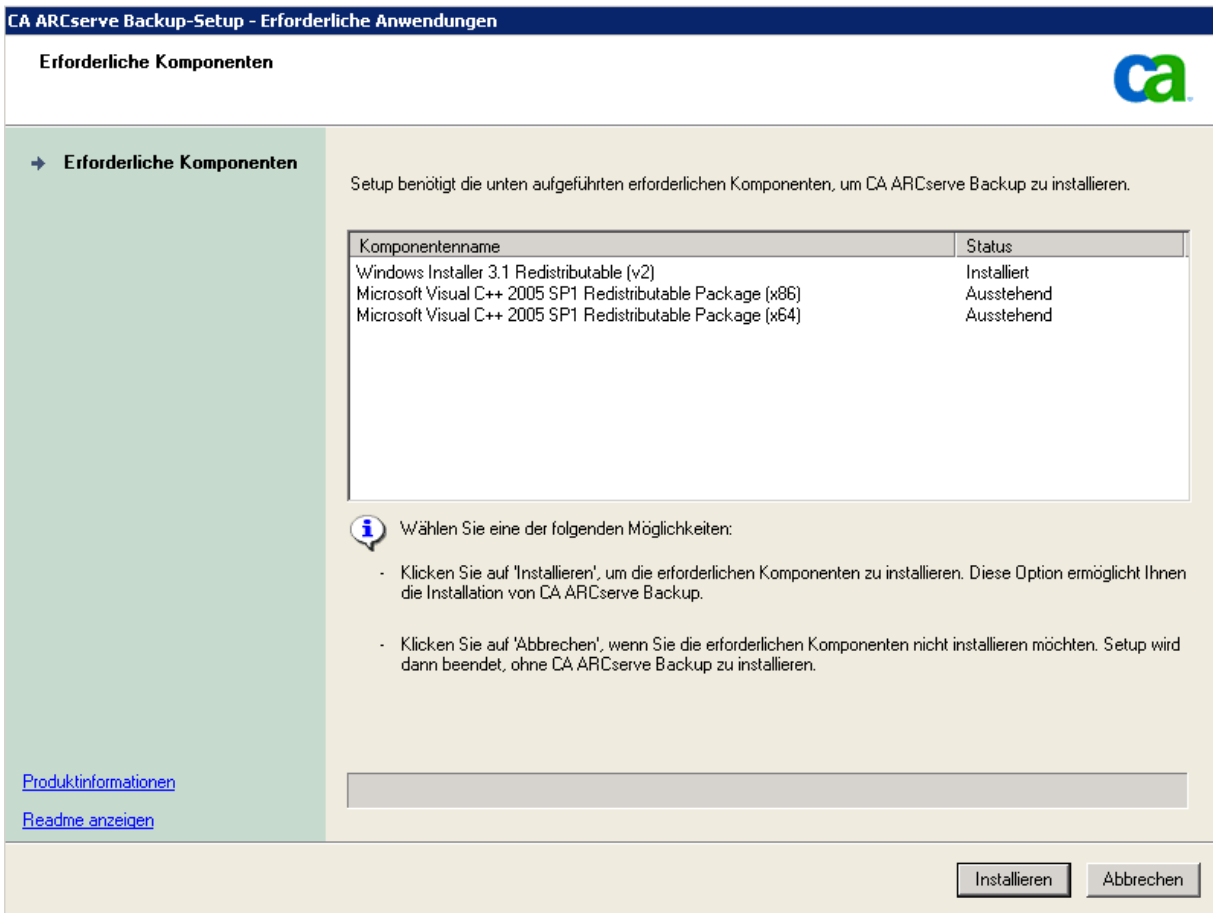

Anlage des Sicherungsordners für die Deduplizierungssicherung (Auf USB2 HDD)

# 6. Installation ARCserve Backup r15

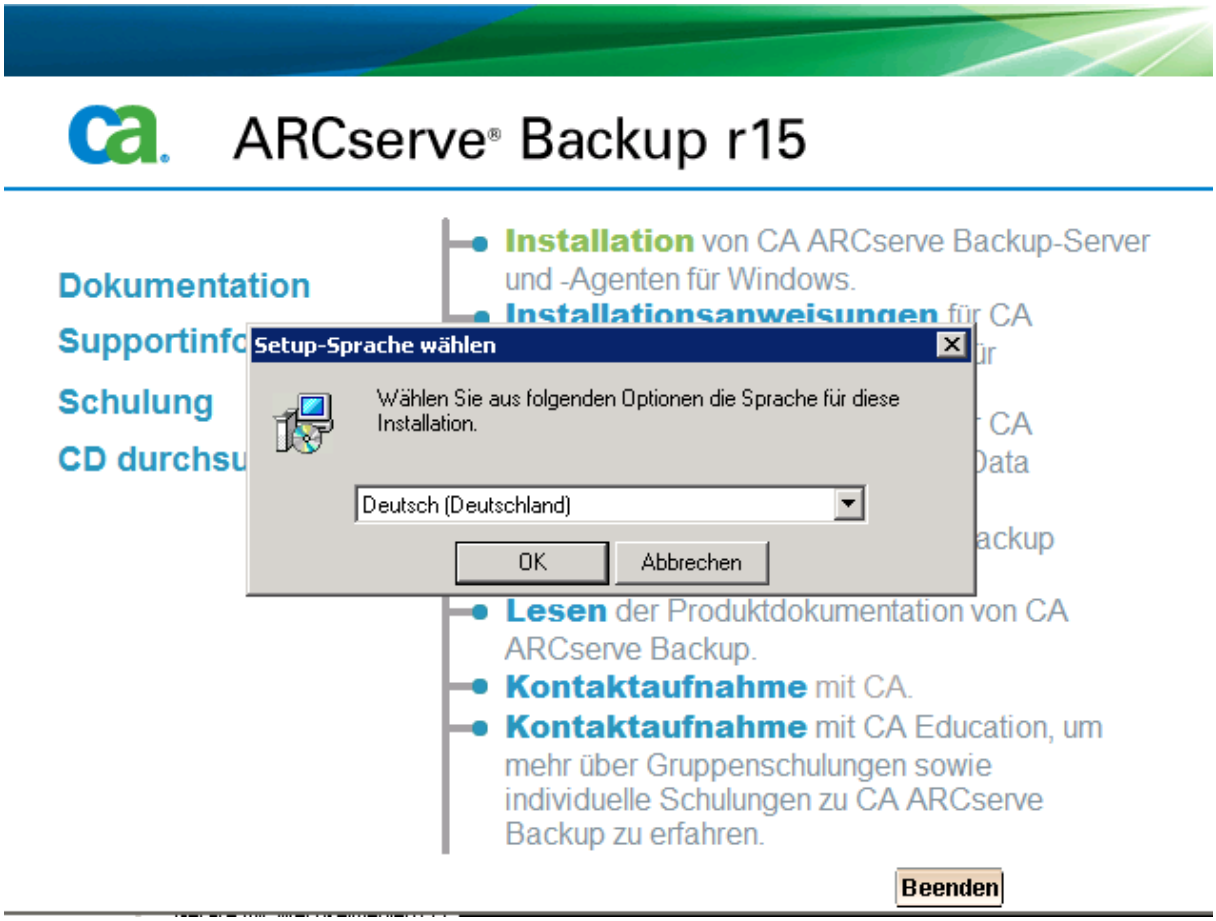
## 6.1 Installation ARCserve Backup r15 auf Server 2008 // R2

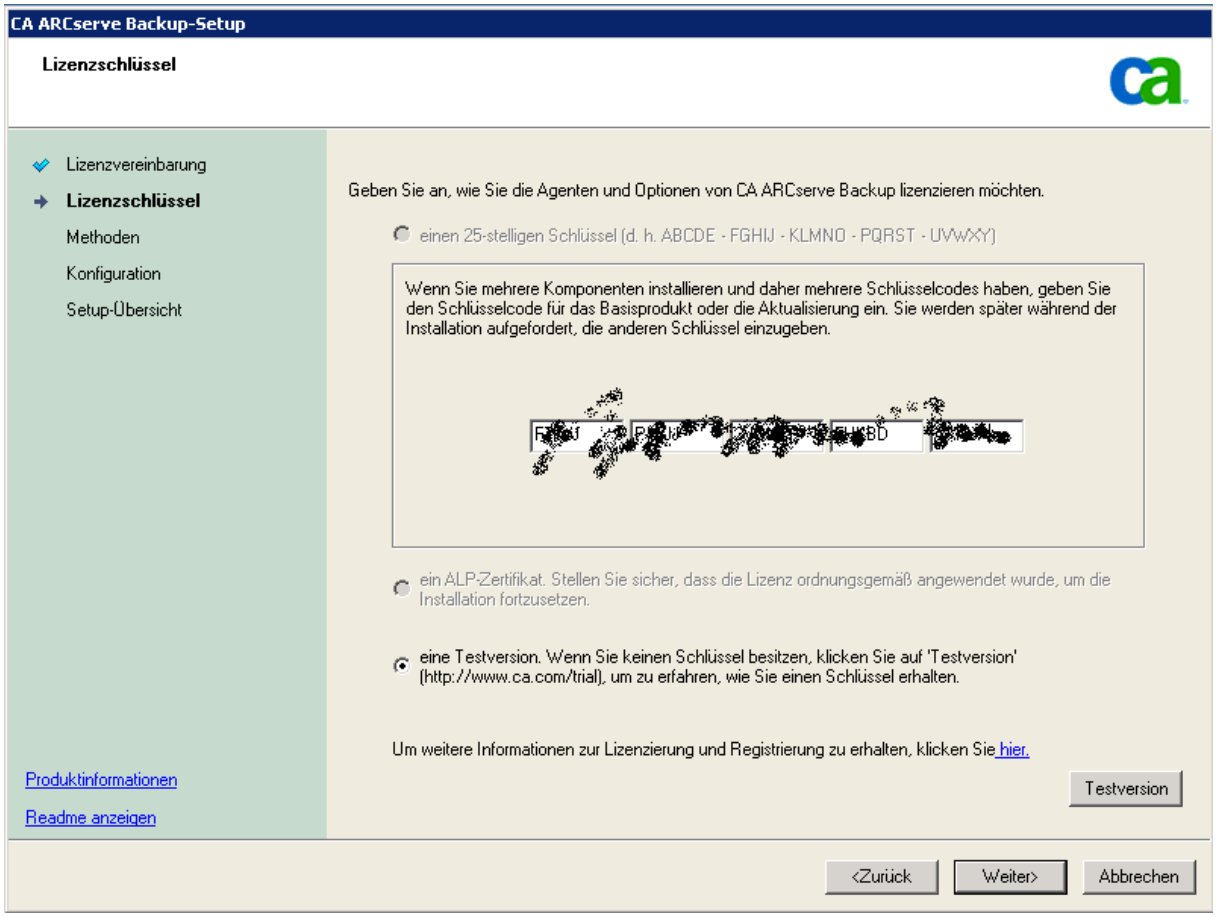



Beginn der Installation durch eingelegten Datenträger oder verbundenes ISO Image.

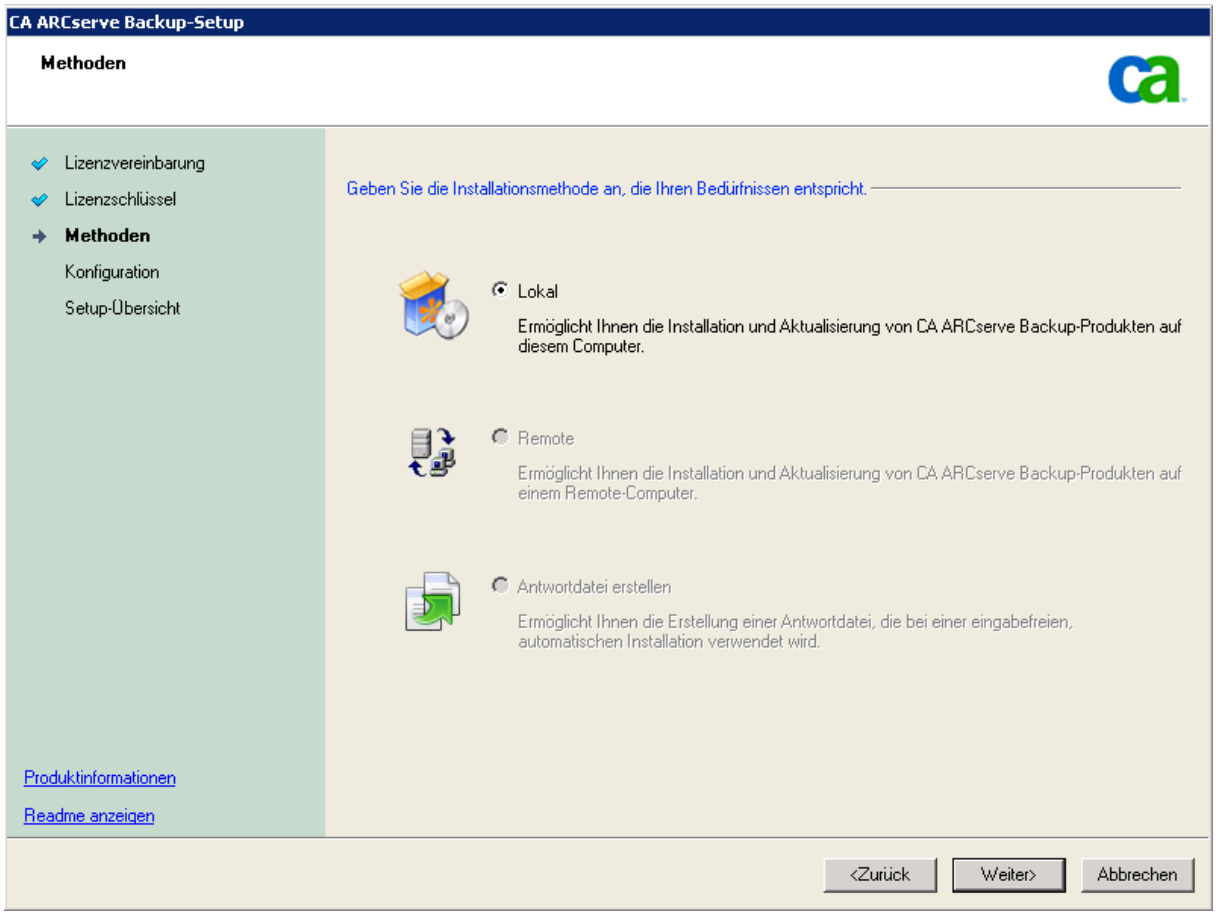


Installation Erforderlicher Komponenten

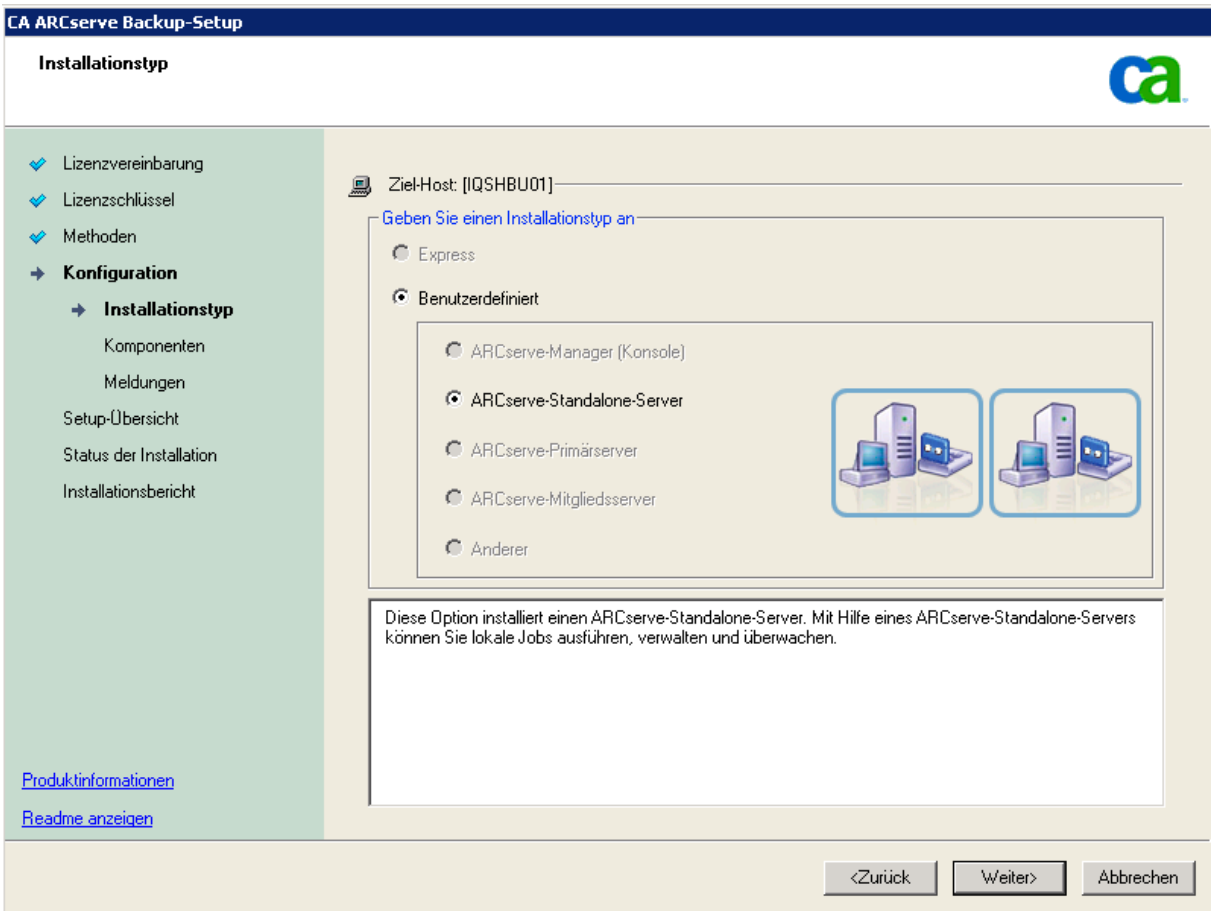

ARCserve® Backup r15
Dokumentation
Supportinfo
Schulung
CD durchsu
Installation von CA ARCserve Backup-Server und -Agenten für Windows.
Installationsanweisungen für CA
Setup-Sprache wählen
Wählen Sie aus folgenden Optionen die Sprache für diese Installation.
Deutsch (Deutschland)
OK
Abbrechen
Lesen der Produktdokumentation von CA ARCserve Backup.
Kontaktaufnahme mit CA.
Kontaktaufnahme mit CA Education, um mehr über Gruppenschulungen sowie individuelle Schulungen zu CA ARCserve Backup zu erfahren.
Beenden



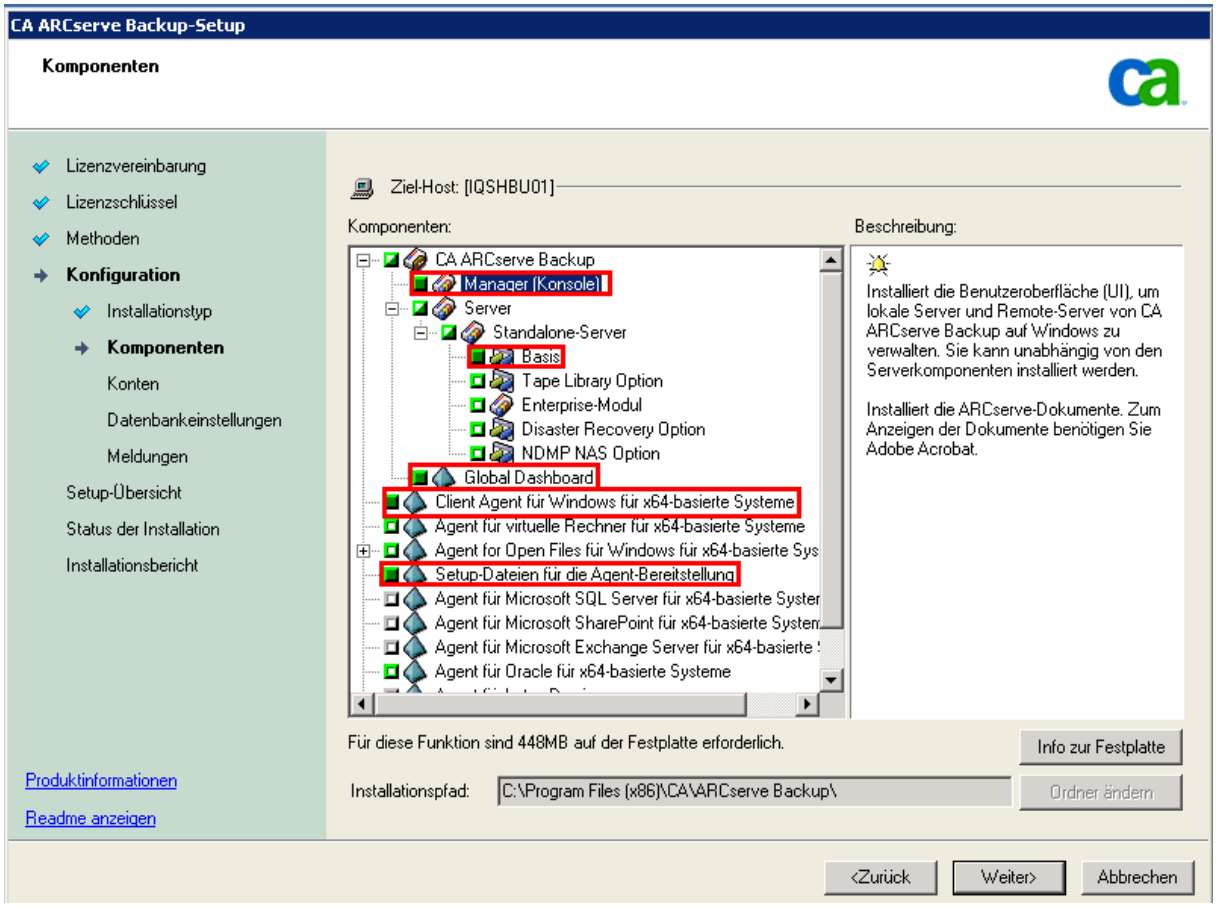
Eingabe des gültigen Lizenzschlüssels für das Windows Standard Modul



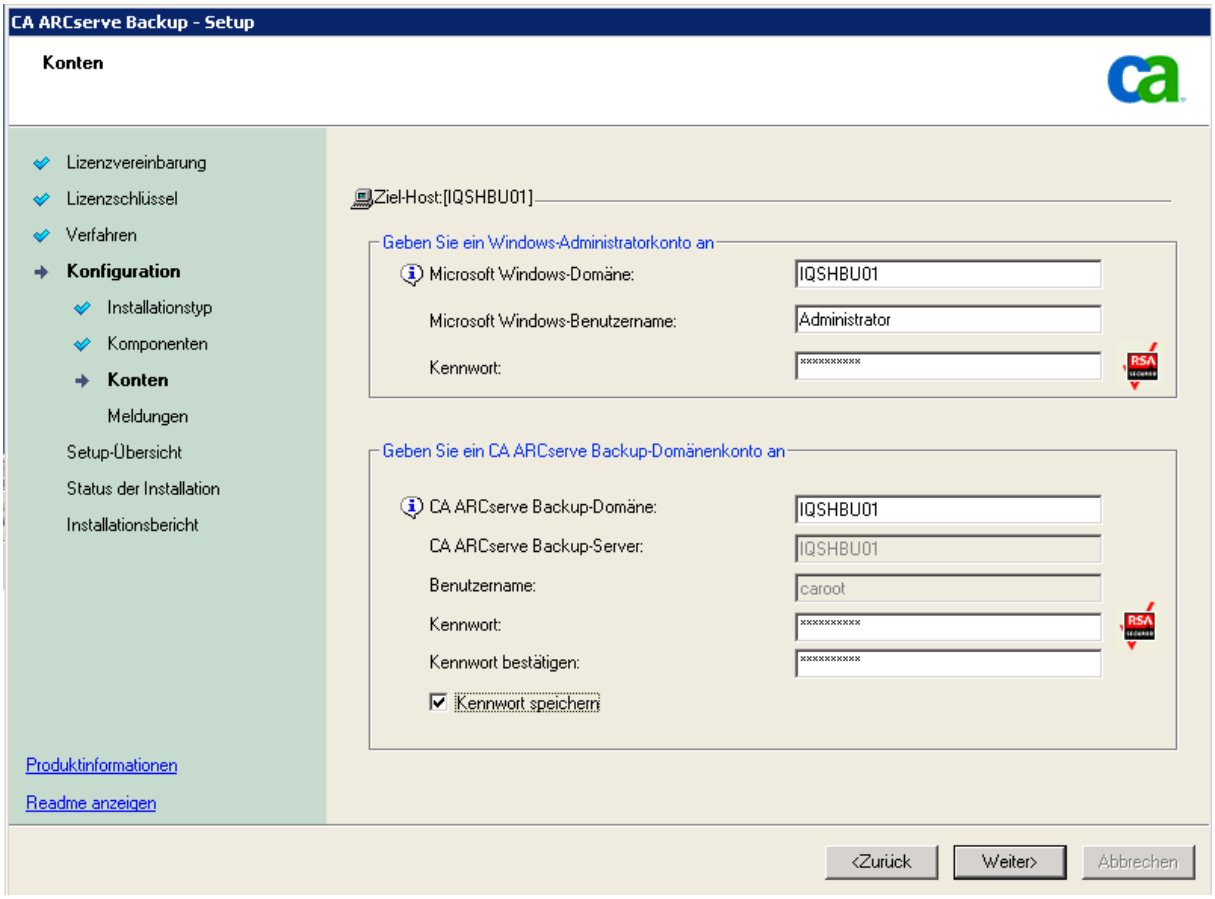
Angabe der lokalen Installationsmethode




Angabe des Installationstyps (Standalone Server)

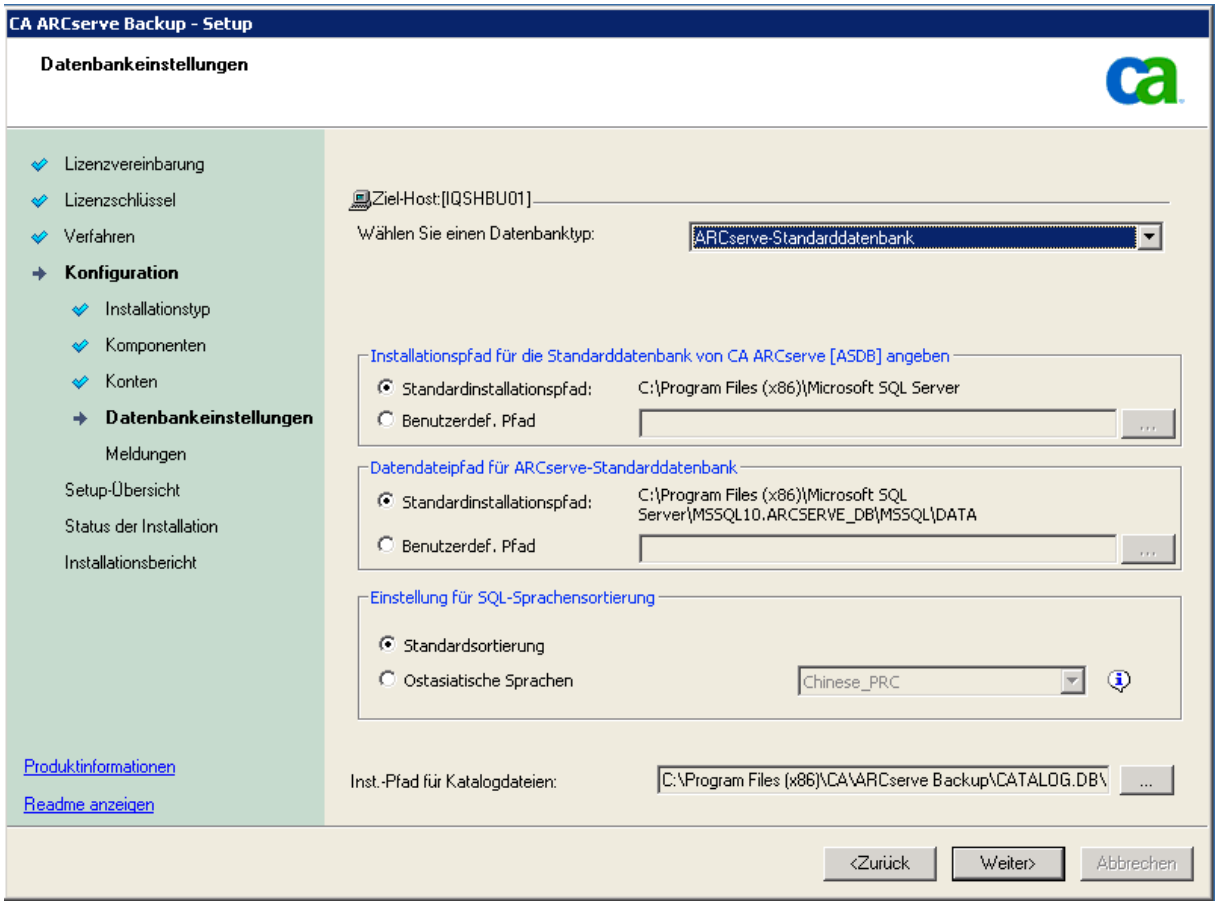


Auswahl der entscheidenden Komponenten.

