



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.

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 Datenschutz 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 angeschlossenen Rechner,
- den sichereren Zugriff auf das Internet und
- den Zugriff auf Haushaltsanwendungen beim Schulträger.

Auch viele neue Verfahren basieren inzwischen auf dem vom Unabhängigen Landeszentrum 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, datenschutz zertifiziert, 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	Berufsschule	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 sobald 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, sobald 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 sobald 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	Westfehmar	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	4
1.1	Allgemein.....	4
1.1.1	Einsatz an den Schulen	4
1.1.2	Zusammenschluss und Vereinheitlichung (Landesnetz Bildung)	5
1.2	Zieldefinition	5
1.2.1	Lokale Sicherung	5
1.2.2	Zentrale Sicherung	5
1.3	Testumgebung Domäne IQSH.INTERN	5
2.	Datenschutz	6
2.1	Einhaltung der Datenschutzmaßnahmen	6
2.2	Anforderung an die Datensicherung.....	6
2.3	Umgang und Handhabung der Datensicherung	6
2.3.1	Auszüge aus dem LDSG (Landesdatenschutzgesetz)	6
2.3.1.1	§ 5 Maßnahmen zur Datensicherheit.....	6
2.3.1.2	§ 6 Maßnahmen zur Datensicherheit bei Einsatz automatisierter Verfahren	7
2.4	Kennwortsicherheit	8
2.4.1	Verwendete Kennwörter und Verfahrensweisen	8
2.5	Verantwortlichkeit und Vorgehensweise	8
2.6	Aufbewahrungsfristen der Datensicherung.....	8
3.	Durchführungsanleitung und Dokumentation	9
3.1	Testbetrieb und Evaluierung	9
3.2	Standortspezifische Dokumentation	9
3.3	Erweiterung des Netzplanes durch Datensicherungsanteil.....	9
3.4	Inventarisierung der Geräte und der eingesetzten Software	9
4.	Sicherungstechnologien	10
4.1	<u>Hardware</u>	10
4.1.1	Eckdaten zum Datensicherungsmedium (NAS).....	11
4.1.2	Sicherungsfestplatten.....	11
4.1.3	Backup-Server.....	11
4.2	<u>Software</u>	12
4.2.1	Betriebssysteme	12
4.2.2	CA ARCserve Backup r15.....	12
4.2.2.1	Leistungsmerkmale CA ARCserve Backup R15.....	13
4.2.2.2	Systemvoraussetzungen CA ARCserve Backup R15	14
4.2.2.3	Erforderlicher Festplattenplatz zum Installieren	15
4.2.2.4	Datensicherungskonto	15
4.2.3	CA ARC Serve Replication and High Availability	16
4.2.3.1	Leistungsmerkmale CA ARCServe Replication and High Availability	16
4.2.3.2	Systemvoraussetzungen CA ARCServe Replication and High Availability	16
4.2.4	CA ArcServe D2D r15 (Disk to Disk Backup)	17
4.2.4.1	Leistungsmerkmale CA ArcServe D2D R15	17
5.	Vorbereiten der Hardware für die Sicherung	18

5.1	Vorbereitung des Datensicherungslaufwerks (Iomega NAS)	18
5.1.1	Grundeinrichtung als Backuplaufwerk	18
5.1.1.1	Anlegen eines Backup-Benutzers	19
5.1.1.2	Anlegen eines Backup-Ordners	20
5.1.1.3	Prüfung der Datensicherheit	21
5.1.1.4	Kennwort für Benutzer und Backup-Ordner.....	21
5.2	Vorbereitung des Datensicherungslaufwerks (Externes USB Laufwerk)	22
5.2.1	Anlage der Sicherungs- und Index Dateiordner	23
6.	Installation ARCserve Backup r15	25
6.1	Installation ARCserve Backup r15 auf Server 2008 // R2.....	25
6.2	Kurzübersicht Global Dashboard (Optional)	37
6.2.1	Konfiguration des Global Dashboards	38
6.2.2	Anpassung der Lizenzierung	39
6.2.3	Abschluss der Installation.....	40
6.3	Installation ARCserve Backup r15 auf Server 2003 // R2.....	40
7.	Einrichtung von ARCserve Backup r15	41
7.1	Einrichtung CA ARCserve Backup r15 unter Server 2008 / R2 <u>(USB Laufwerk)</u>	41
7.1.1	Ersteinrichtung der Datensicherungslaufwerke (USB)	41
7.2	Einrichtung CA ARCserve Backup r15 unter Server 2008 / R2 <u>(NAS Laufwerk)</u>	52
7.3	Einrichtung CA ARCserve Backup r15 unter Server 2003/ R2 <u>(USB Laufwerk)</u>	58
7.4	Einrichtung CA ARCserve Backup r15 unter Server 2003/ R2 <u>(NAS Laufwerk)</u>	58
8.	Verschlüsselung der Daten während der Sicherungen mit CA ARCserve	59
8.1	Festlegen der Verschlüsselungsfunktion	59
8.1.1	Einstellen der Verschlüsselung für einen bestehenden Sicherungsjob	60
8.1.2	Einstellungen	60
8.2	Einrichtung einer normalen Sicherung mit Verschlüsselung	61
8.2.1	Zuweisung der Geräte zu neu erstellten Sicherungsgruppen	62
8.2.2	Testsicherung mit Verschlüsselung.	63
9.	Wiederherstellung	67
9.1	Wiederherstellen von Daten (Ordner und Dateien)	67
9.2	Wiederherstellung von Datenträgern	71
9.2.1	Wiederherstellen von Servern nach einem Systemausfall	72
9.2.2	Empfehlung: Einsatz von CA ArcServe D2D.....	72
9.2.3	Parallele Installation zur CA ARCserve Backup R15	72
9.2.4	Voreinstellung D2D	72
9.2.5	Herstellung eines Notfall Boot Mediums für die Wiederherstellung (BMR)*	75
9.2.5.1	Herstellung eines USB Notfallmediums für die Komplettwiederherstellung.	76
9.2.5.2	Verschlüsselung (Hinweis und Empfehlung)	78
9.2.5.3	Wiederherstellung eines Servers vor Ort	78

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)	lomega Nas StorCenter ix2-200
iqshbu01	192.168.3.223	Alpha 2000 Schul-Mitgliedserver (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 Protokollbestände 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 Dienstkenwort 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 Wiederherstellungskennwort, 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 DSGVO **[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 DSGVO. 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)

lomega 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, dass 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 Datenschutzerfordernungen 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 angepasst 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

Mitgliedserver: 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.
- Mitgliedserver: 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.
- Mitgliedserver: 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 Availability