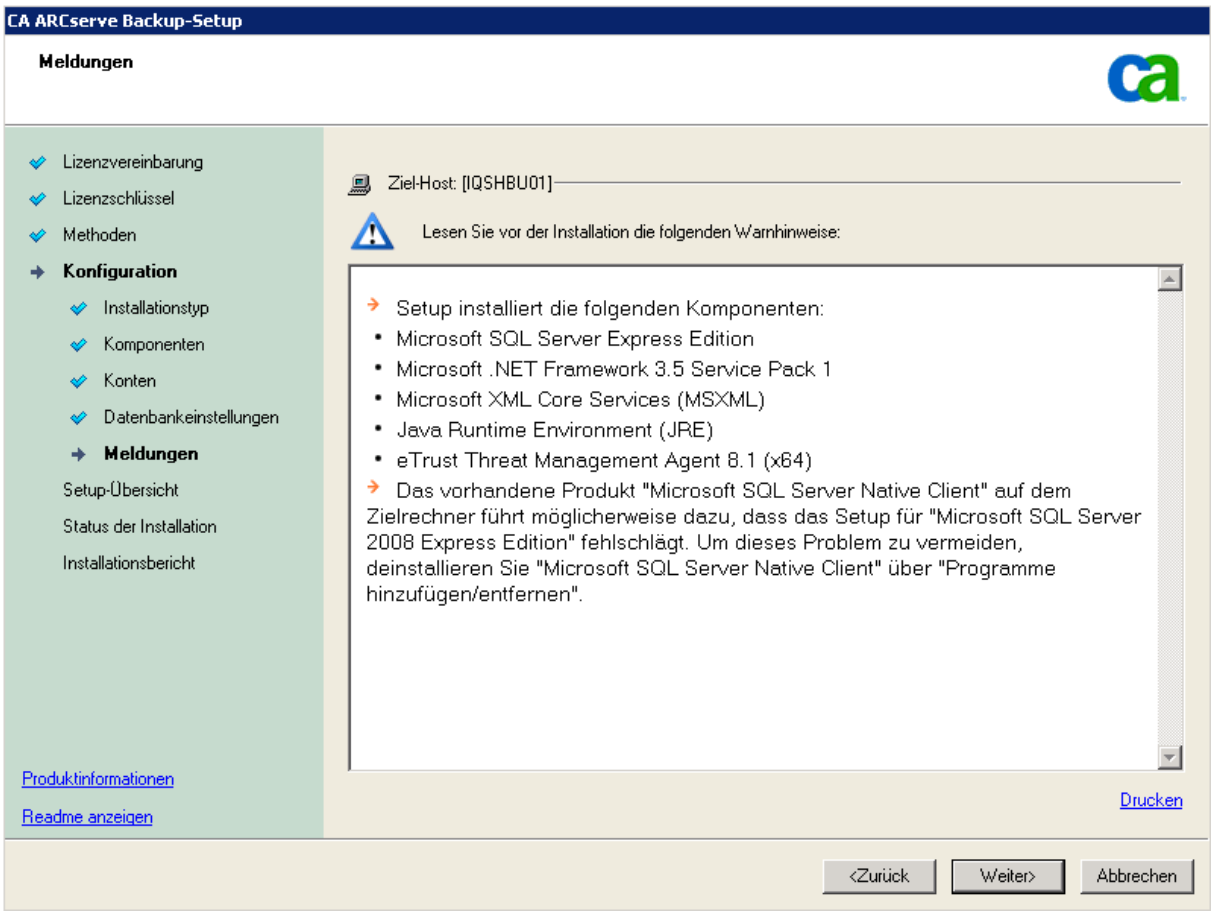



Angabe der Sicherungskonten.

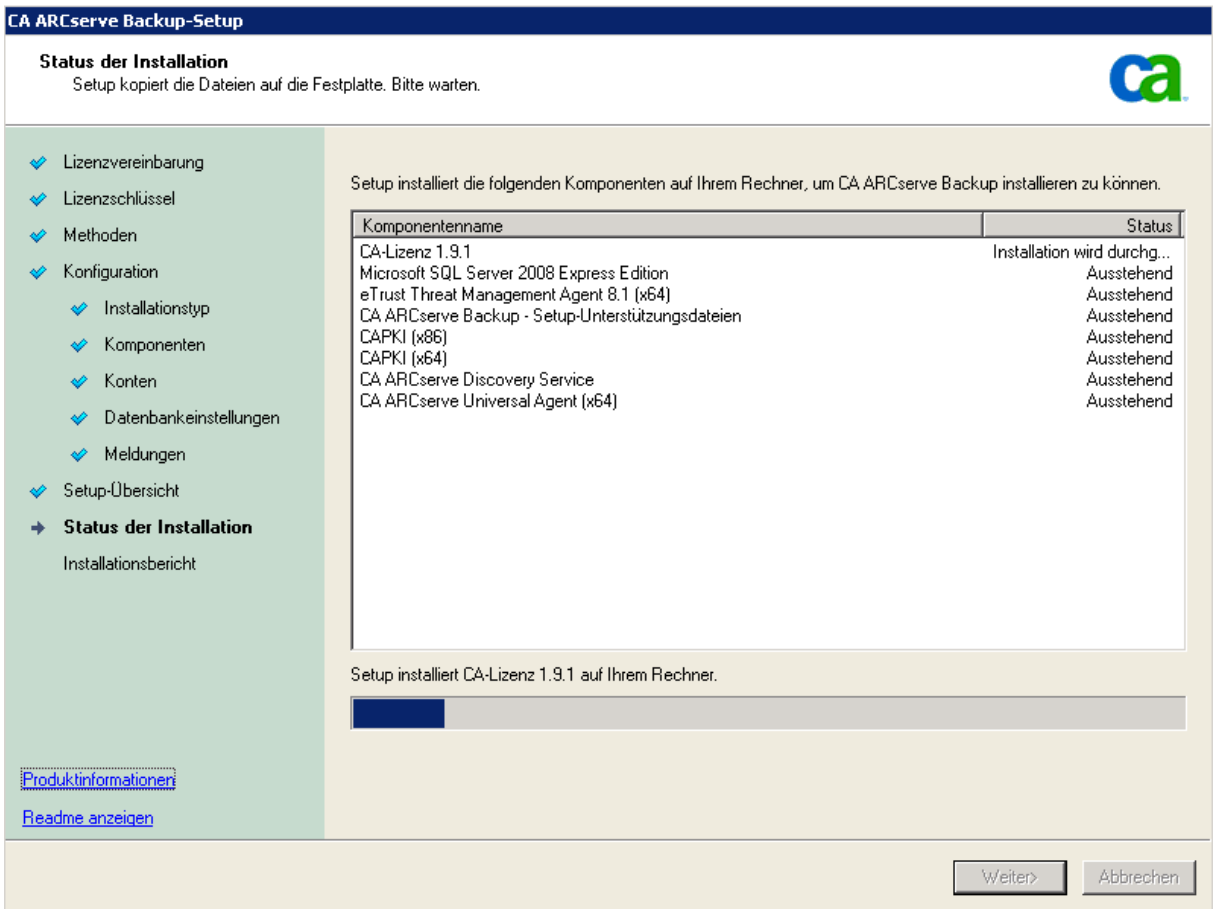
Das Kennwort des „caroot“ Backup Domänenkontos ist pro Standort individuell festzulegen.



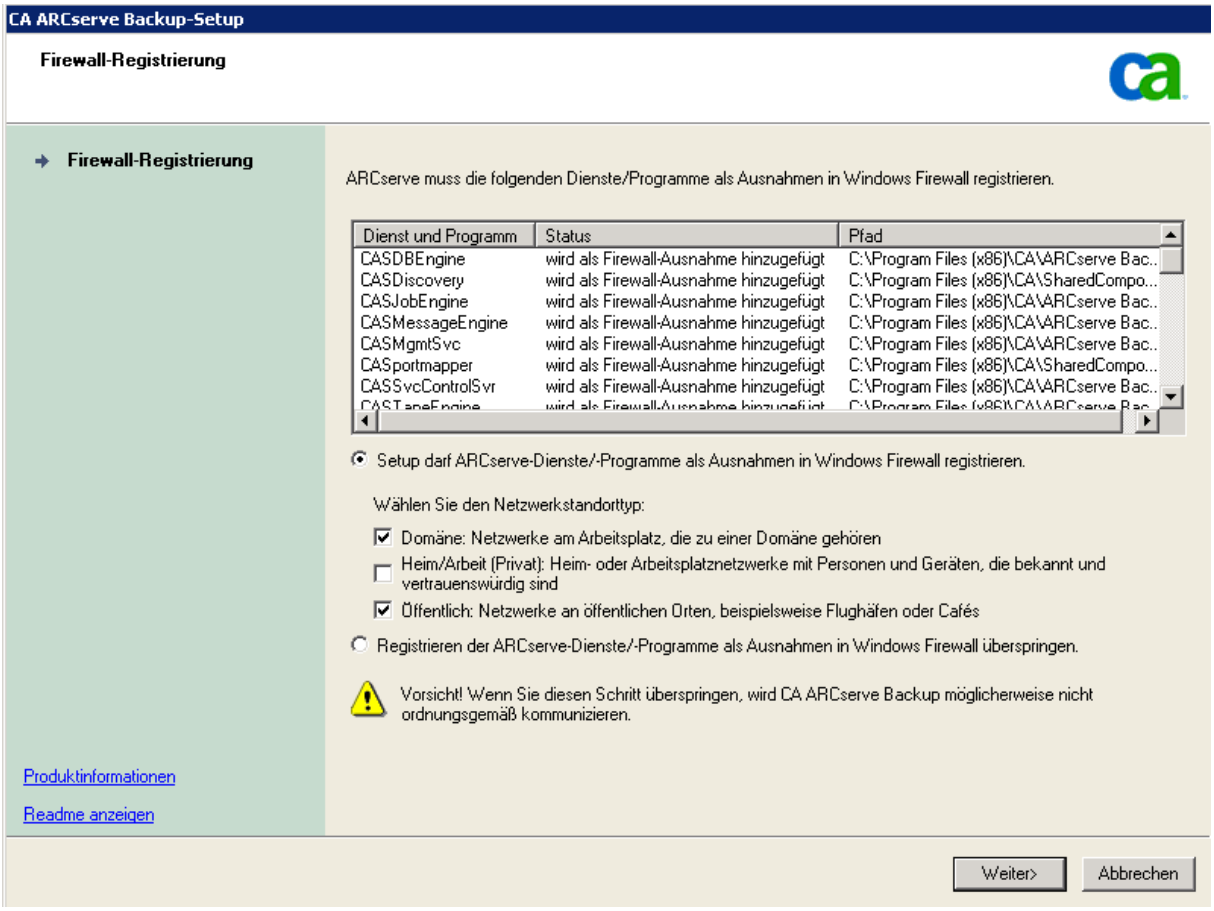
Angabe der Datenbankeinstellungen



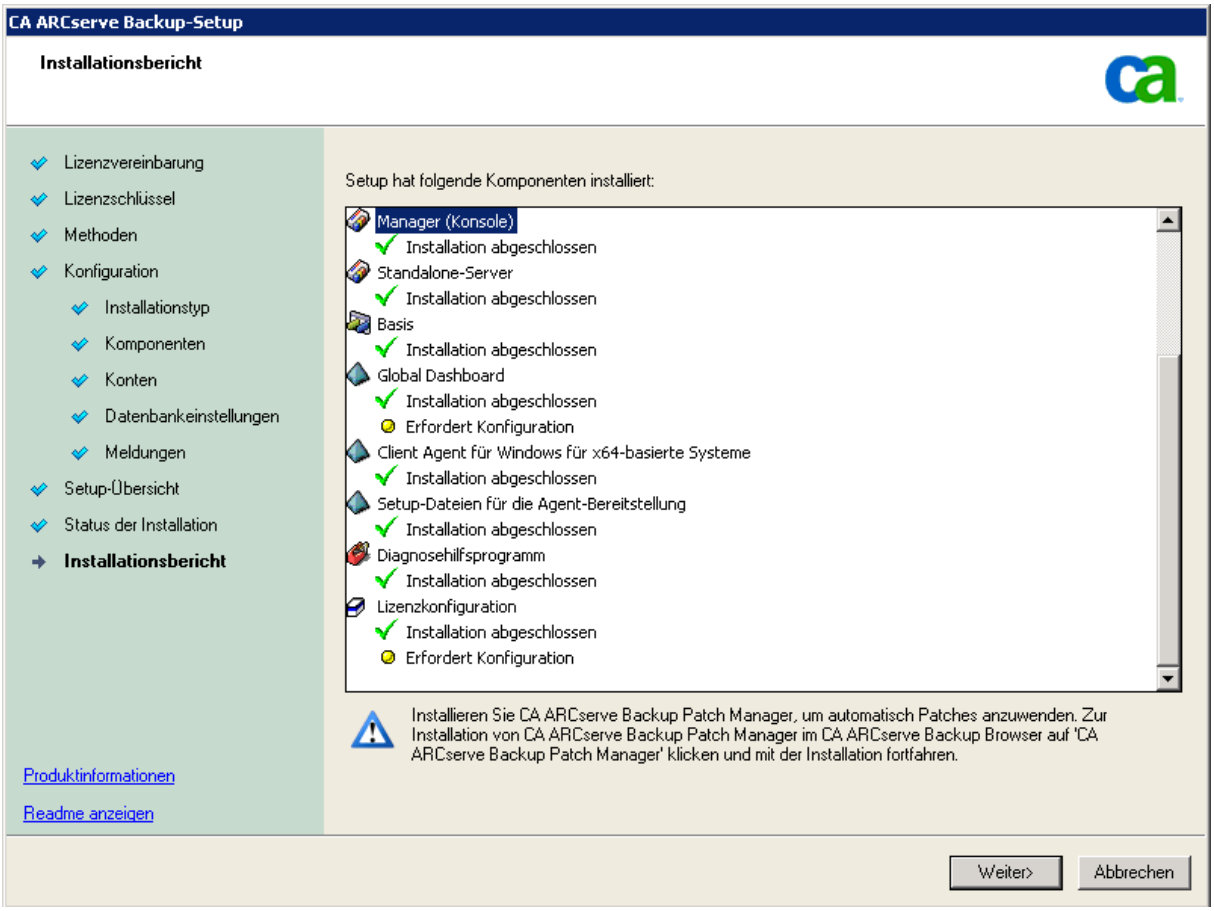

Zusammenfassung



Durchführung der Installation.



Registrierung in der Windows Firewall

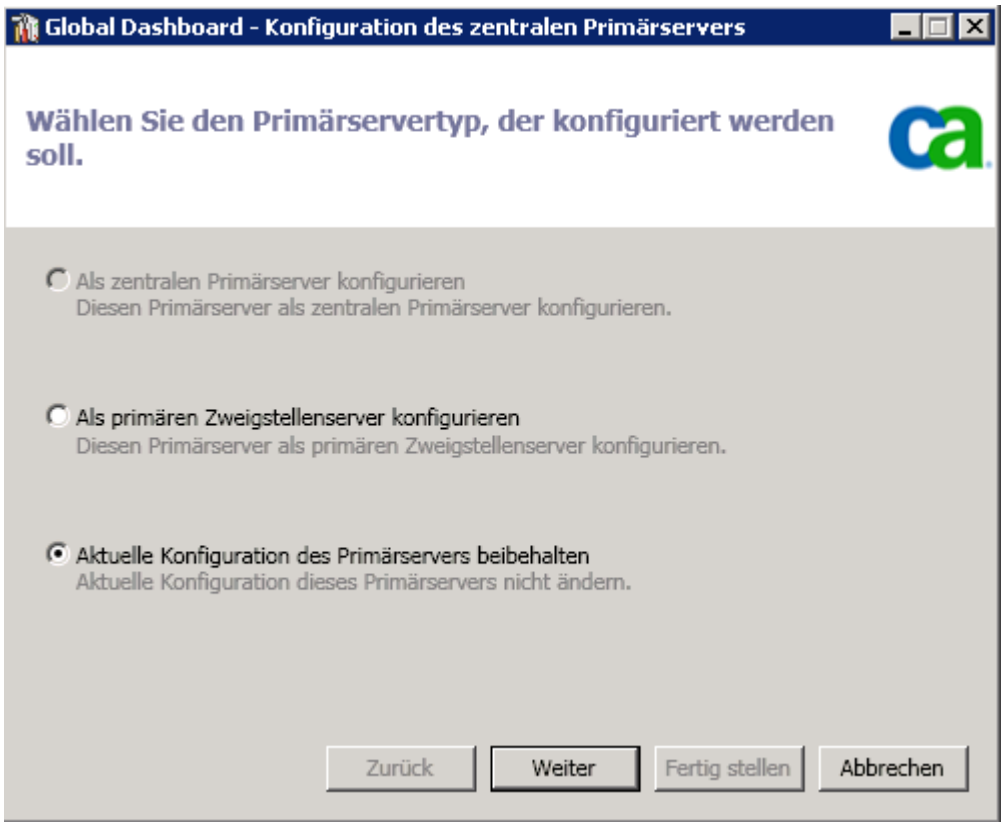



Installationsbericht
(Global Dashboard* und die Lizenzkonfiguration müssen angepasst werden)

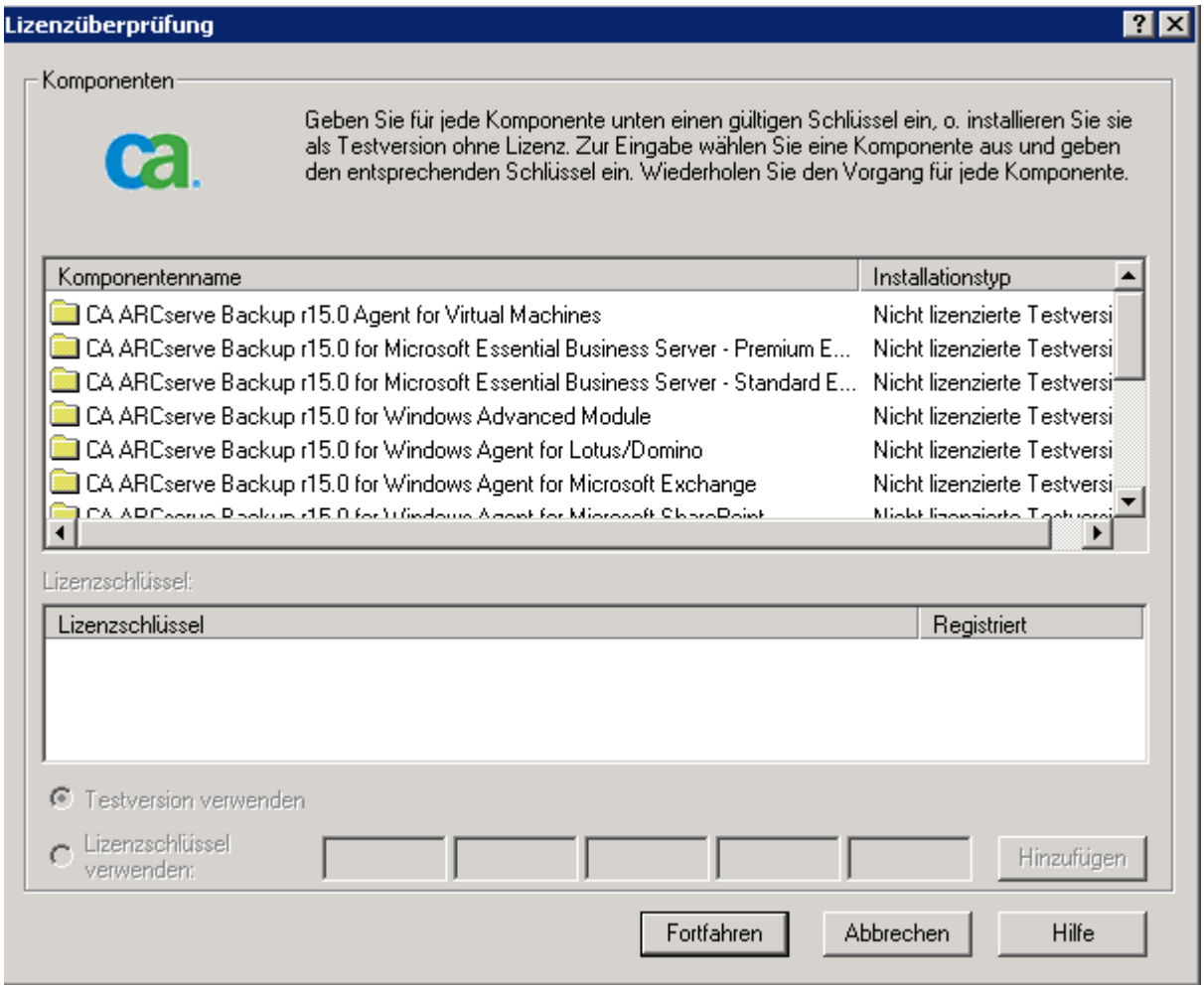
## 6.2 Kurzübersicht Global Dashboard (Optional)

- Informationszentrale zur Sammlung von Sicherungsdaten
- Abrufen von Hardware – und Sicherungsinformationen
- Übersicht von Speicherplatzkapazität
- Benutzerverwaltung für das Ausführen von Backupjobs
- Kennwortverwaltung für die Datensicherungsverschlüsselung

### 6.2.1 Konfiguration des Global Dashboards



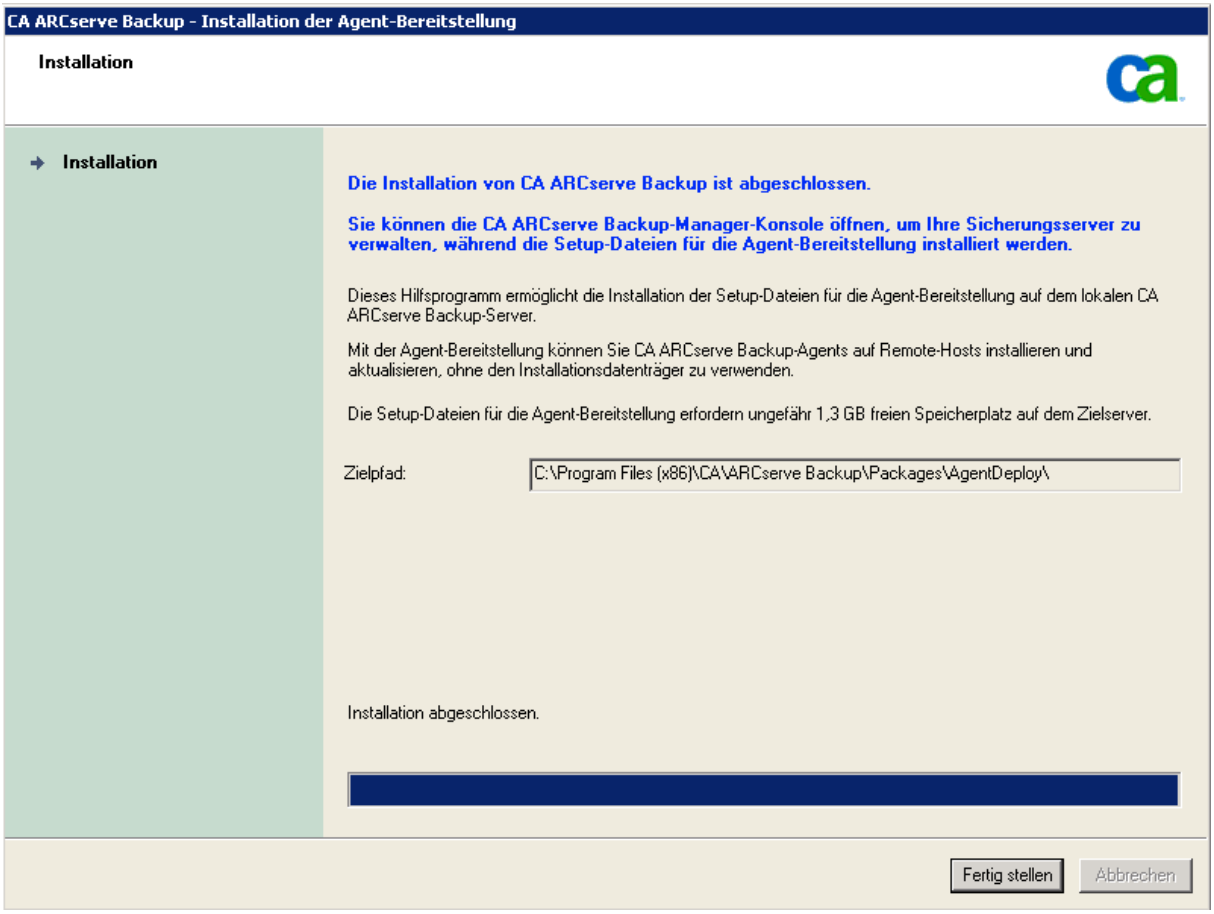
### 6.2.2 Anpassung der Lizenzierung




GGF. sollte die Global Dashboard Funktion hinzugefügt werden. Soll das Global Dashboard nicht verwendet werden, kann dieses während der Installation angegeben werden. Ansonsten wird nur die Backup Manager Konsole verwendet.

**Wenn SQL-Server, Exchange-Server oder zusätzliche virtuelle Maschinen gesichert werden sollen, sind entsprechende Lizenzen einzuspielen. In diesem Workflow wird nur das Basisprodukt behandelt.**

### 6.2.3 Abschluss der Installation




## 6.3 Installation ARCserve Backup r15 auf Server 2003 // R2

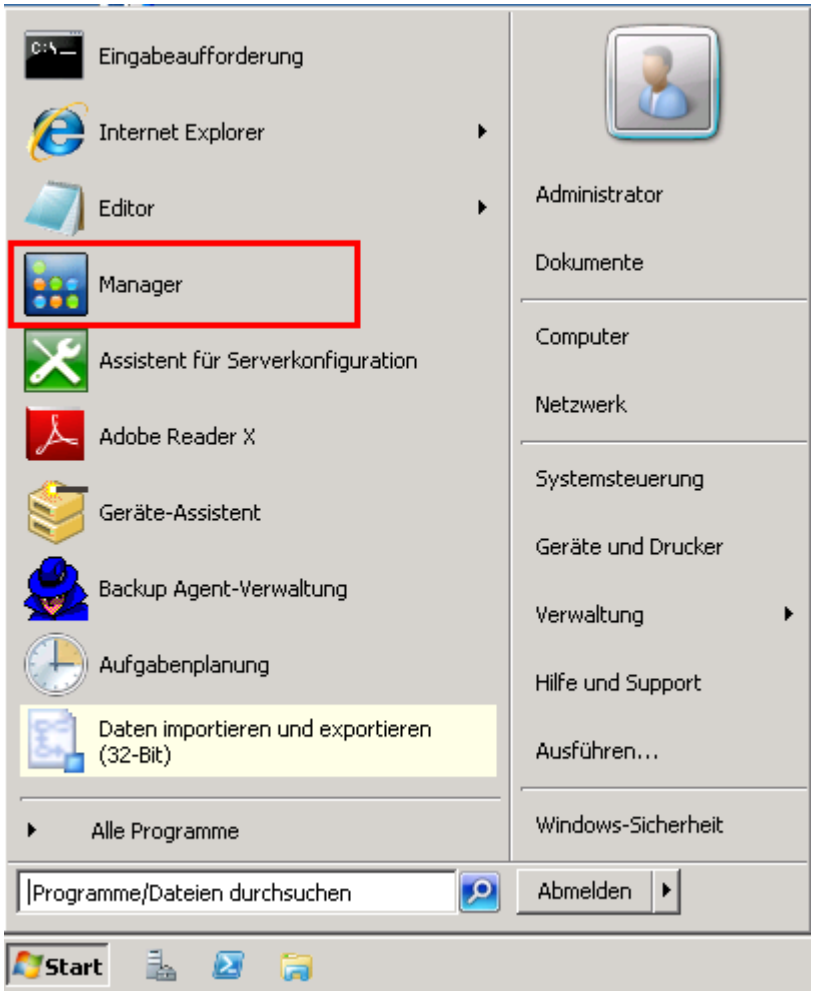
Die Installation unter Server 2003 / R2 unterscheidet sich nicht. Voraussetzung ist ein aktueller Updatestand des Hostsystems.

# 7. Einrichtung von ARCserve Backup r15

## 7.1 Einrichtung CA ARCserve Backup r15 unter Server 2008 / R2 (USB Laufwerk)

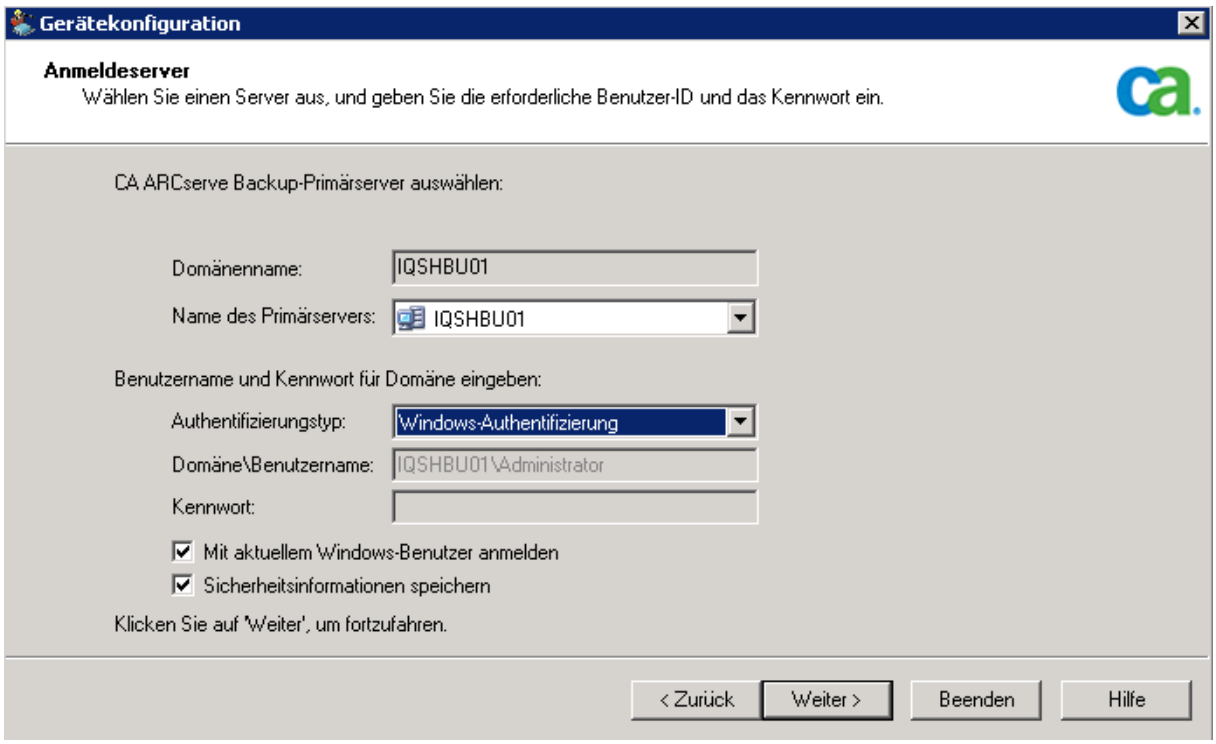
### 7.1.1 Ersteinrichtung der Datensicherungslaufwerke (USB)

Für die Einrichtung der Laufwerke, werden in diesem Workflow, Laufwerke für die normale Sicherung sowie Laufwerke für die Sicherung mit Deduplizierung eingerichtet.

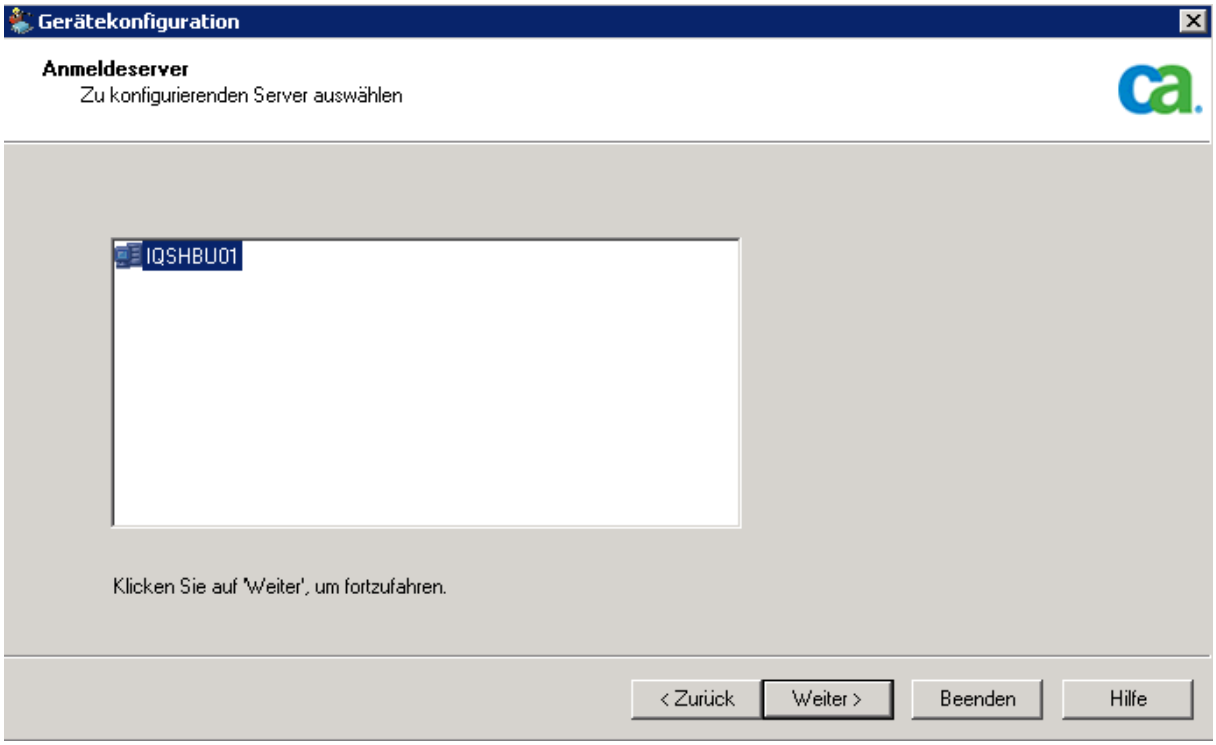


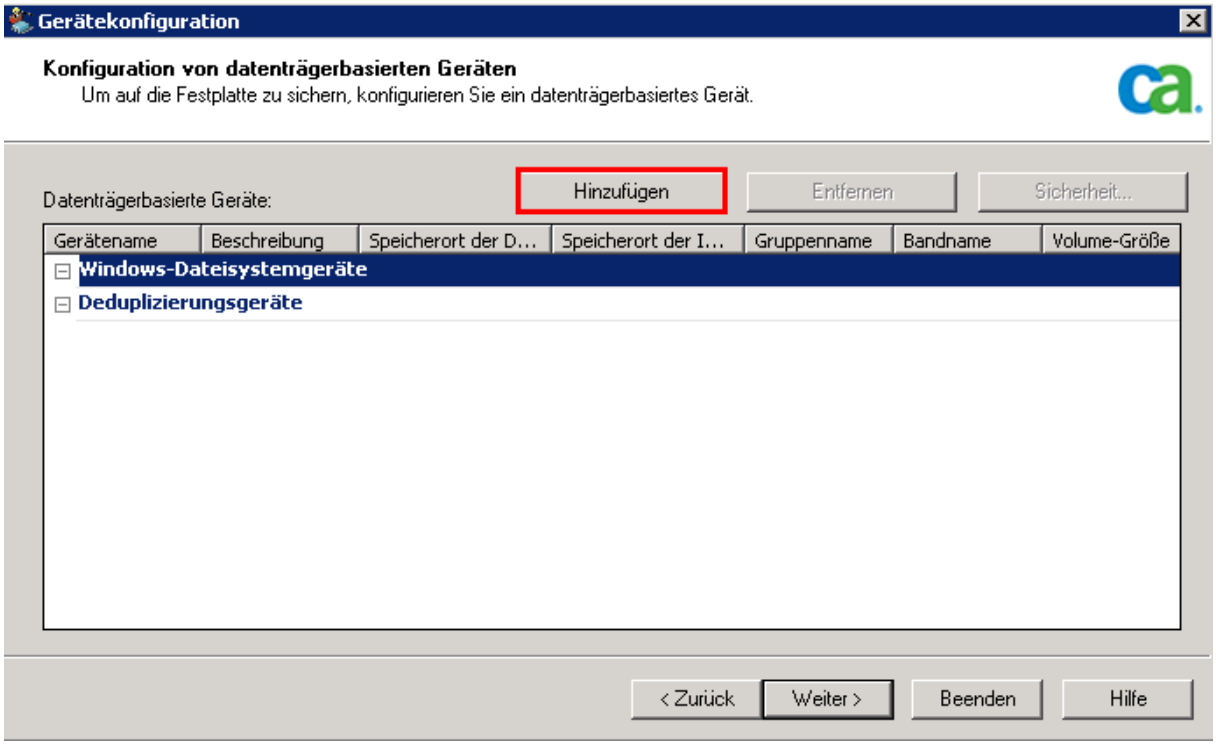

Erster Start des Backup Managers


Start der Sicherungseinrichtung (Einrichtung der Geräte / des Gerätes)

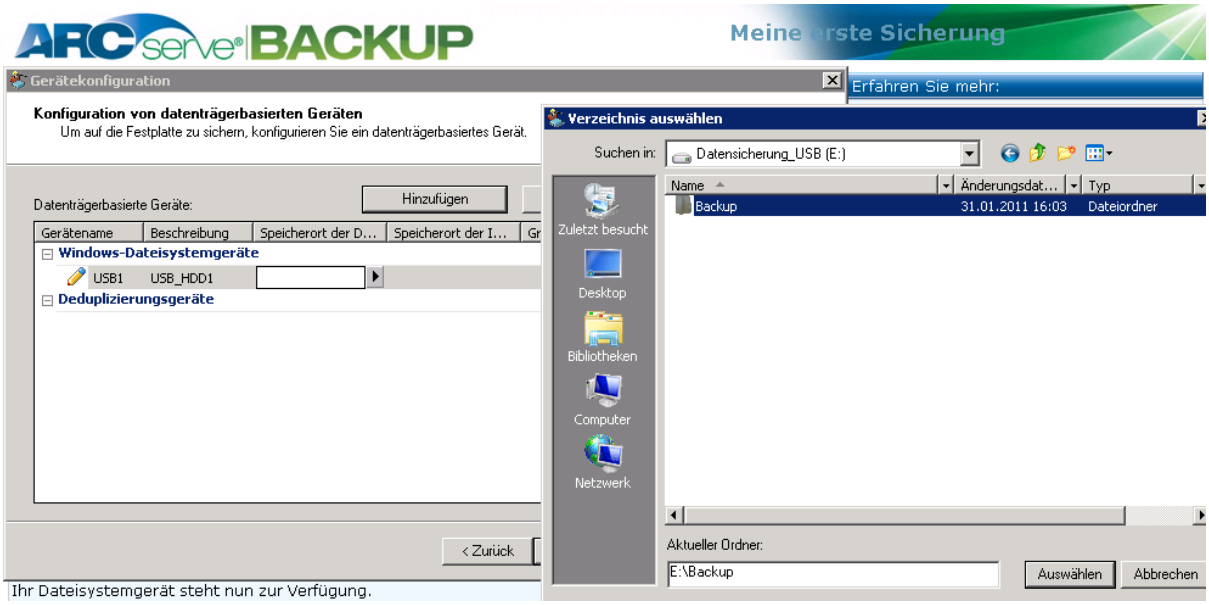



Festlegend der Anmeldeinformation

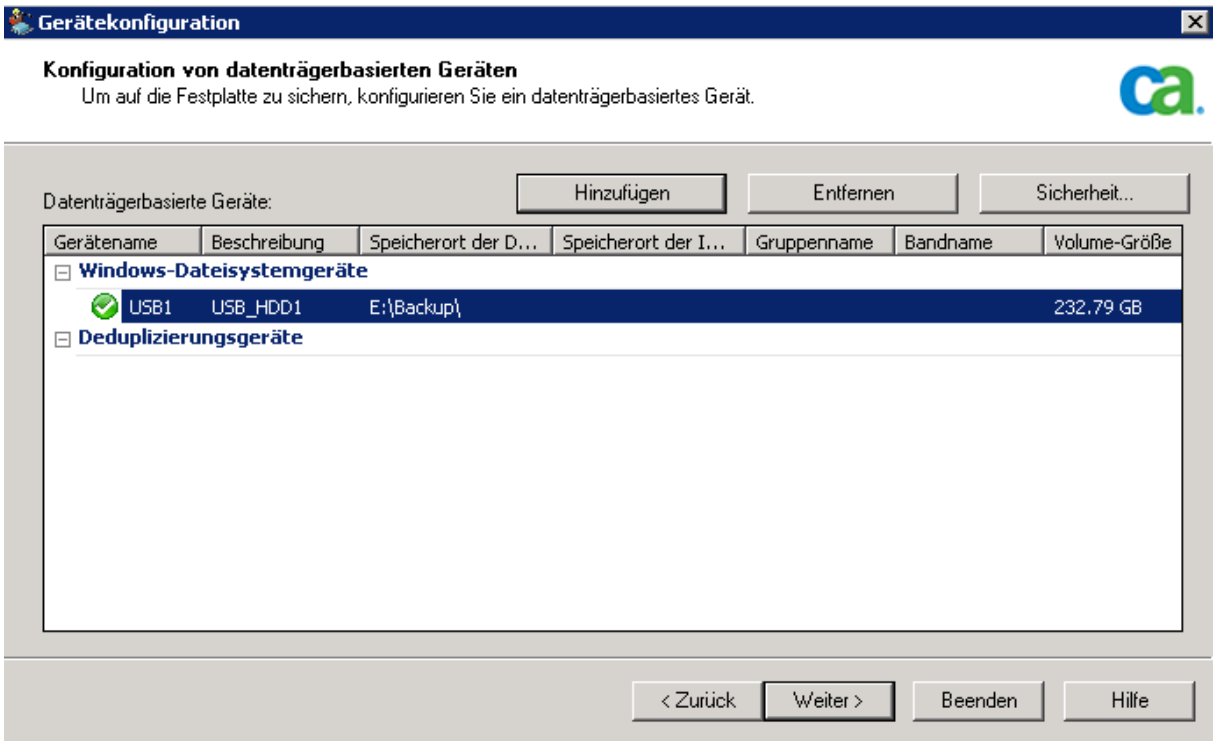


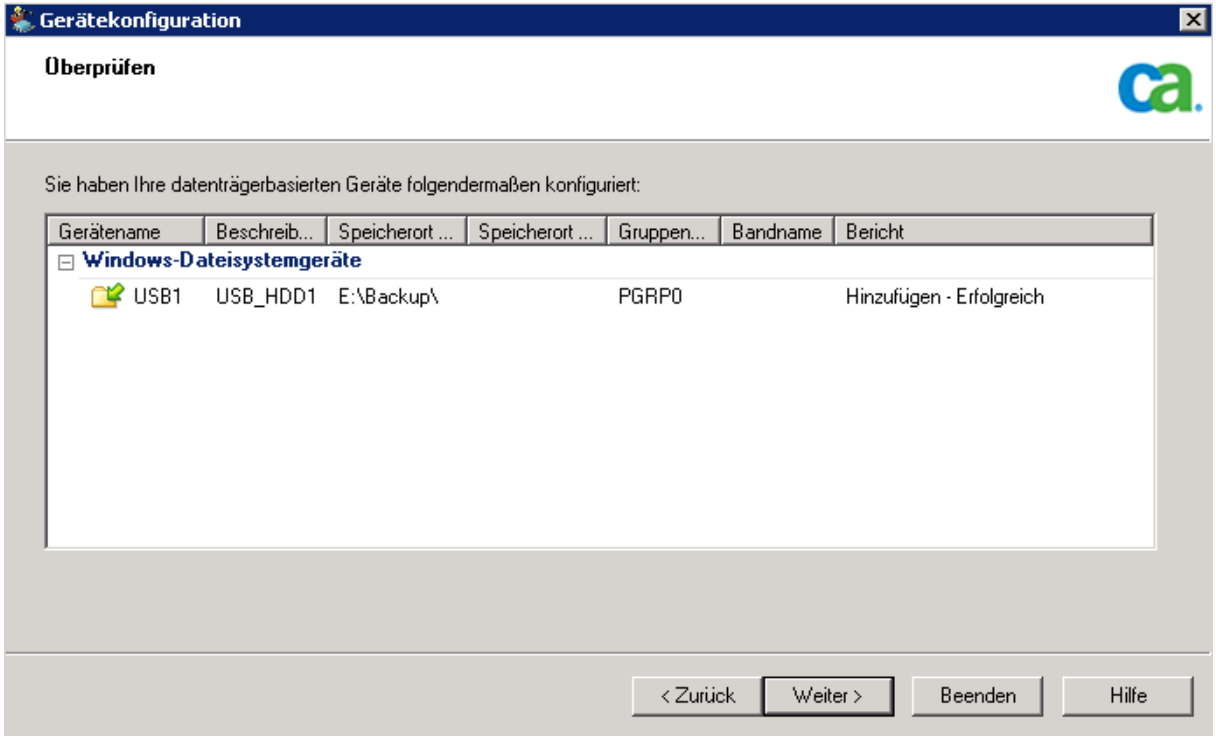



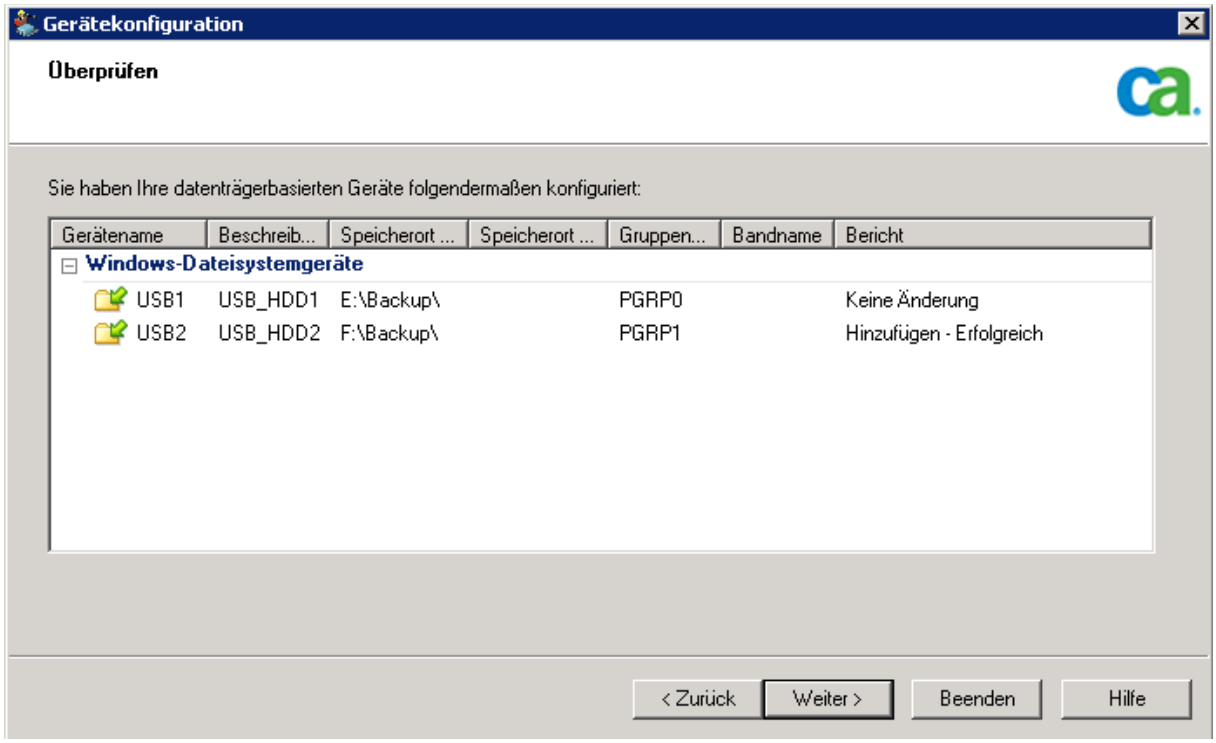

Ersteinrichtung des Datensicherungsgerätes



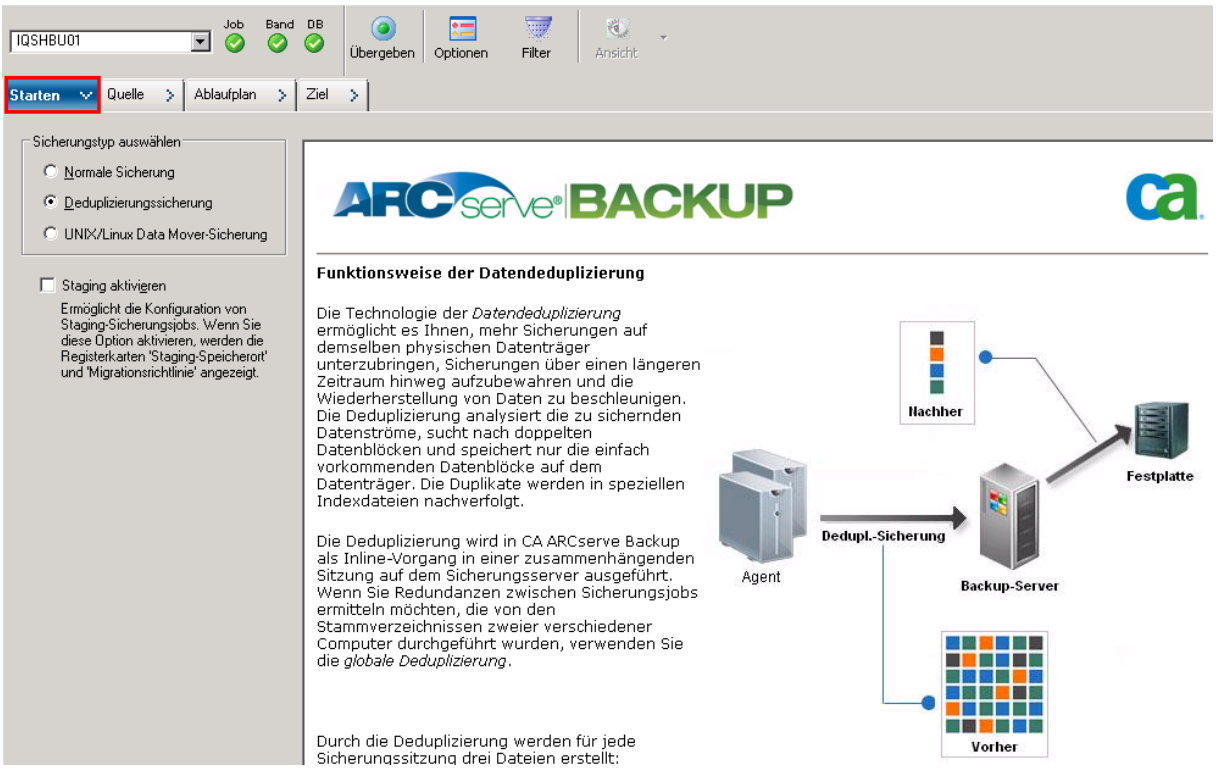

Beschreibung und Auswahl des Speicherortes auf der USB Festplatte.





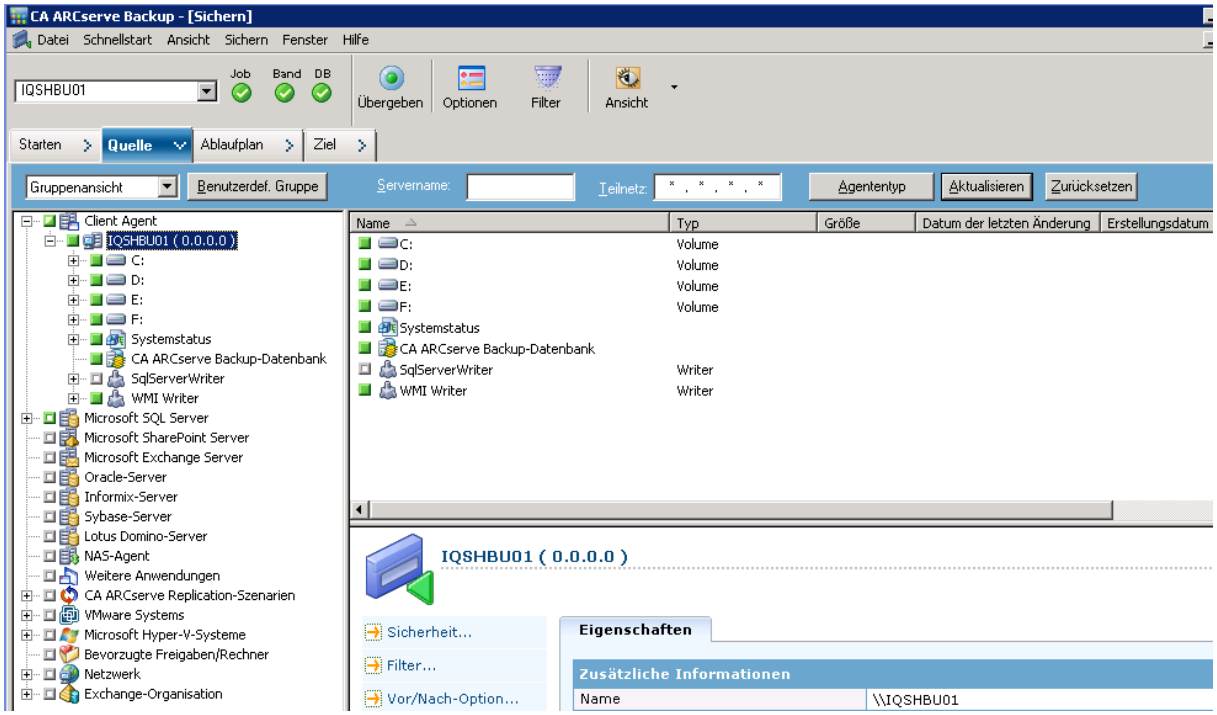




Hinzufügen einer weiteren USB Festplatte. Die Schritte sind indentisch.

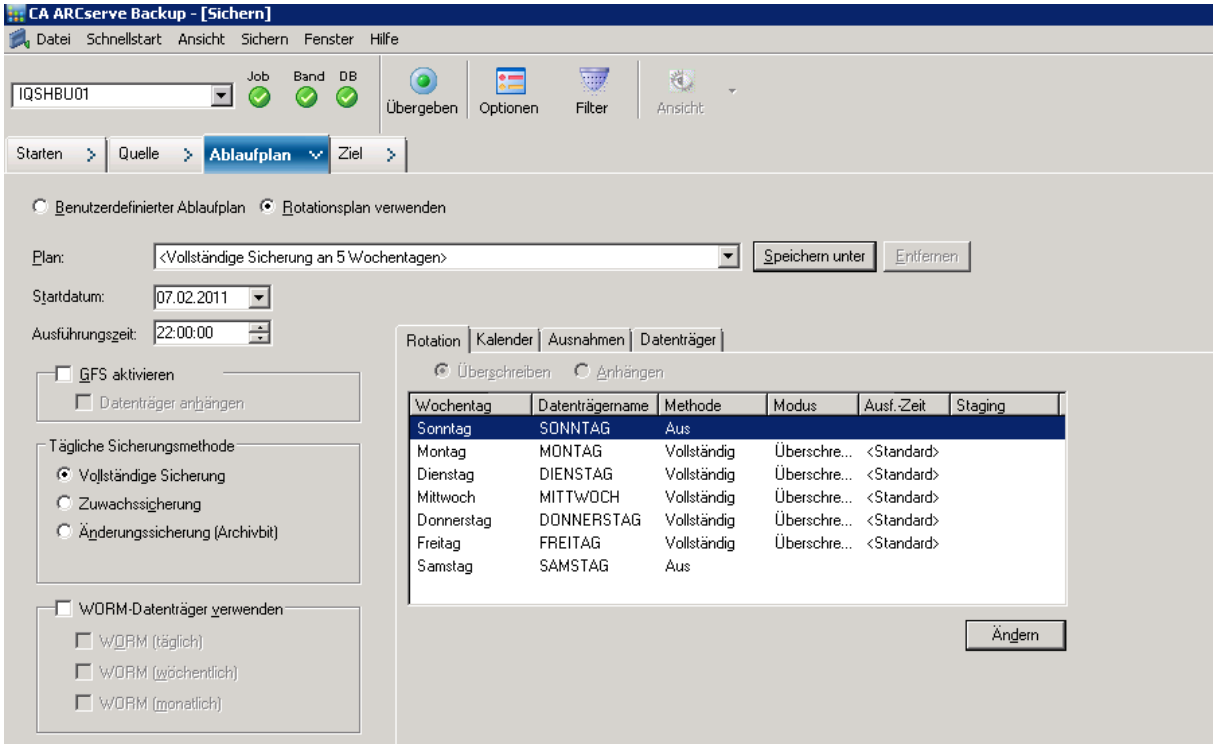


Auswahl der Datendeduplizierung* (Eine Optimierungsmöglichkeit für die Schulen)

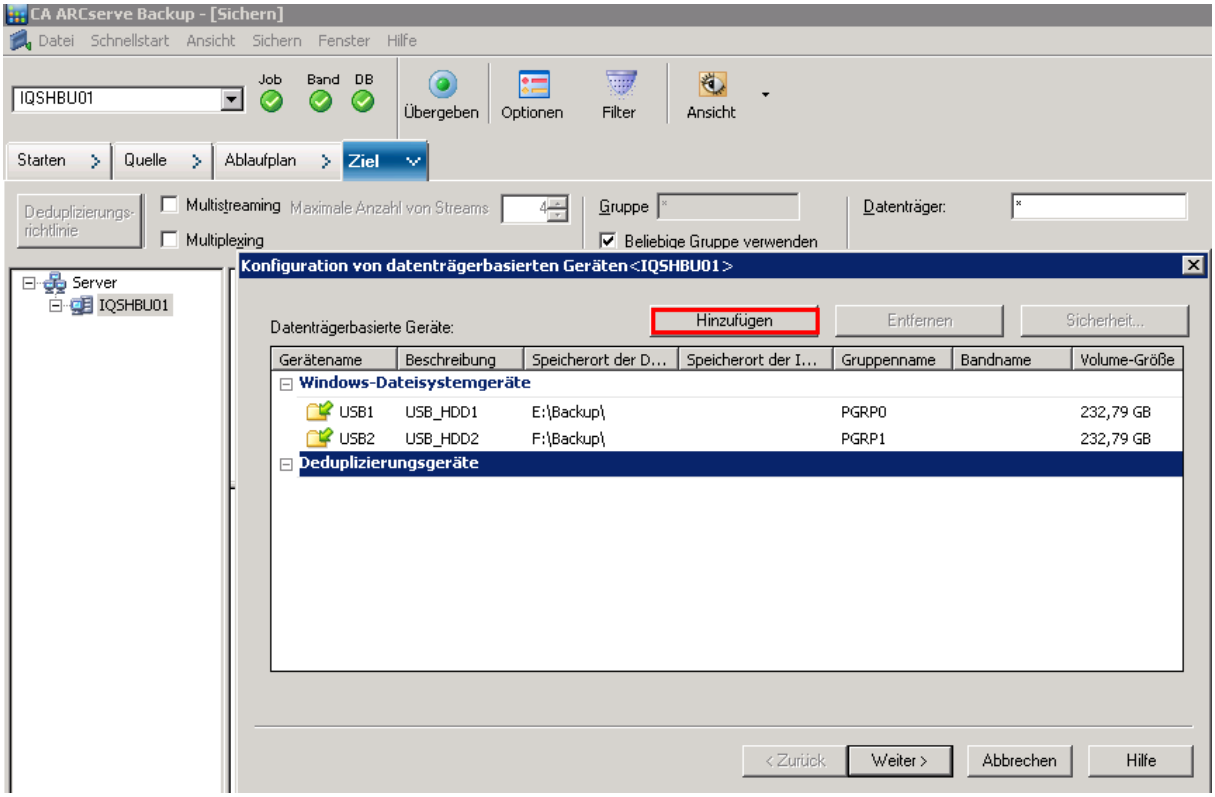
*Deduplizierungssicherung
- Mehrere Sicherungen auf demselben physischen Datenträger
- Sicherungen über einen längeren Zeitraum vorhalten
- Beschleunigung der Wiederherstellung



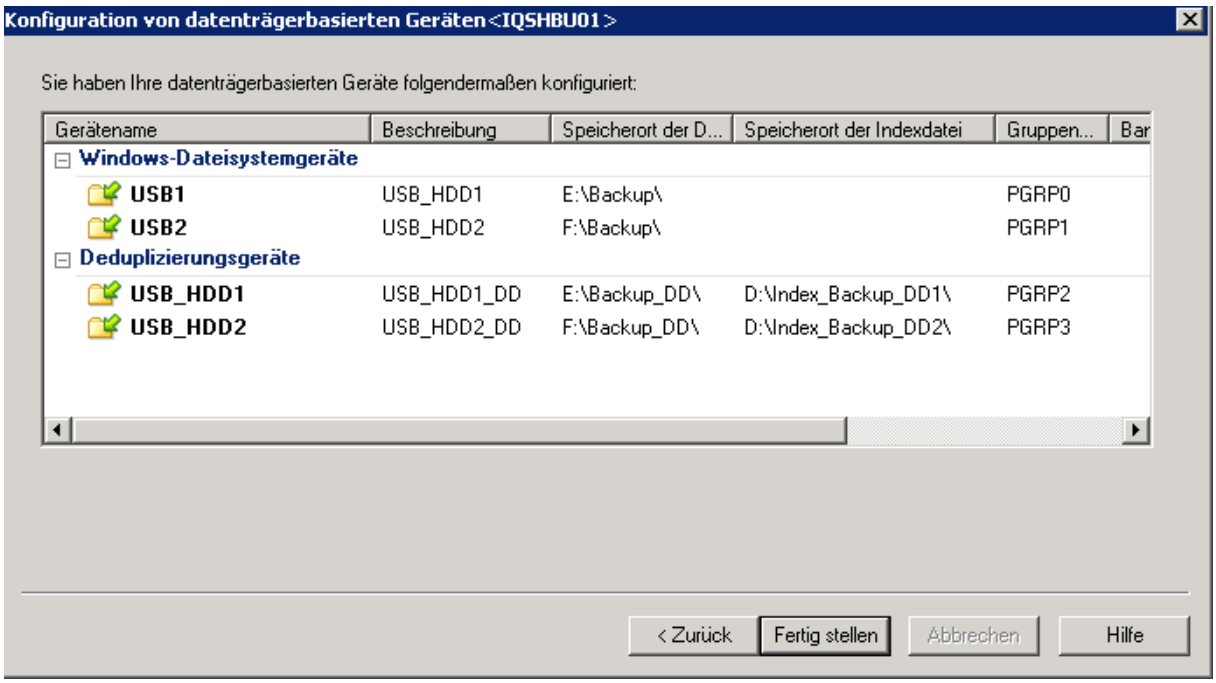

Individuelle Auswahl der zu sichernden Dateien. (Beispiel: Gesamtsicherung)



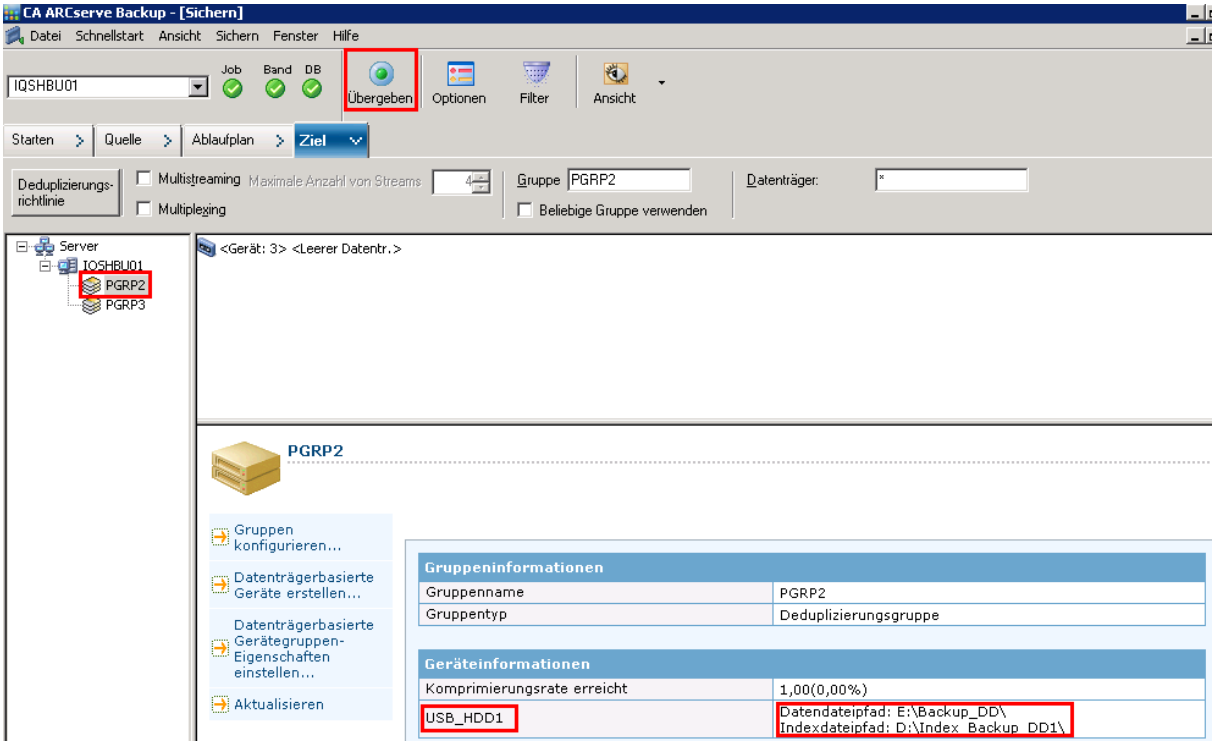

Erstellen eines Rotations- Sicherungszeitplans. (Auswahl der Vollständigen Sicherung)



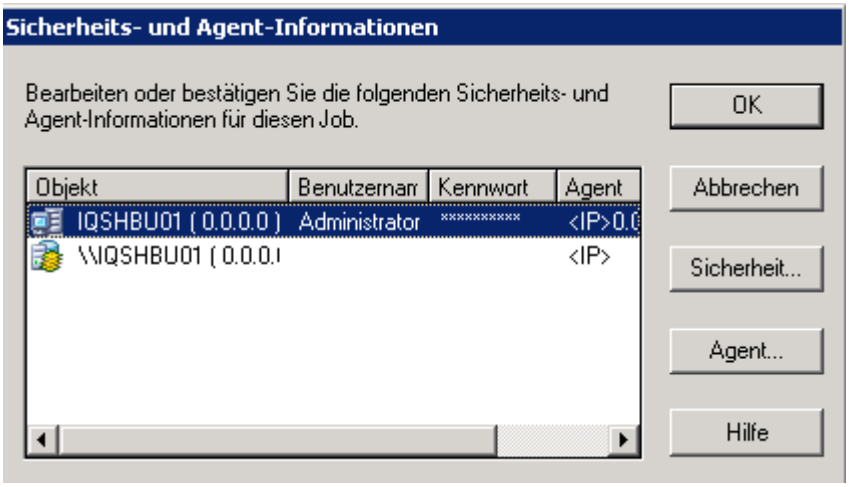

Hinzufügen der Deduplizierungsgeräte



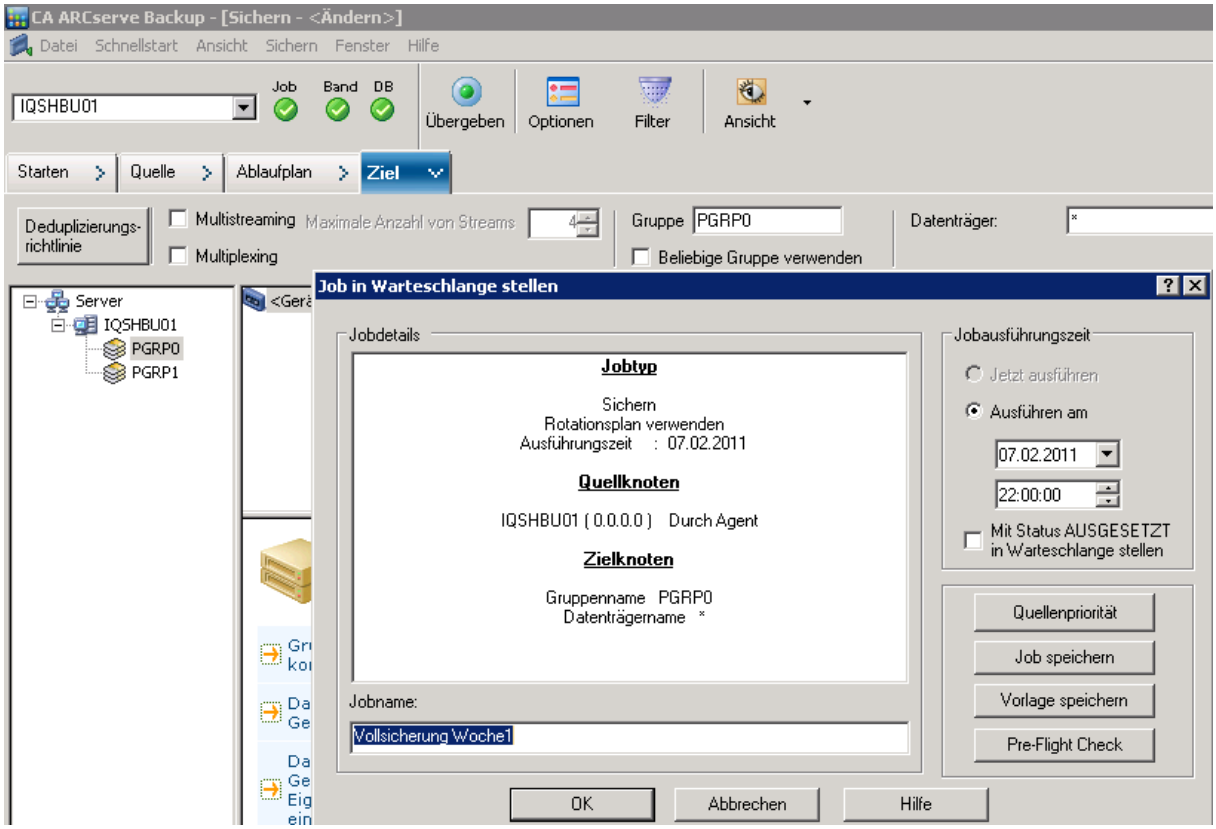
Zusammenfassung der erstellten Deduplizierungsorte. Die gewählten Ordner werden im Vorwege auf den USB Festplatten angelegt. **(Siehe 4.2.1)**



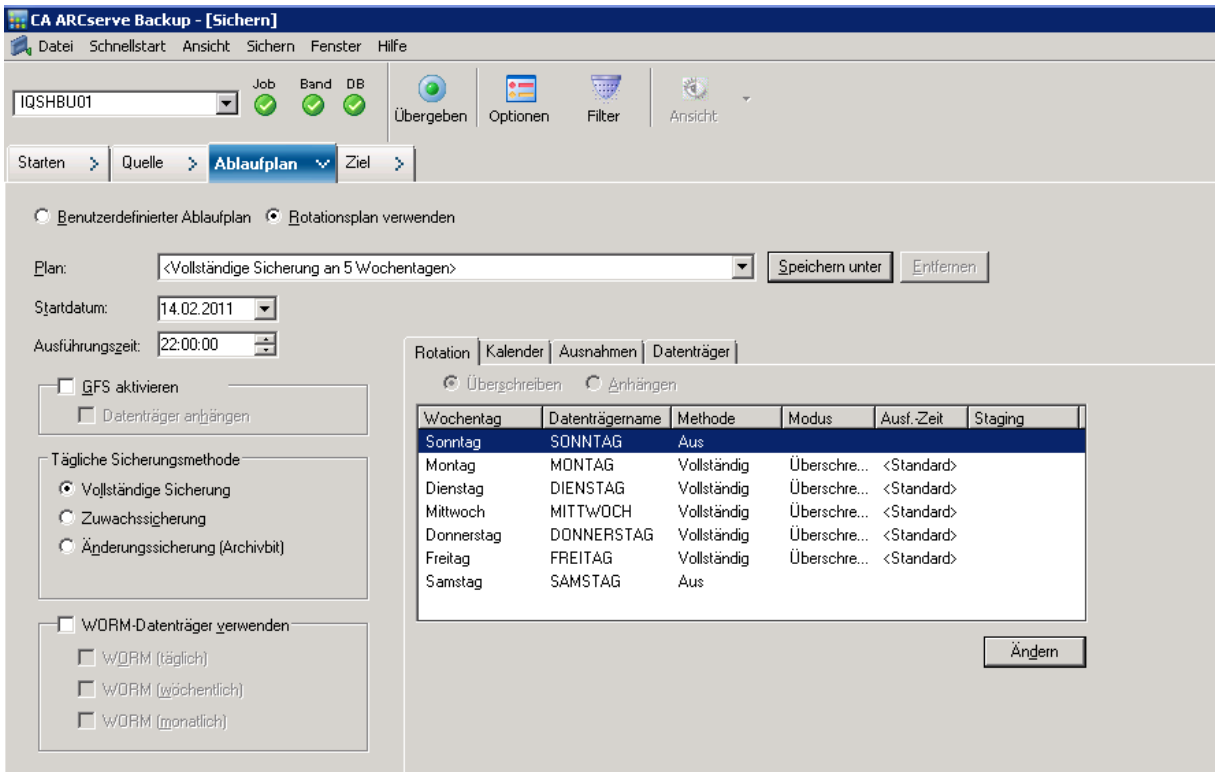
Übergabe des ersten Sicherungsjobs auf angelegter USB_HDD1



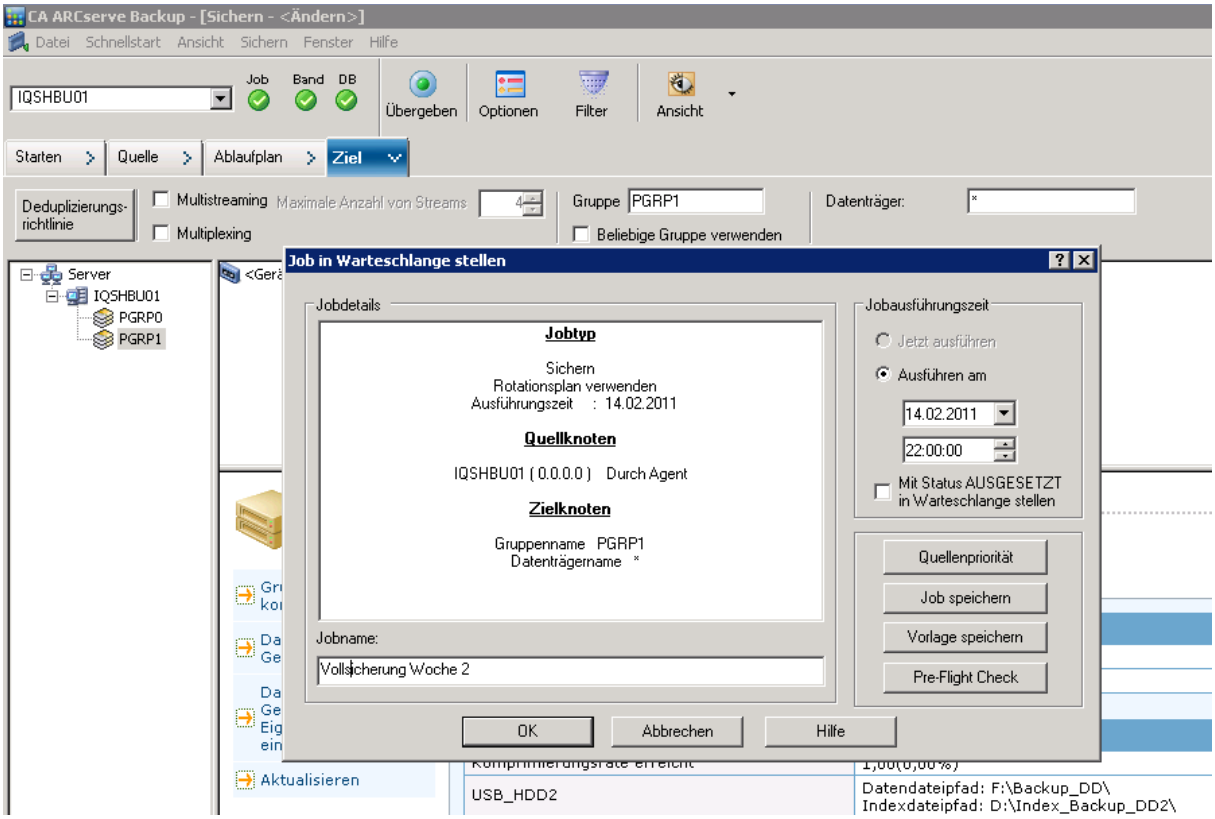
Auswahl des Sicherungsoperators.



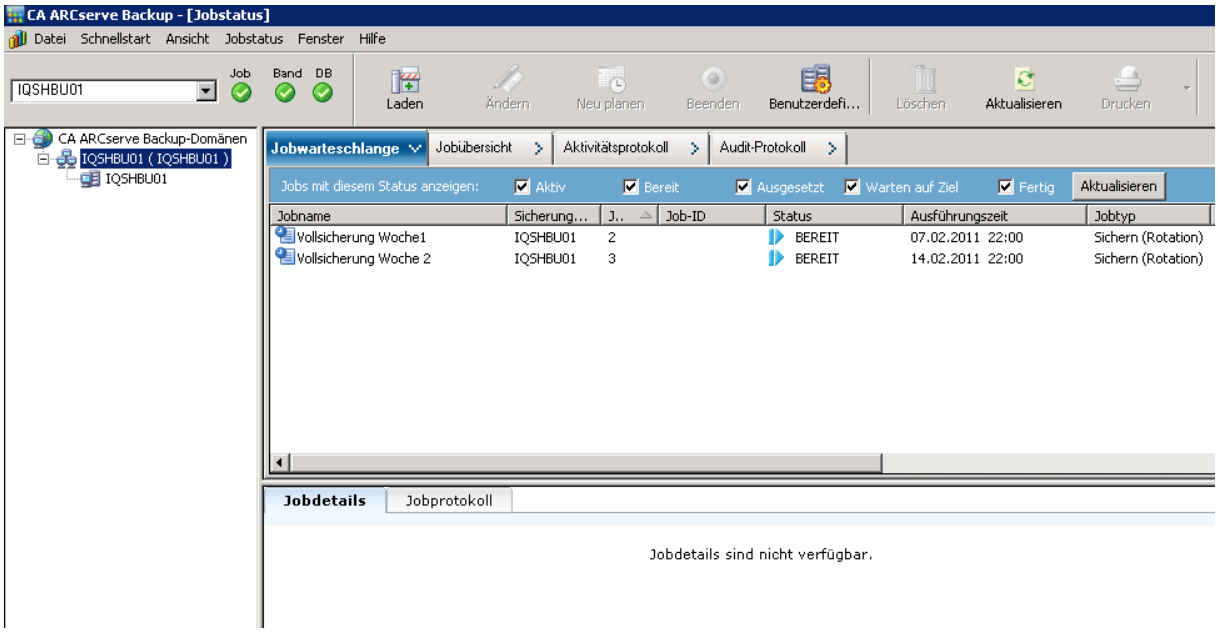

Sicherungszeitplan übergeben und in Warteschlange stellen.



Zurück zum Ablaufplan, zur Einrichtung der zweiten USB Festplatte für Woche2.

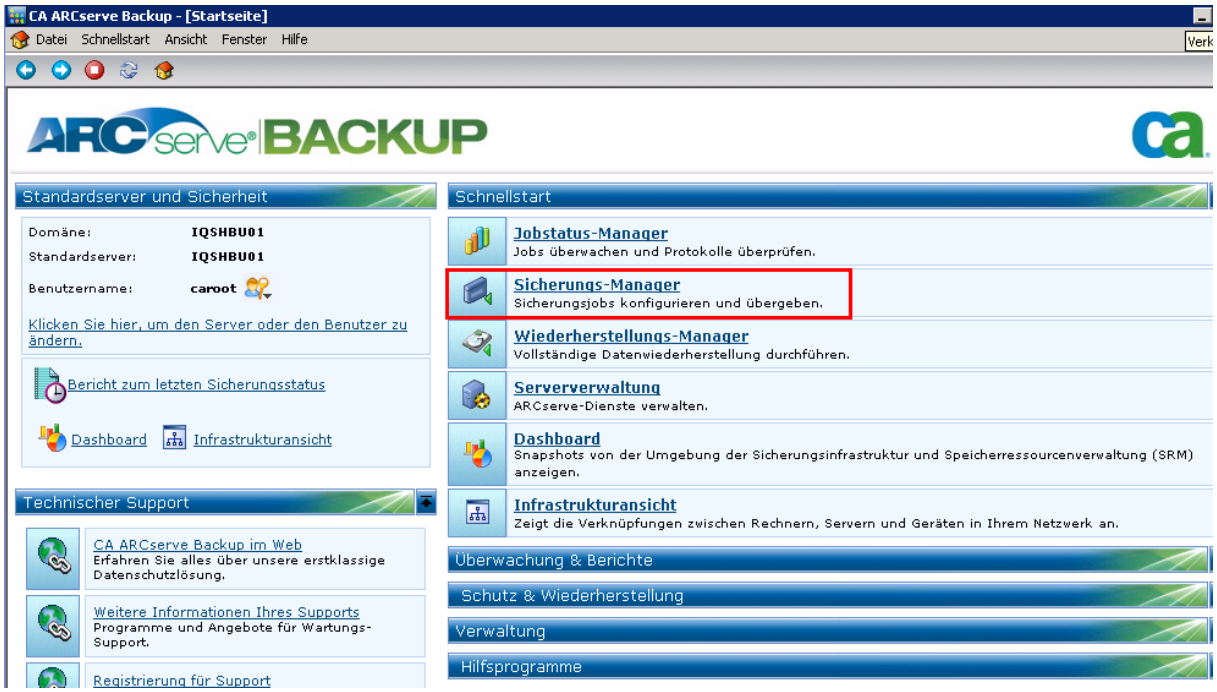


Übergabe an Festplatte 2

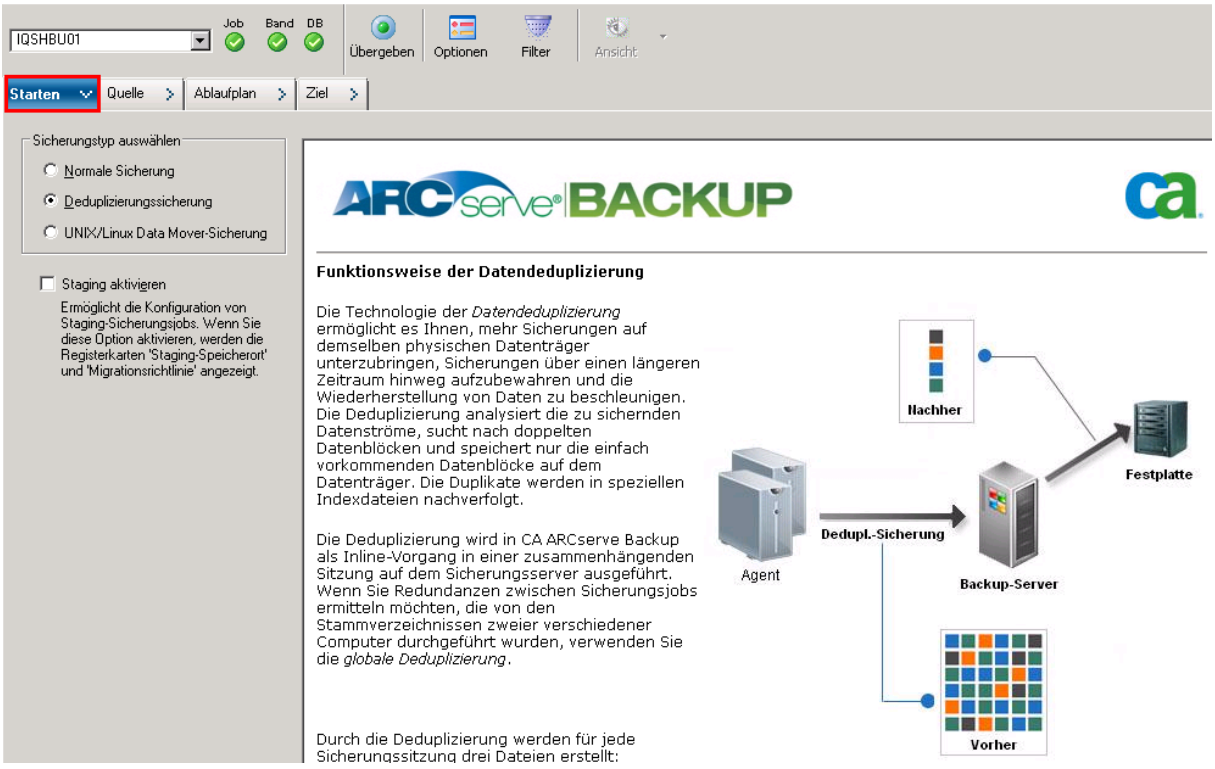



Übersicht der angelegten Sicherungen.

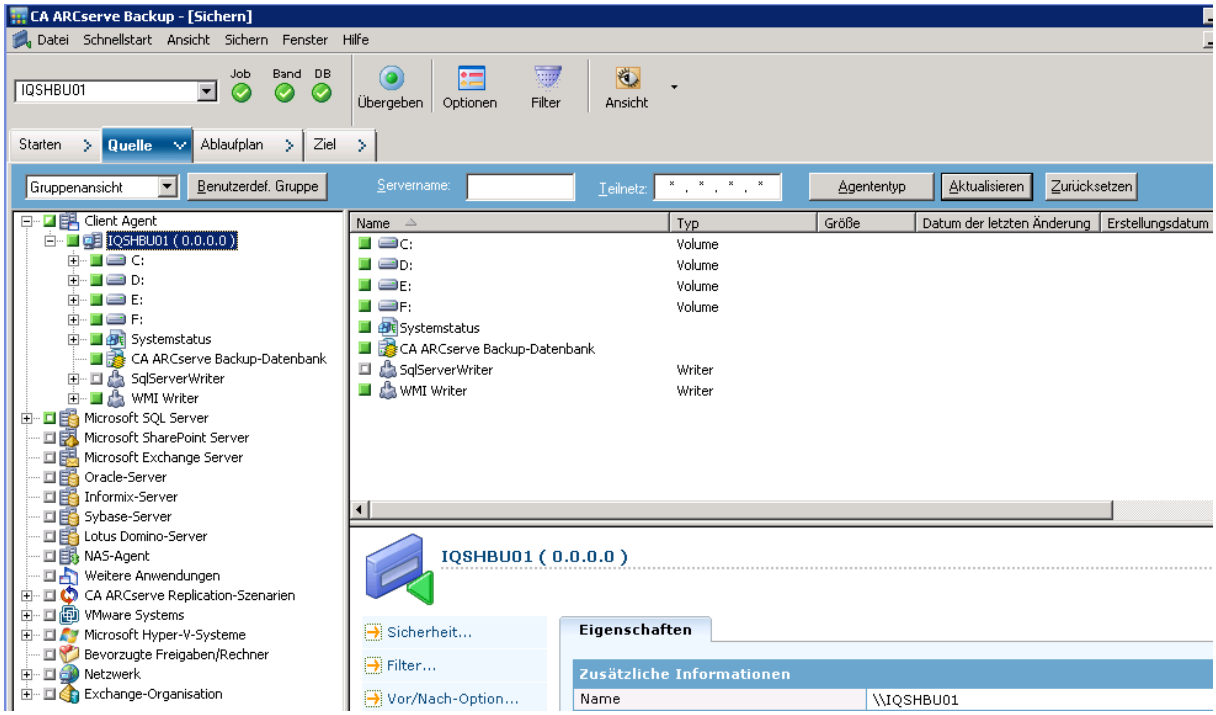
## 7.2 Einrichtung CA ARCserve Backup r15 unter Server 2008 / R2 (NAS Laufwerk)



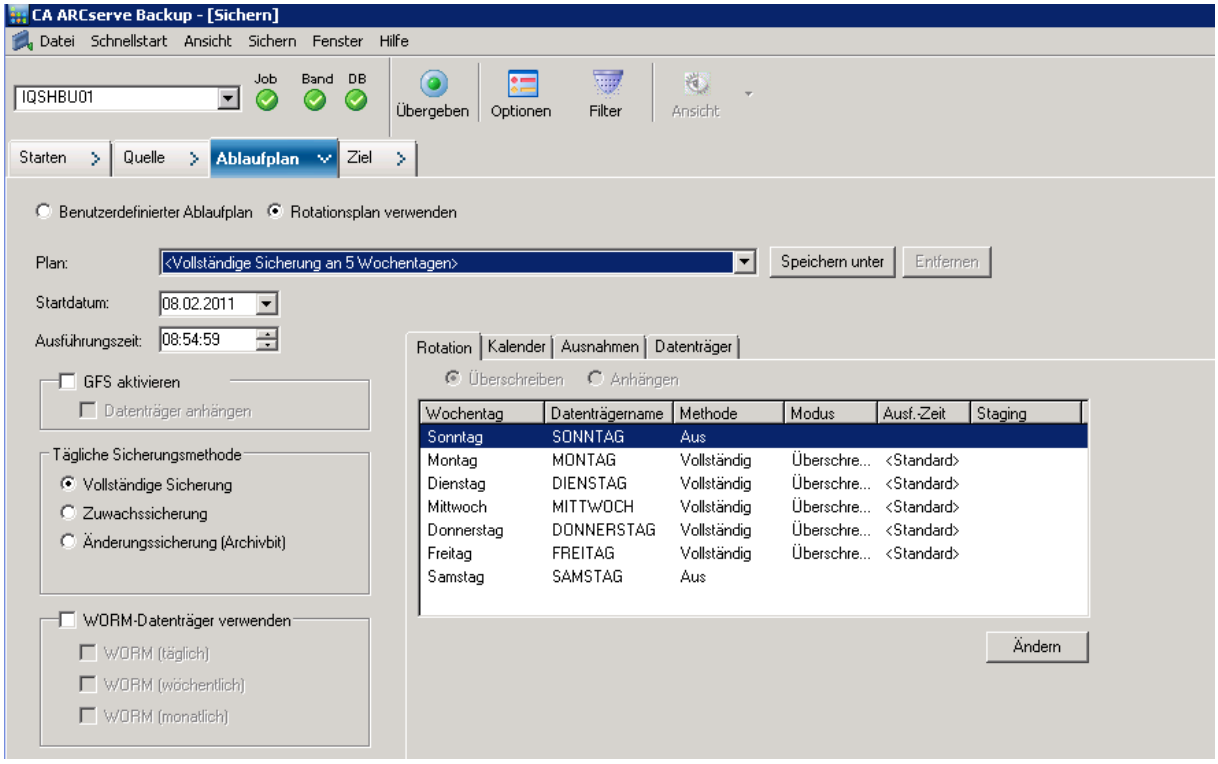

Auswahl des Sicherungsmanagers



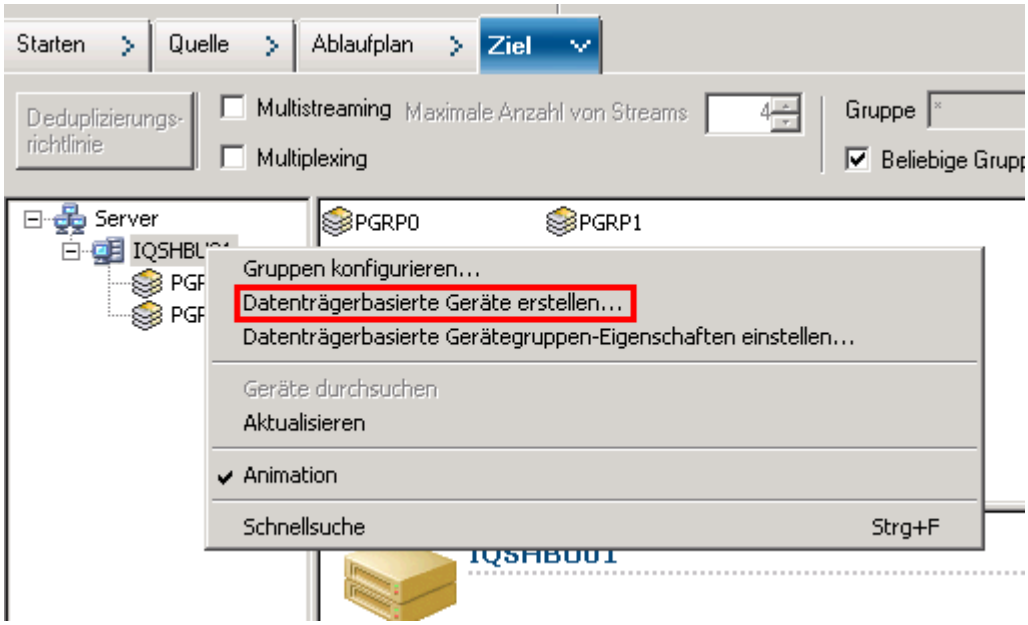

Erneute Wahl der Deduplizierungssicherung



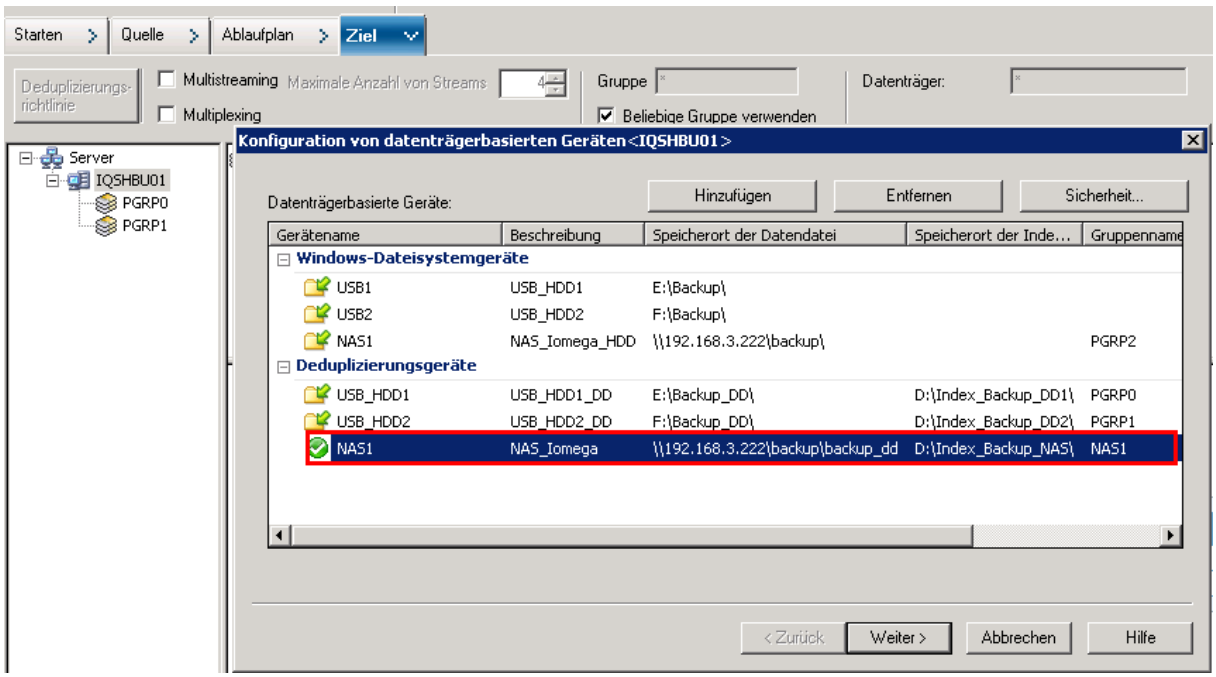

Auswahl der zu Sichernden Dateien (Hier Vollsicherung)



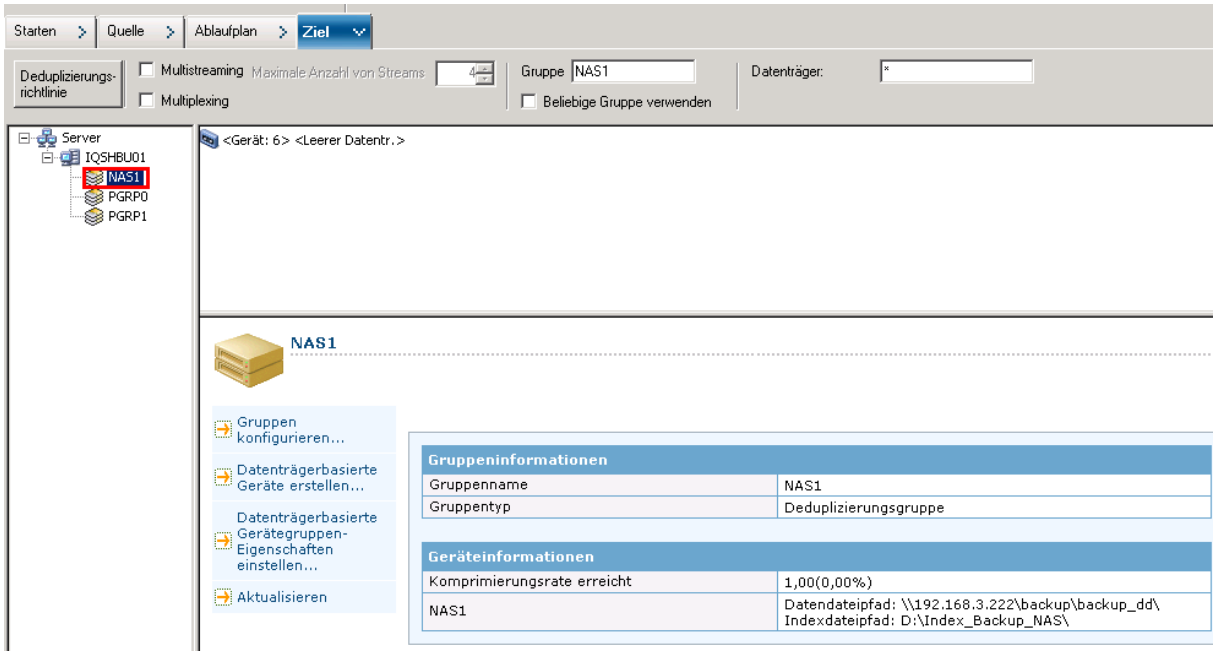

Ablaufplan bestimmen. (Vollständige Sicherung, alle 5 Tage)



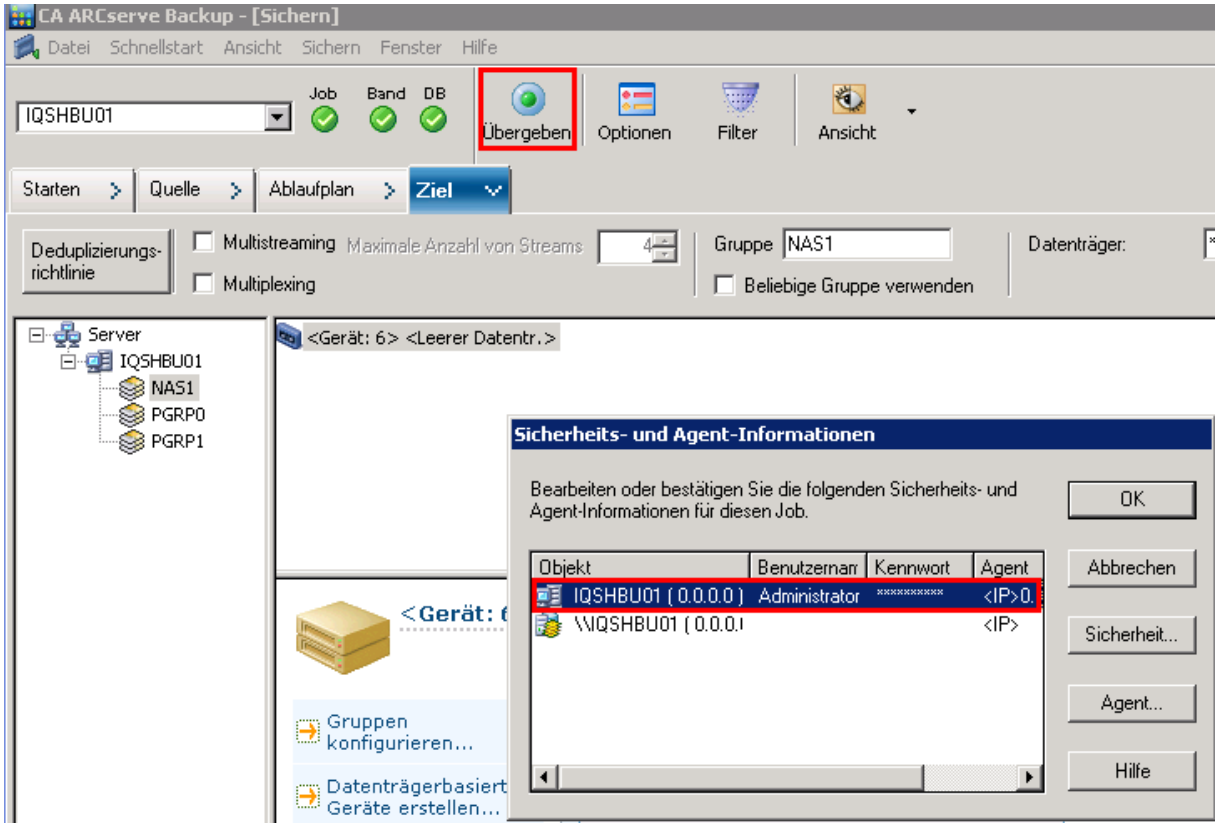

Zielbestimmung: Um das NAS-Laufwerk als Ziel zu bestimmen, und zu deduplizieren, ist es erforderlich ein neues Datenträgerbasiertes Gerät zu erstellen.



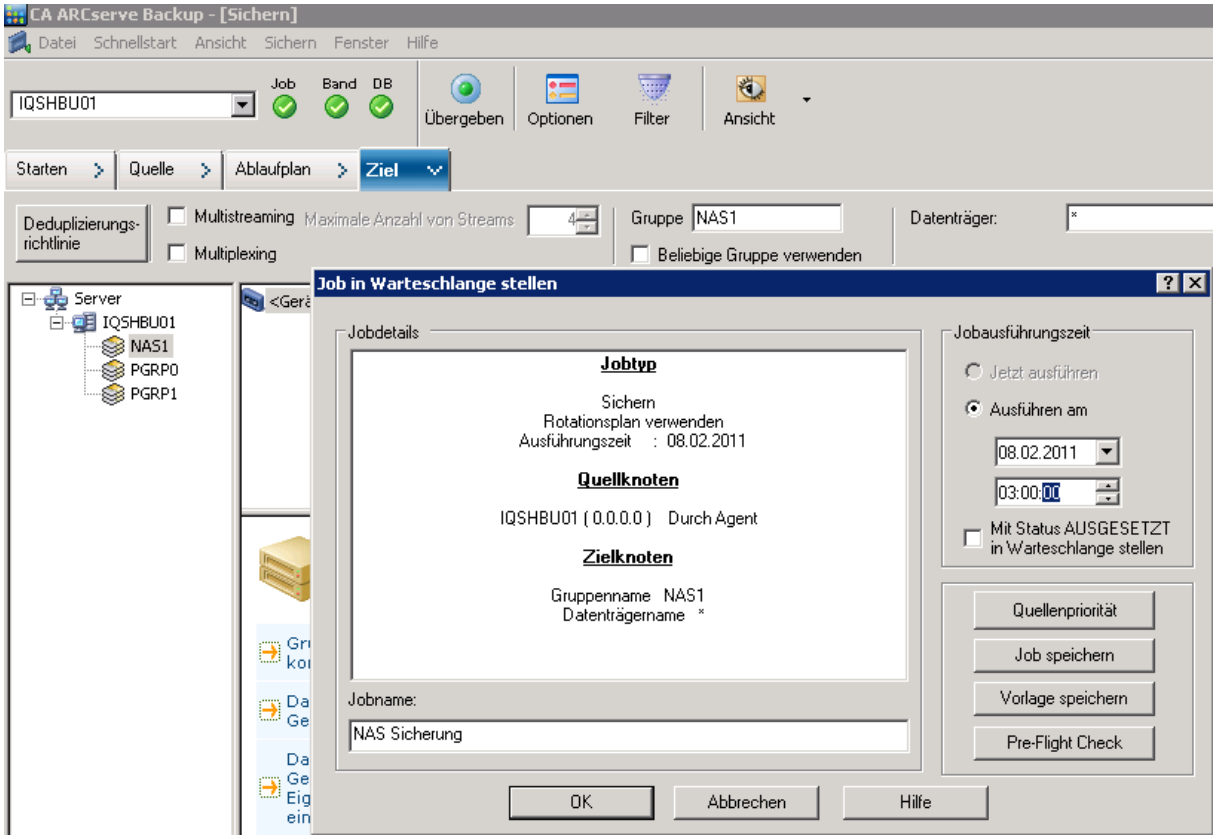

Erstellter neuer Pfad inkl. Indexpfad für die Sicherung auf dem NAS.



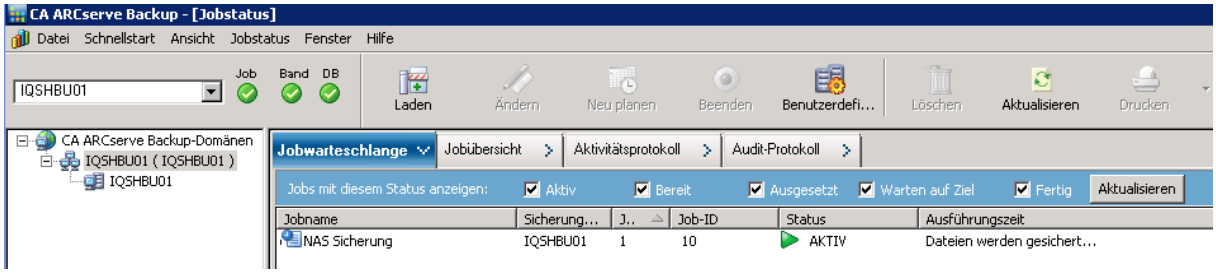

Ein neu erstelltes Datenträger basiertes Gerät.



Übergabe des Datensicherungsjobs inkl. Angabe des Sicheungsoperators.




Den Sicherungsjob in Warteschlange stellen, inkl. Angabe der Jobausführungszeit.




Übergebender Job.

## 7.3 Einrichtung CA ARCserve Backup r15 unter Server 2003/ R2 (USB Laufwerk)

Die Installation und die Handhabung zwischen Server 2008 / R2 und Server 2003 / R2 unterscheiden sich nicht.

## 7.4 Einrichtung CA ARCserve Backup r15 unter Server 2003/ R2 (NAS Laufwerk)

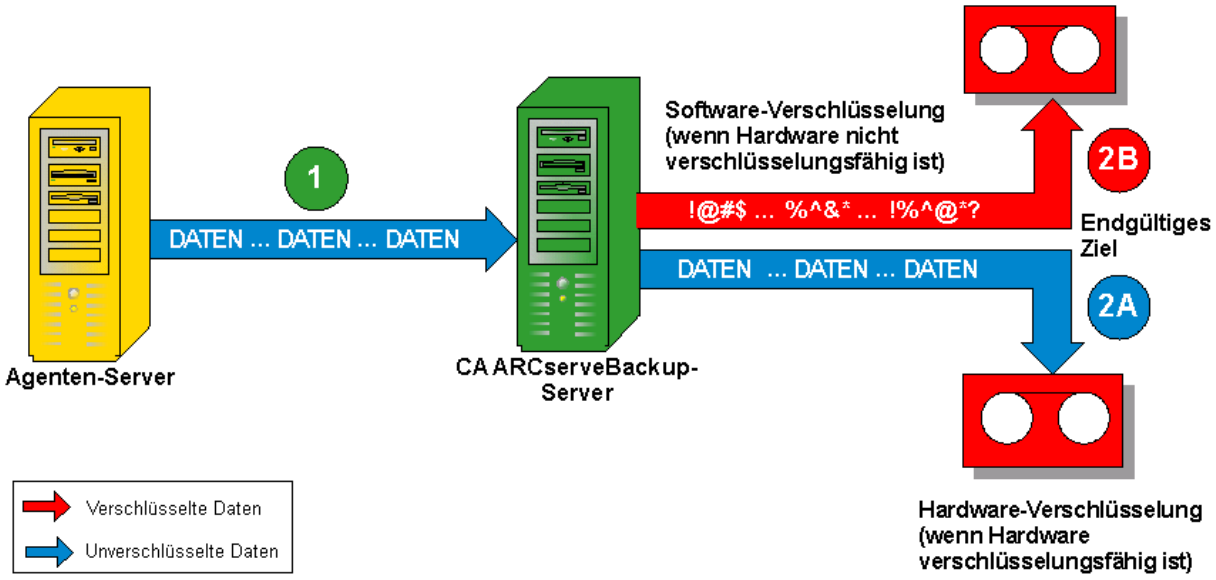
Die Installation und die Handhabung zwischen Server 2008 / R2 und Server 2003 / R2 unterscheiden sich nicht.

# 8. Verschlüsselung der Daten während der Sicherungen mit CA ARCserve

Daten können während des Sicherungsvorgangs auf dem CA ARCserve Backup-Server verschlüsselt werden. Bei dieser Methode werden unverschlüsselte Daten vom Agent-Server auf den CA ARCserve Backup-Server übertragen. CA ARCserve Backup ermittelt dann, ob der Zieldatenträger für die Hardware-Verschlüsselung geeignet ist. Ist dies der Fall, werden die unverschlüsselten Daten an den endgültigen Zieldatenträger gesendet und dort verschlüsselt. Dies ist die bevorzugte und standardmäßige Methode, da sie schneller ist und keine Auswirkungen auf das Sicherungszeitfenster hat.

Der in CA ARCserve Backup verwendete Verschlüsselungsalgorithmus ist AES256*
*( Advanced Encryption Standard)

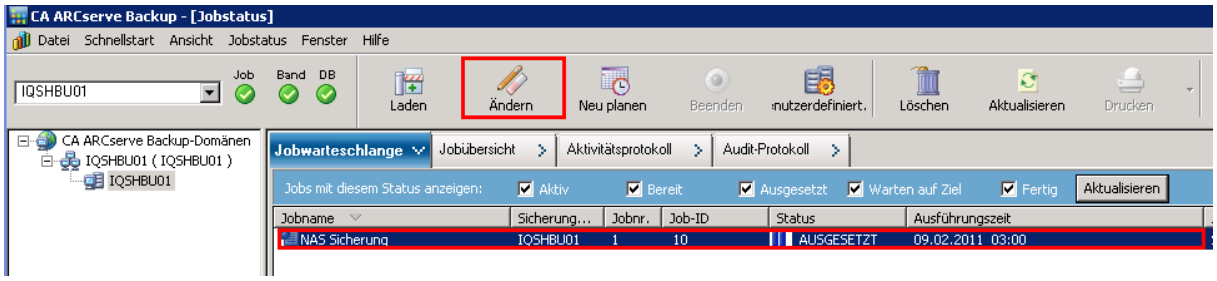
Wenn CA ARCserve Backup feststellt, dass der endgültige Zieldatenträger keine Hardware-Verschlüsselung unterstützt, verwendet CA ARCserve Backup Software-Verschlüsselung zum Verschlüsseln der Daten vor deren Übertragung an den endgültigen Zieldatenträger.




## 8.1 Festlegen der Verschlüsselungsfunktion

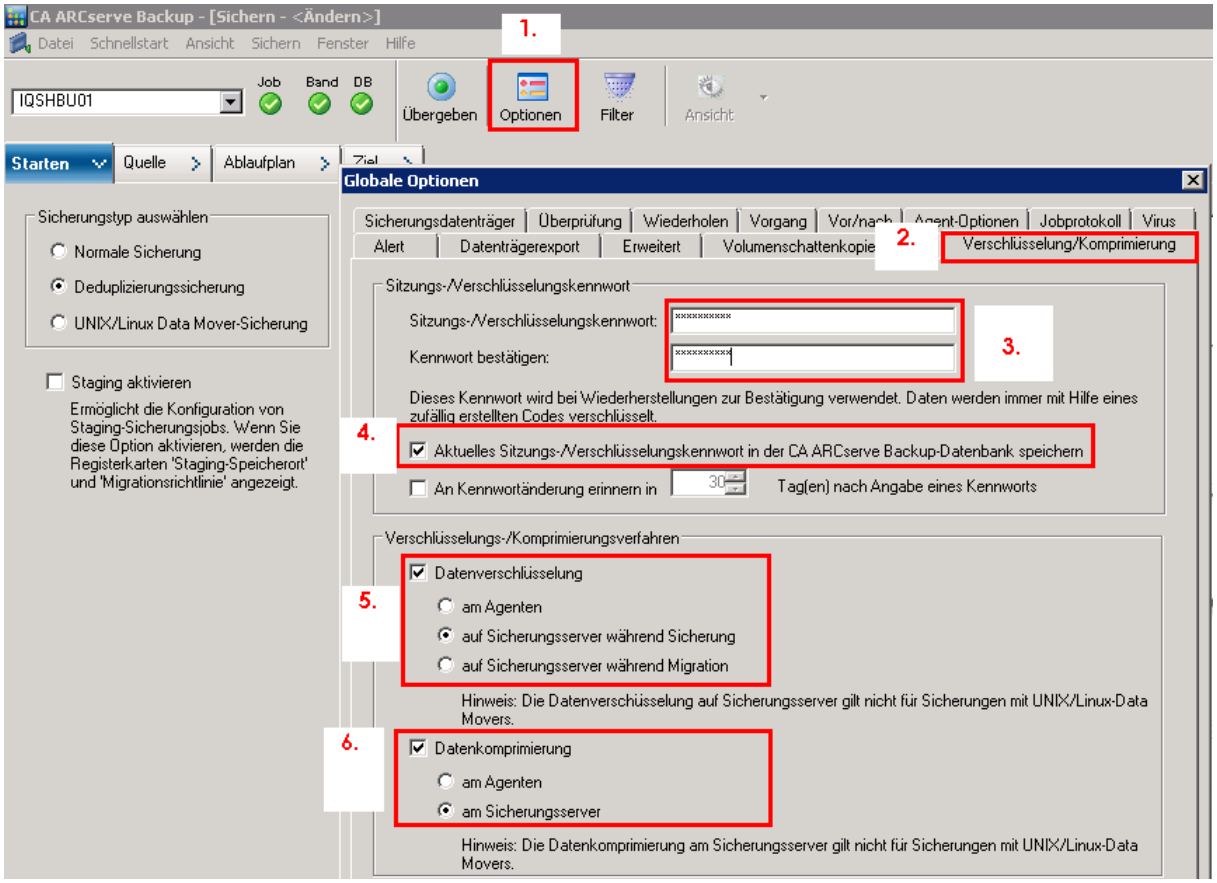
Über die Registerkarte "Verschlüsselung/Komprimierung" im Dialogfeld "Globale Optionen" des Sicherungs-Managers, kann auf die Verschlüsselungsoptionen zugegriffen werden. In diesem Dialogfeld kann die Datenverschlüsselung auf dem Agenten, auf dem Sicherungsserver während der Sicherung, oder auf dem Sicherungsserver während der Migration ausgewählt werden.

### 8.1.1 Einstellen der Verschlüsselung für einen bestehenden Sicherungsjob




Beispiel NAS-Sicherung (Selektieren und Ändern wählen)

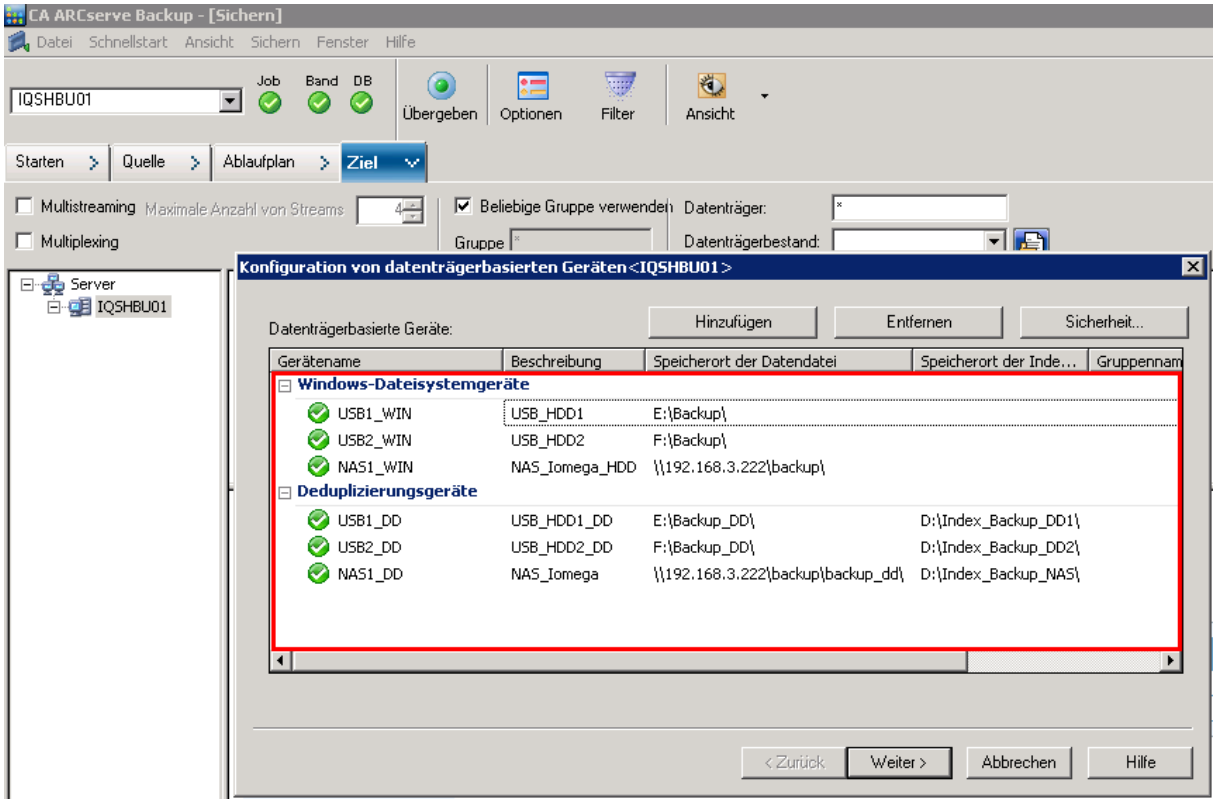
### 8.1.2 Einstellungen




1. Wählen der Optionen für den bestehenden Sicherungsjob
2. Registerkarte Verschlüsselung / Komprimierung
3. Festlegen eines Sitzungs-und Verschlüsselungskennwortes (Optional)
4. Verschlüsselungsverfahren: (auf dem Sicherungsserver während der Sicherung
5. Auswahl der Datenkomprimierung am Sicherungsserver

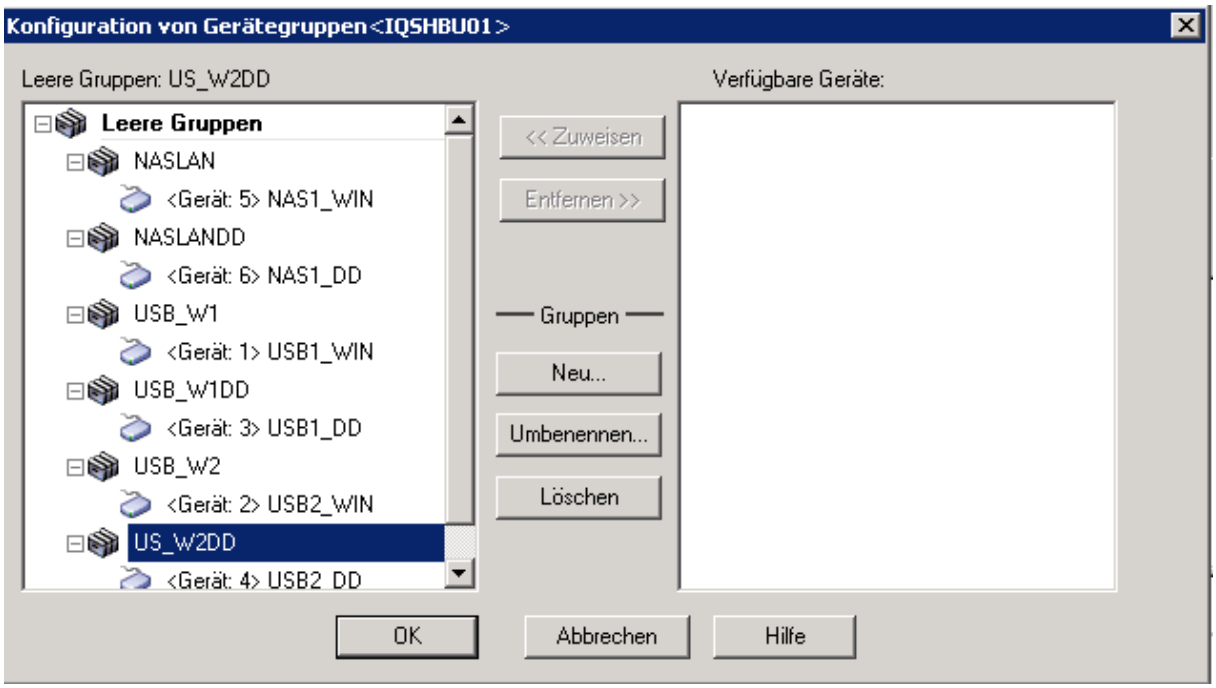
## 8.2 Einrichtung einer normalen Sicherung mit Verschlüsselung

**Hinweis: Die Verschlüsselung kann nicht mit Deduplizierung durchgeführt werden. Die Verschlüsselung wird nur bei normalen Sicherungen möglich.**

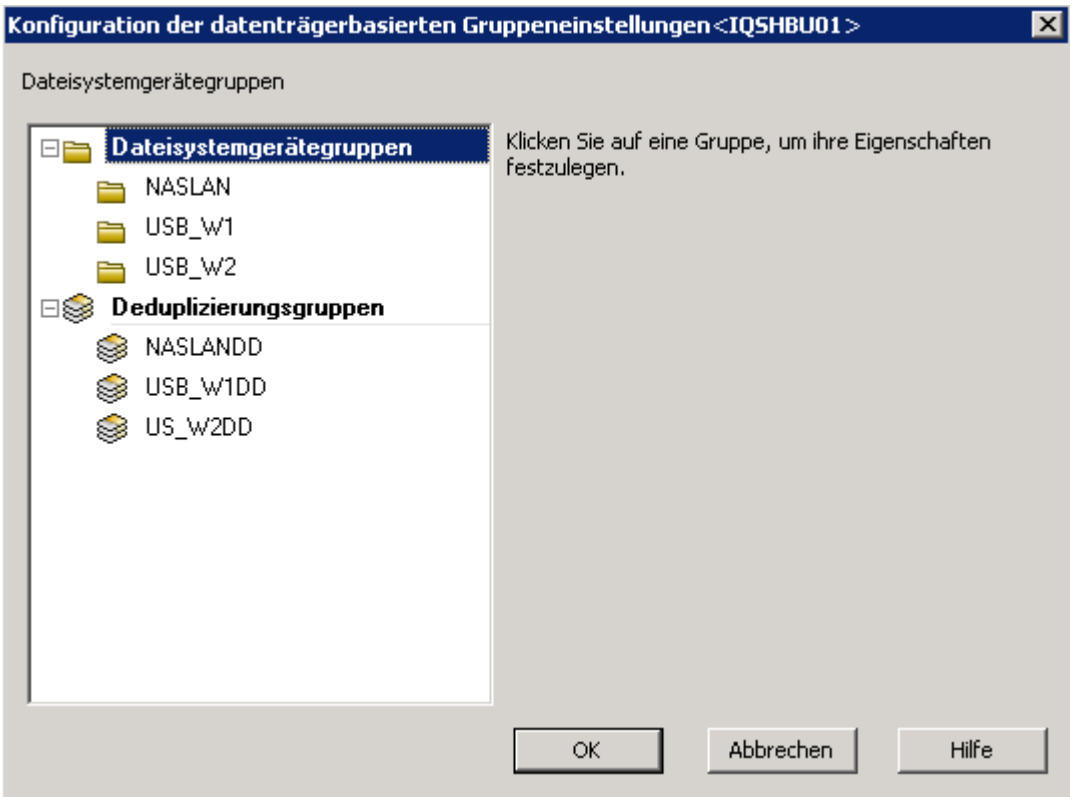



Angelegte Datenträgerbasierte Geräte
(Unterscheidung für Windows (NTFS)- und Sicherungen mit Deduplizierung)

### 8.2.1 Zuweisung der Geräte zu neu erstellten Sicherungsgruppen

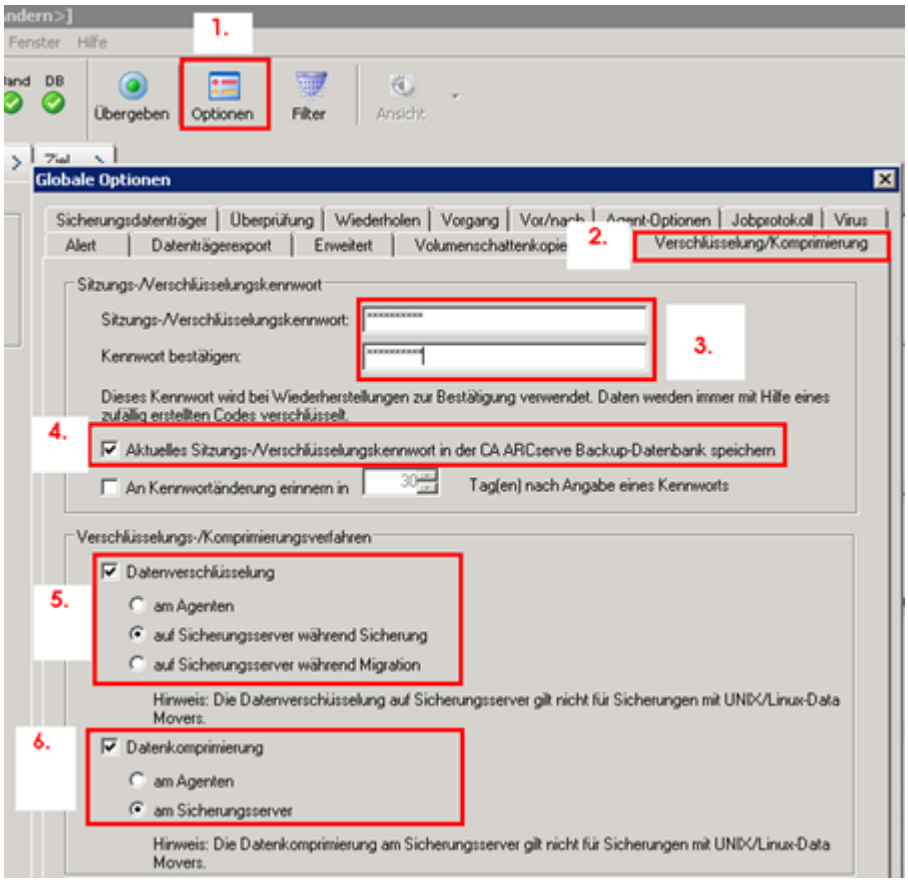



Erstellte Gruppen für die Sicherung mit Verschlüsselung und Deduplizierung, mit bereits zugewiesenen Geräten.

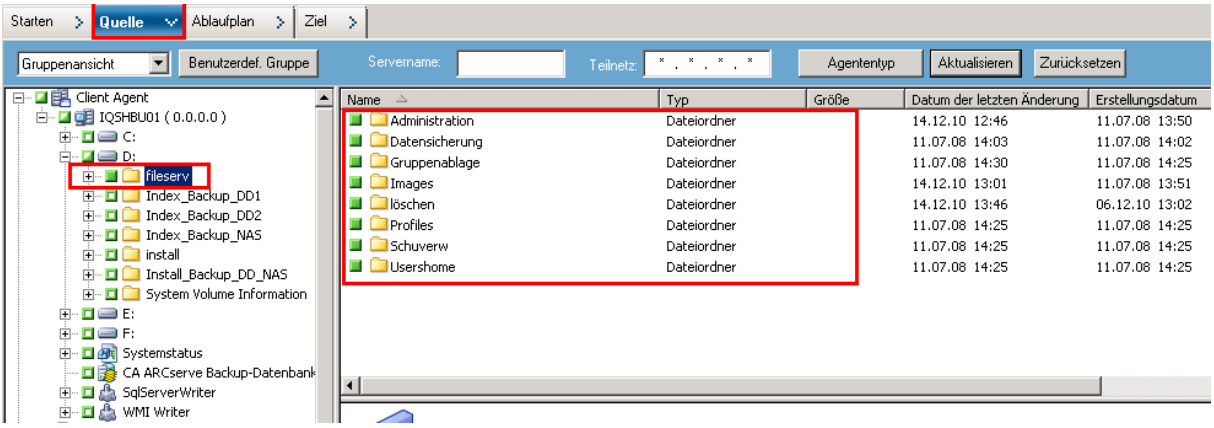



Zusammenfassung der Dateisystemgerätegruppen

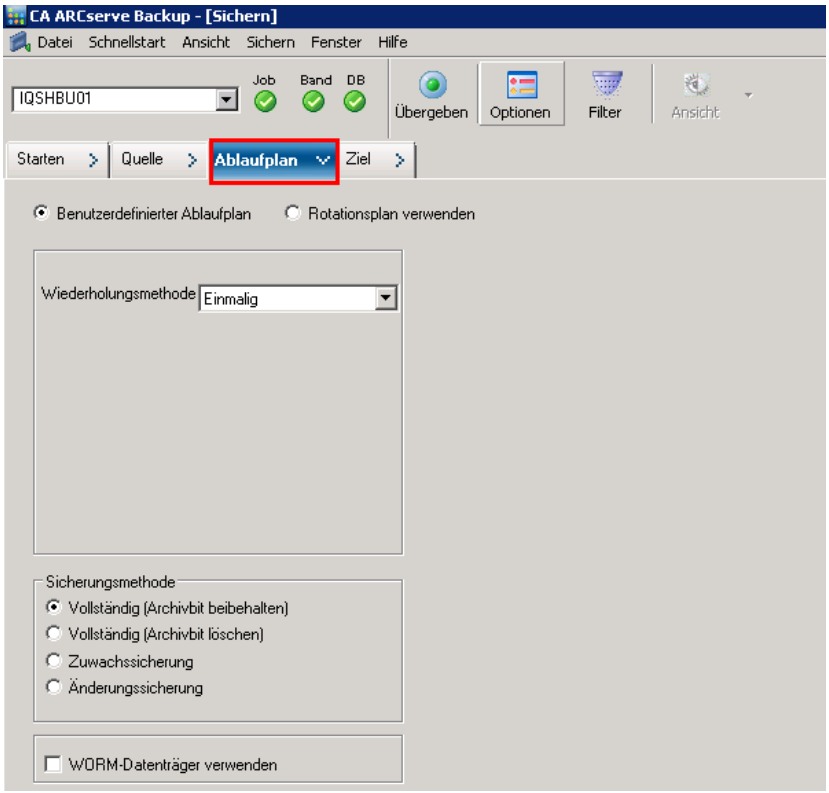
### 8.2.2 Testsicherung mit Verschlüsslung.

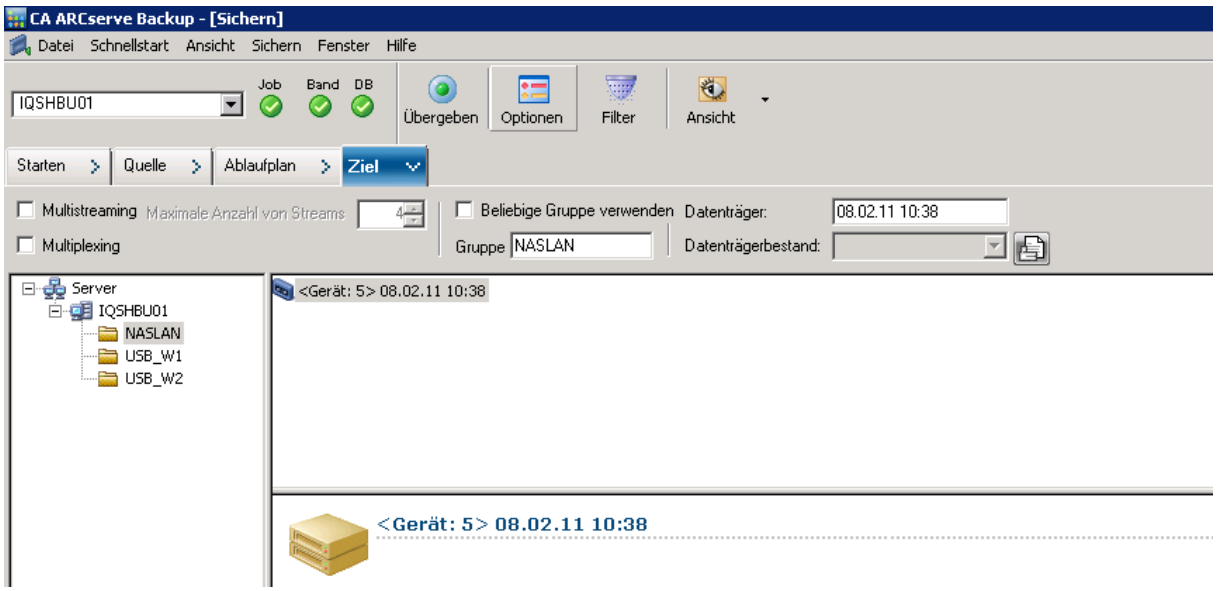

Anwenden der Verschlüsselungsfunktionen




Beispielauswahl des Ordners „fileserv“

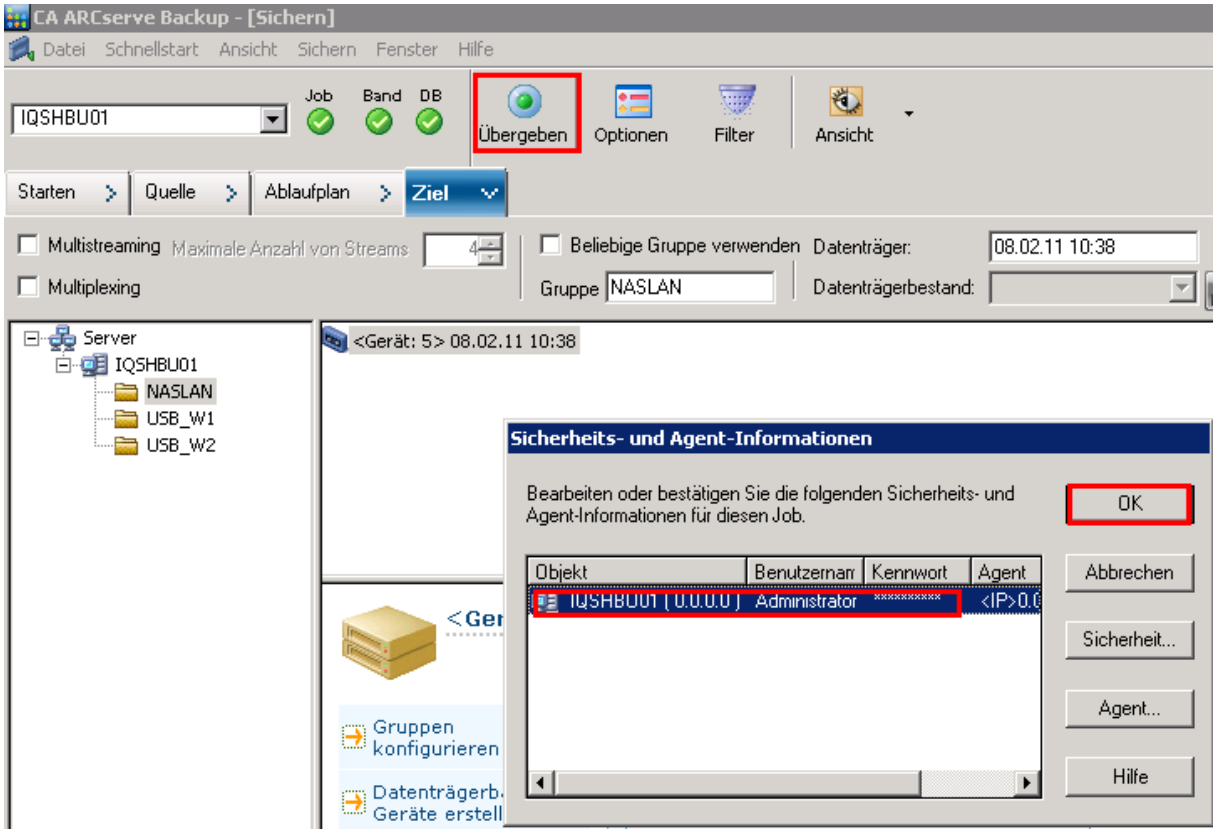


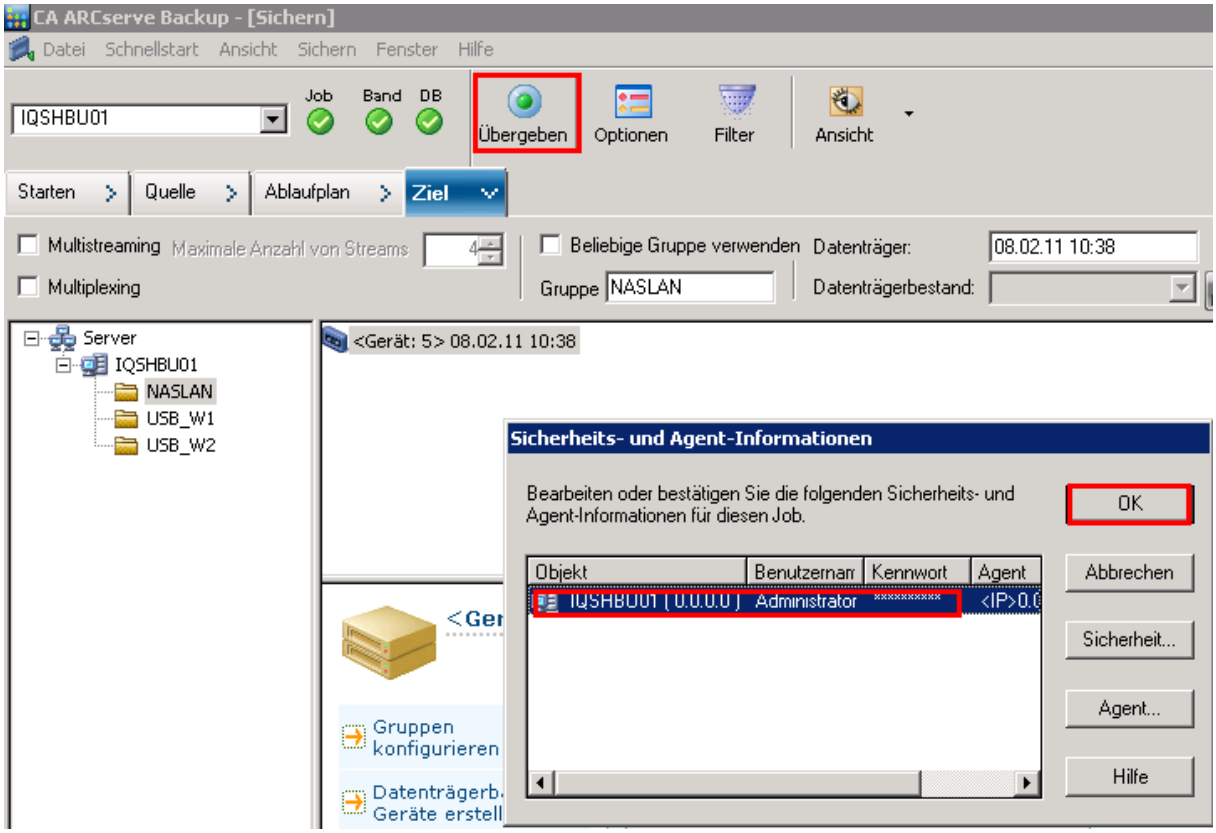

Bestimmen des Ablaufplans (Hier einmalig)



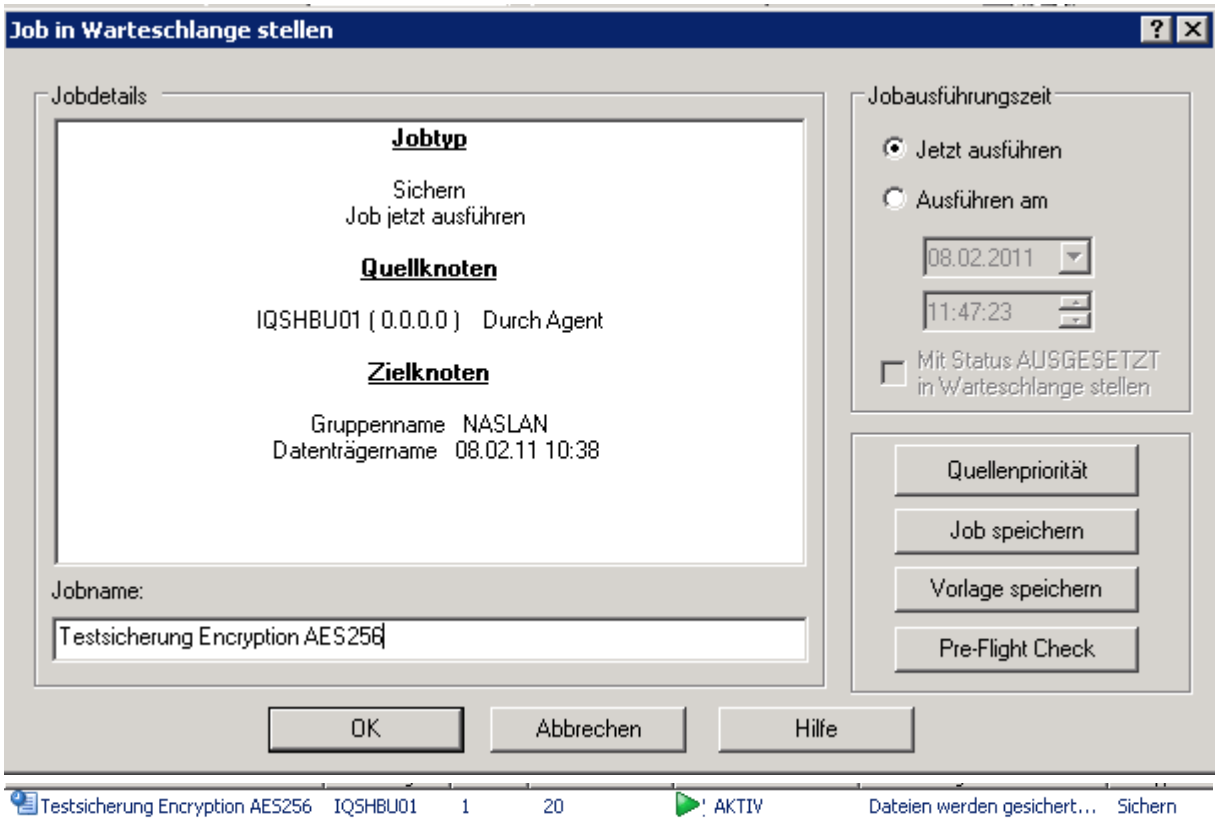

Auswahl des Ziels. (Hier NASLAN)

**Hinweis: Wenn beim Start der Einrichtung der Sicherung die normale Sicherung gewählt wird, tauchen in der Übersicht auch nur die einst hierfür erstellen Datenträger auf.**



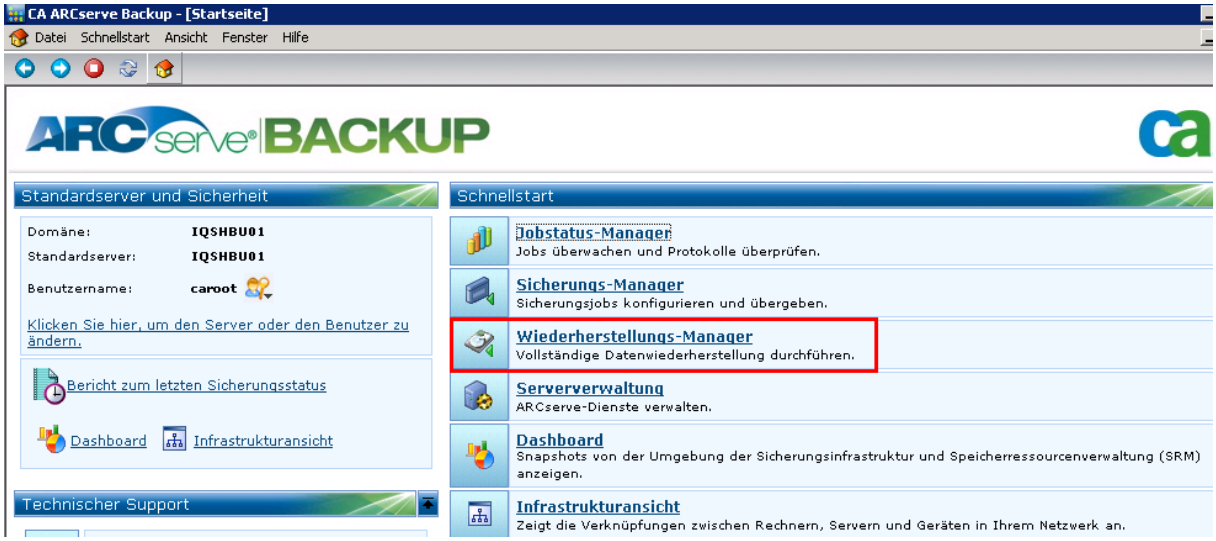



Übergabe des definierten Sicherungsjobs.

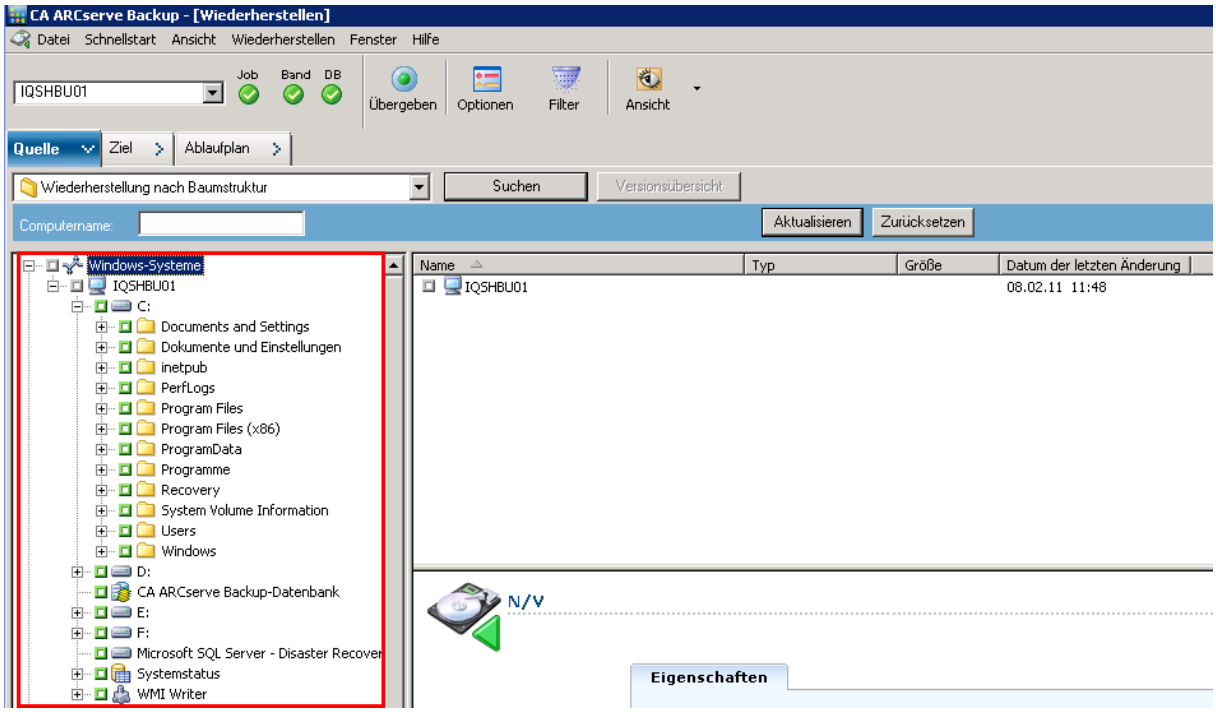


# 9. Wiederherstellung

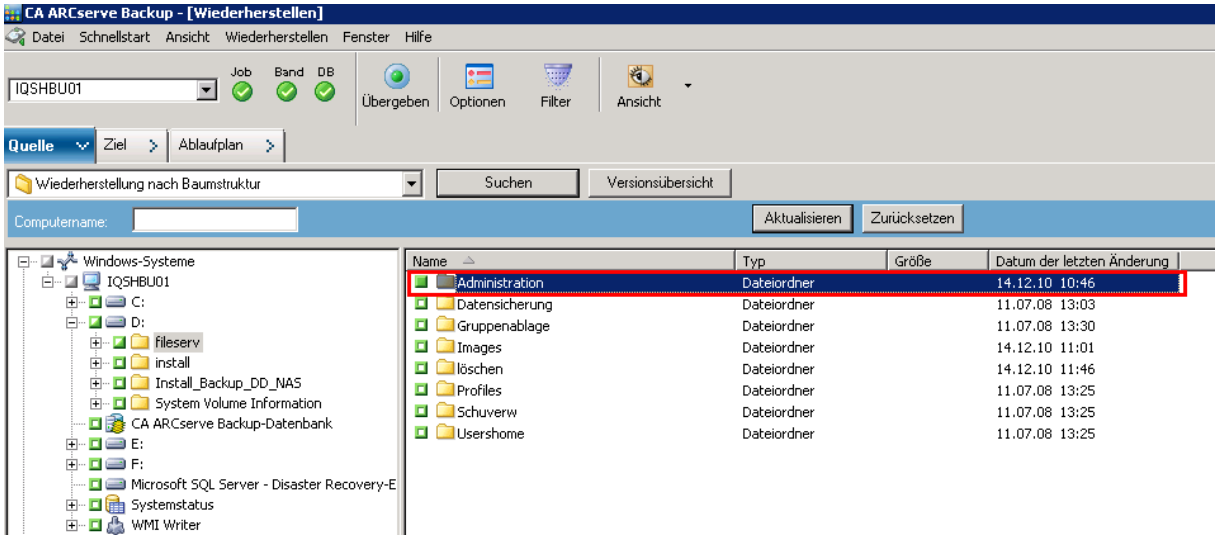
## 9.1 Wiederherstellen von Daten (Ordner und Dateien)



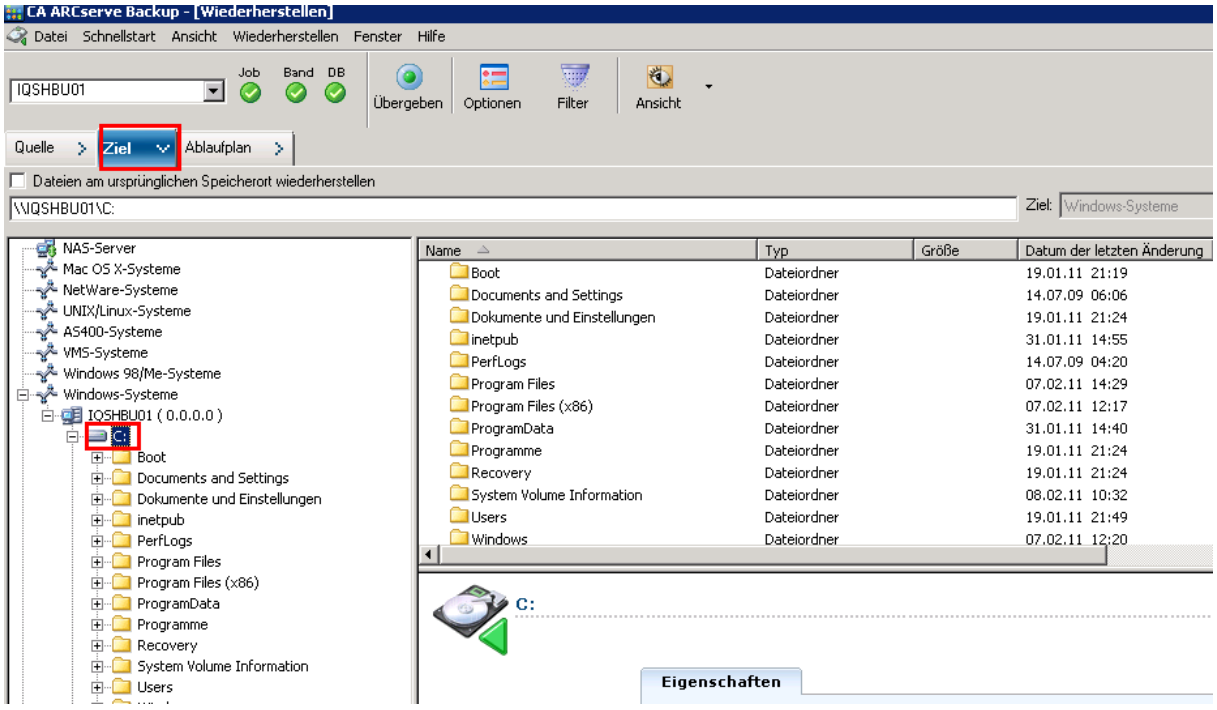

Wählen des Wiederherstellungsmanagers



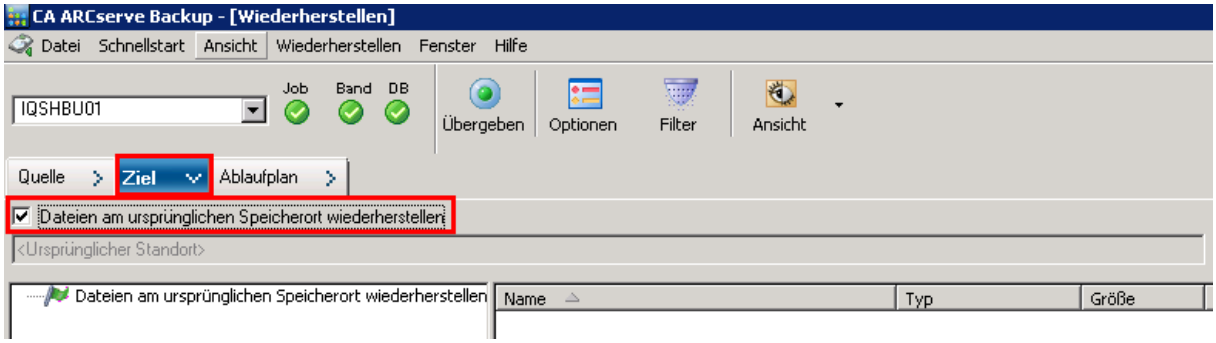

Auswahl des Pfades



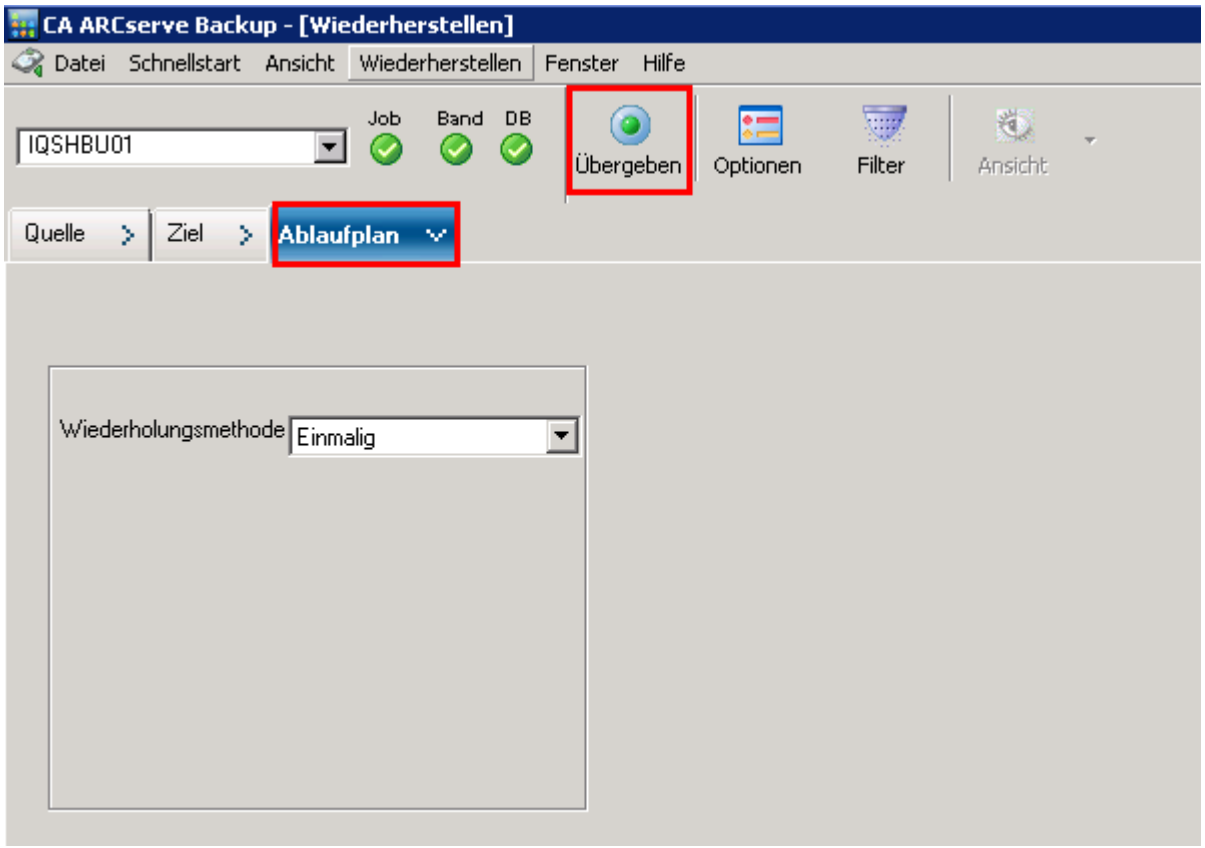

Beispielordner „Administration“



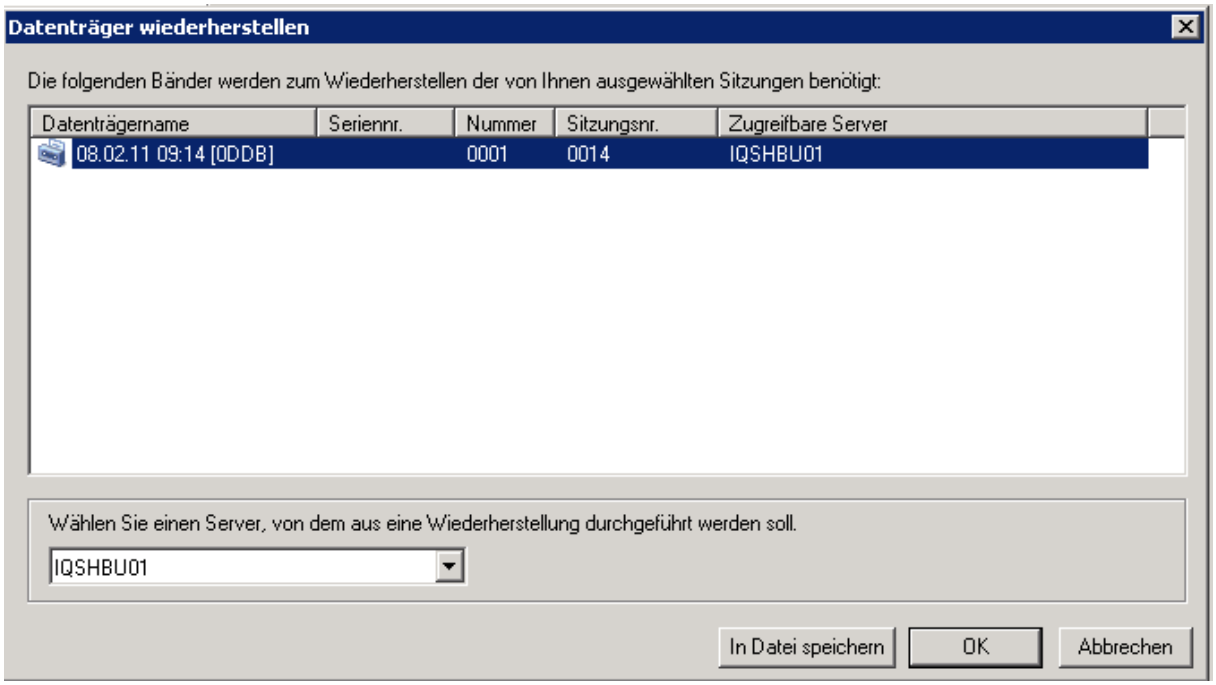

Wiederherstellung nach C:\ (Beispiel)



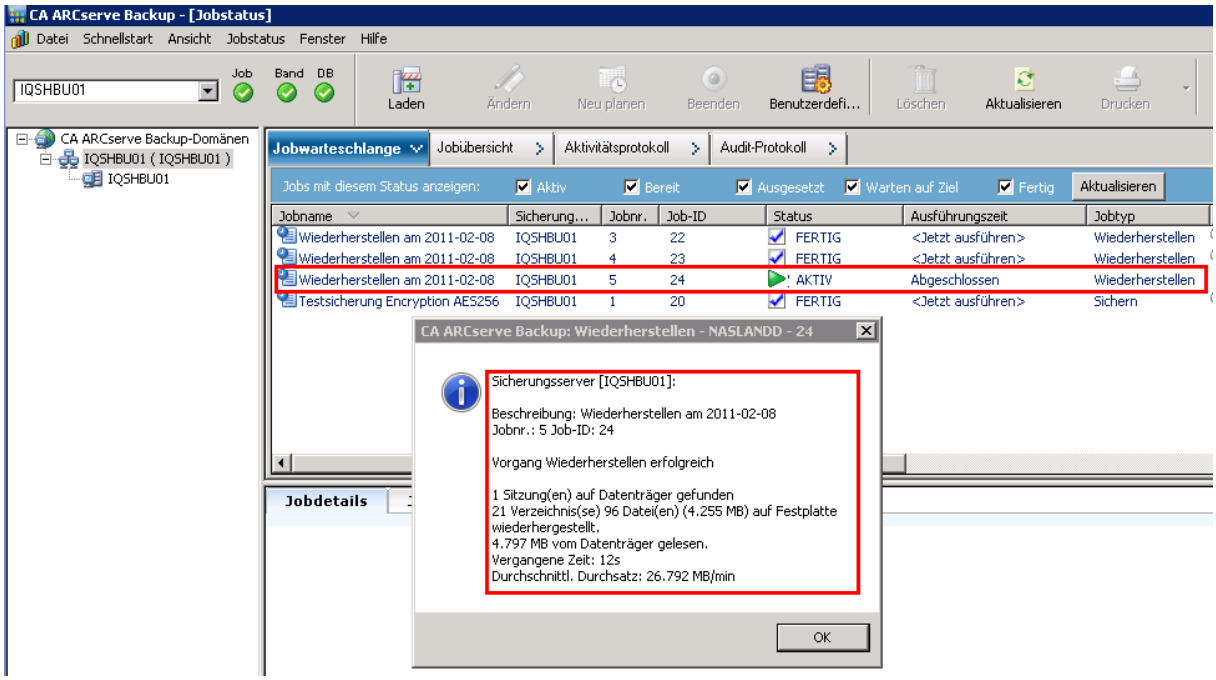

Option: „Dateien am ursprünglichen Speicherort wiederherstellen“



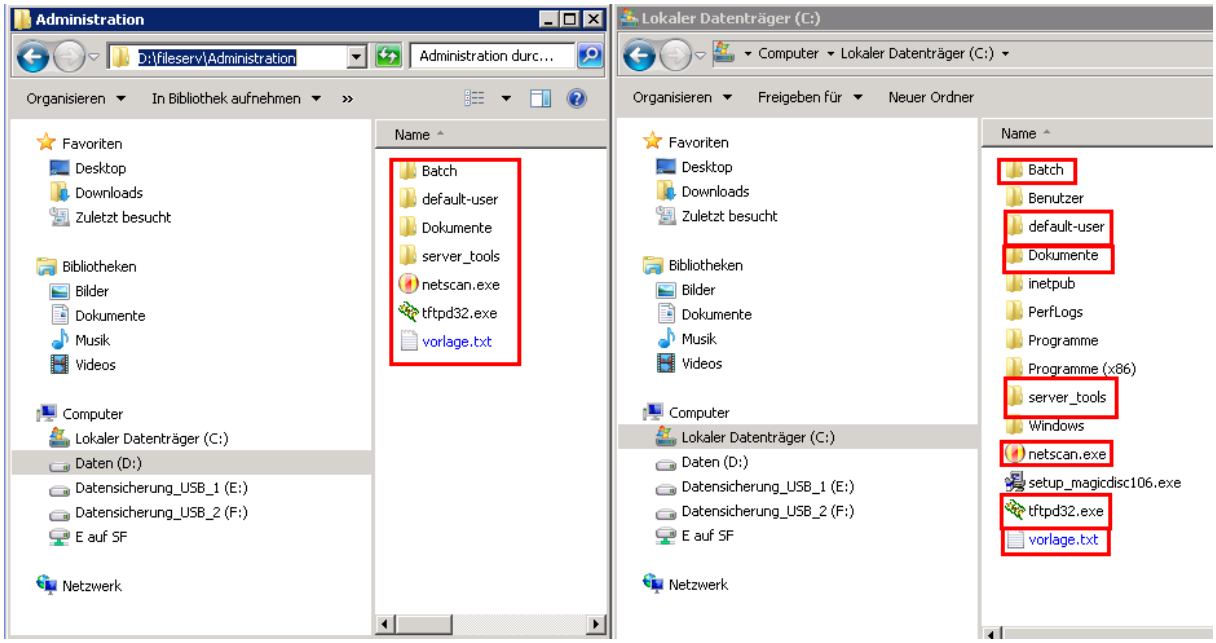

Übergabe an das System




Hinweis auf den benötigten Datenträger für die Wiederherstellung.

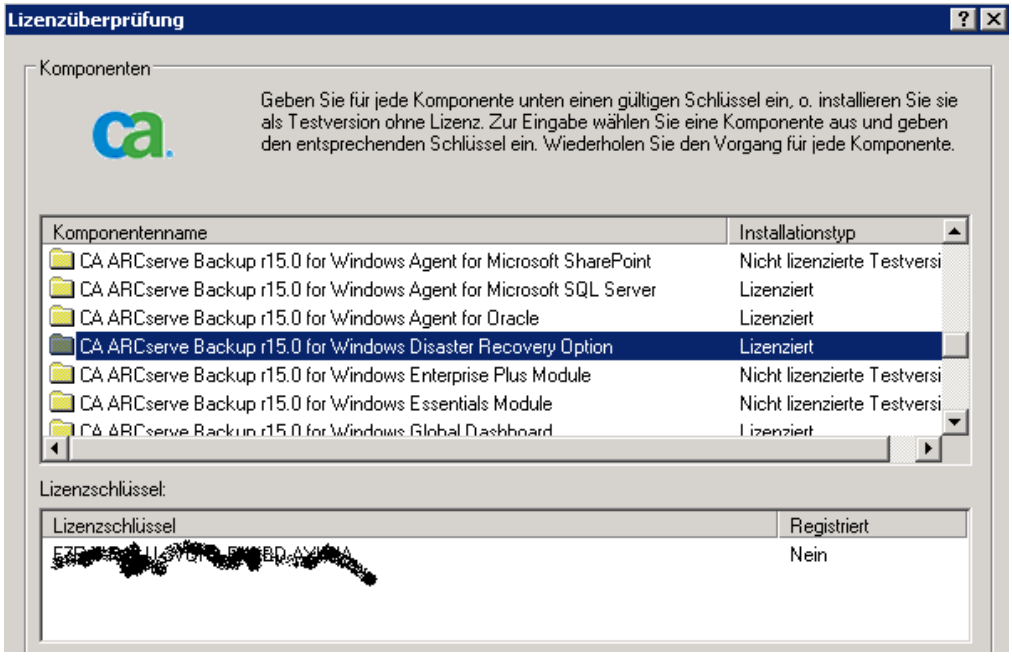



Fertigstellung der Wiederherstellung




Ergebnis

## 9.2 Wiederherstellung von Datenträgern




**Hinweis: Um eine Gesamtwiederherstellung eines Systems oder einer Partition zu gewährleisten ist die Desaster-Recovery Option zu Lizenzieren.**

### 9.2.1 Wiederherstellen von Servern nach einem Systemausfall

### 9.2.2 Empfehlung: Einsatz von CA ArcServe D2D

Grundsätzlich kann die Desaster Recovery Option zusätzlich Lizenziert und eingesetzt werden. Es hat sich jedoch als praktikabler erwiesen, das Backup R15 parallel mit dem D2D Produkt zu vereinen.

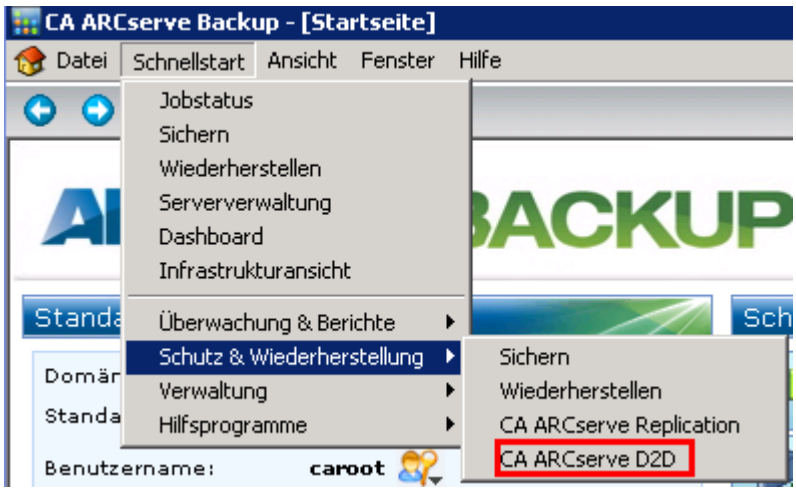
**Hinweis: In dieser Empfehlung wird kurz beschrieben, wie ein Server mit der Image Funktion D2D wiederhergestellt wird. Diese Funktion ist Anwendbar auf Server 2003 sowie Server 2008.**

### 9.2.3 Parallele Installation zur CA ARCserve Backup R15

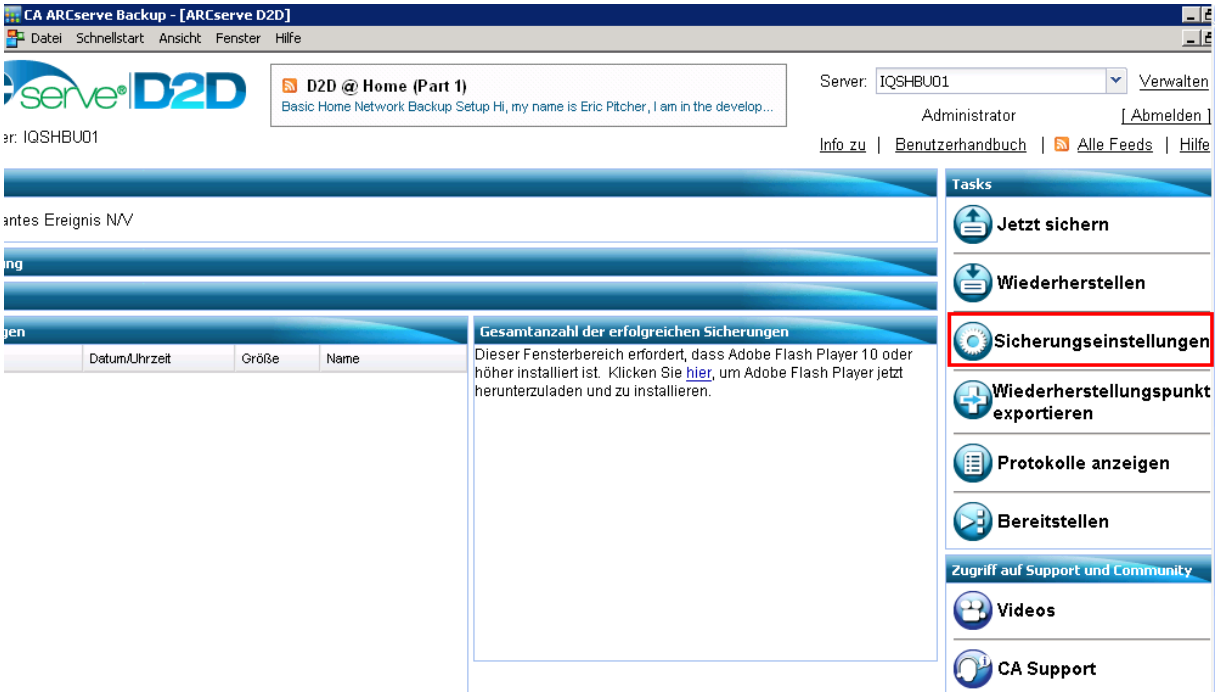
Die Installation von CA ARCserve D2D kann parallel zu bestehenden Backup R15 Version erfolgen.

### 9.2.4 Voreinstellung D2D

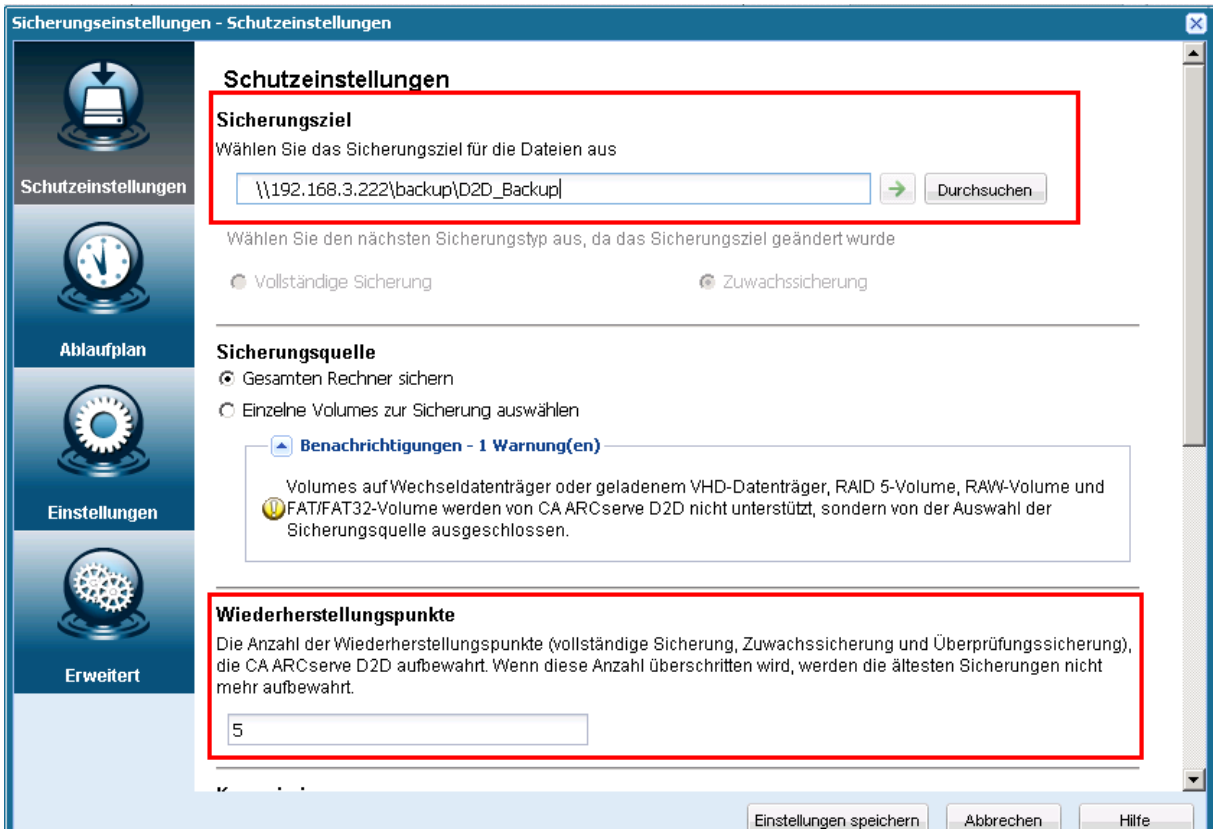
Nach erfolgter Installation ist Im ersten Schritt ist das D2D zu konfigurieren.
D2D implementiert sich vollständig in das Backup r15 Produkt.




Anmeldung an der Weboberfläche



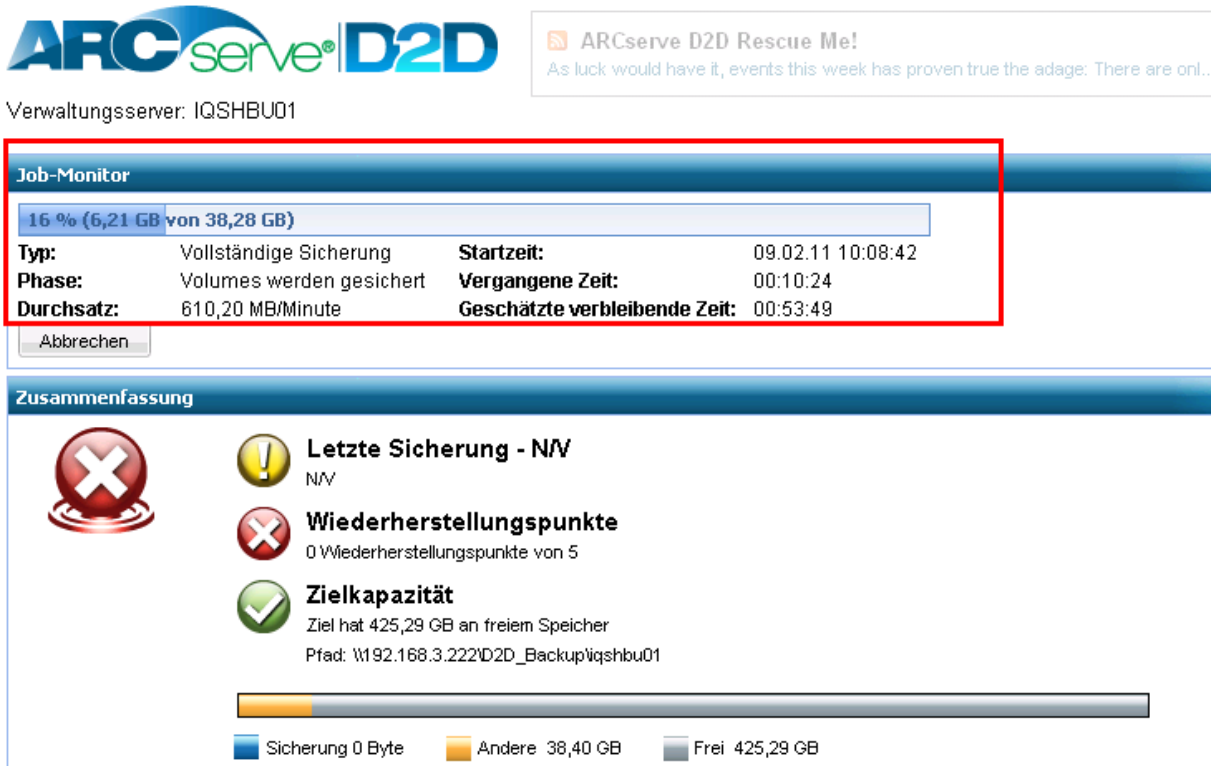

Im ersten Schritt werden die Sicherungseinstellungen ausgewählt.




Wesentlichen Einstellungen: Ziel der Sicherung.
(Hier das NAS Laufwerk mit bereits angelegten Sicherungsordner D2D_Backup)

Die Anzahl der Widerherstellungspunkte.
(In diesem Beispiel 5 Tage)

Im Vorwege ist sicherzustellen, dass auf dem NAS Laufwerk die entsprechenden Sicherheitseinstellungen auf dem Ordner vergeben sind.



Laufendes vollständiges Backup.

### 9.2.5 Herstellung eines Notfall Boot Mediums für die Wiederherstellung (BMR)*

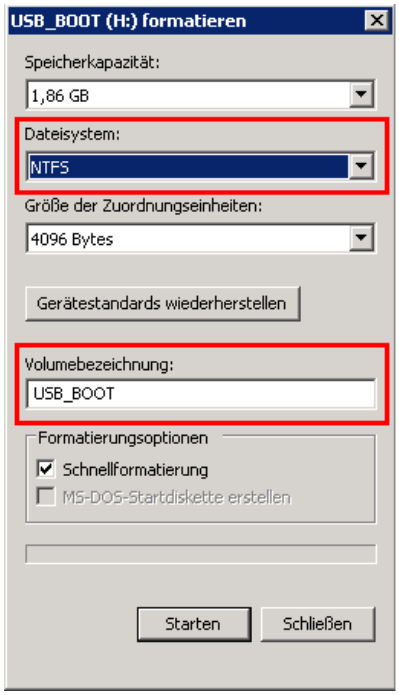
Da es sich bei den Schulservern um Geräte handelt, die kein integriertes CD / DVD Laufwerk haben, ist es erforderlich den Startvorgang von einem Wechseldatenträger zu Gewährleisten.

* BMR = Bare Metal Recovery

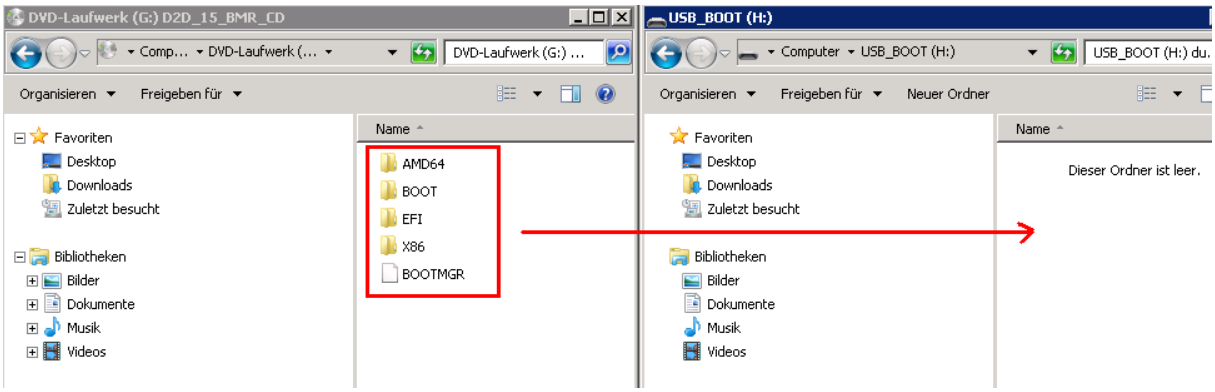
### 9.2.5.1 Herstellung eines USB Notfallmediums für die Komplettwiederherstellung.

**Hinweis: Mindestkapazität des USB Sticks: 2 GB**

1. Formatieren es USB Sticks (Wichtig: NTFS Dateisystem)



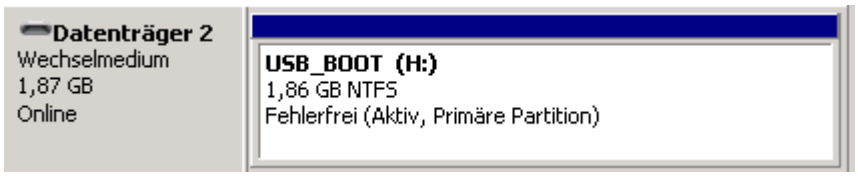

2. Kopieren des Boot Managers auf den USB Stick
   (Der D2DBMR ist als ISO Datei im Installationsmedium vorhanden und wird entsprechend gemounted)



3. Die USB Stick Partition aktivieren
   Der USB Stick ist zu Partitionieren und zu aktivieren, damit dieser Bootfähig wird.
   Dies geschieht mit dem Kommandozeilentool „Diskpart“

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Administrator>cd \

C:\>diskpart

Microsoft DiskPart-Version 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
Auf Computer: IQSHBU01

DISKPART> list disk

  Datenträger ###  Status         Größe     Frei     Dyn  GPT
  ---------------  -------------  -------  -------  ---  ---
  Datenträger 0    Online          232 GB      0 B   *
  Datenträger 1    Online          232 GB      0 B   *
  Datenträger 2    Online         1910 MB      0 B
  Datenträger 3    Online          232 GB      0 B

DISKPART> select disk 2

Datenträger 2 ist jetzt der gewählte Datenträger.

DISKPART> list partition

  Partition ###  Typ              Größe    Offset
  -------------  ---------------  -------  -------
  Partition 1    Primär           1906 MB  4032 KB

DISKPART> select partition 1

Partition 1 ist jetzt die gewählte Partition.

DISKPART> active

Die aktuelle Partition wurde als aktiv markiert.

DISKPART> list partition

  Partition ###  Typ              Größe    Offset
  -------------  ---------------  -------  -------
* Partition 1    Primär           1906 MB  4032 KB
```

4. Ergebnis in der Datenträgerverwaltung



#### 9.2.5.2 Verschlüsselung (Hinweis und Empfehlung)

In vorherigen Absatz wurde das Wiederherstellungs-Backup direkt auf den Netzwerkspeicher geschrieben. Um auch hierfür eine Verschlüsselung zu gewährleisten, wären folgende Schritte notwendig:

1. D2D Backup auf einen lokalen Datenträger des Servers (Beispiel D:\)
2. Verschlüsselte Sicherung durch ARCserve Backup r15 auf USB oder Netzwerkspeicher.

Die Beschreibung für die Verschlüsselung ist in Kapitel 7 beschrieben.

#### 9.2.5.3 Wiederherstellung eines Servers vor Ort

Hinweis: Um einen Server bei einem Hardware oder Systemausfall vollständig wiederherzustellen, wird das in 8.2.5.1 erstellte USB Medium benötigt.

1. Eingelegen des USB Sticks
2. Änderung der Boot Reihenfolge im Bios des Servers
3. Boot vom USB Stick
4. Wahl des Backup Ortes (Netzwerkspeicher oder USB Festplatte)
5. Ggf. Auswahl eines Storage Treibers.
   (Von Fall zu Fall unterschiedlich und nicht weiter behandelt)
6. Auswahl der Wiederherzustellenden Partition
7. Wiederherstellung und Neustart des Systems.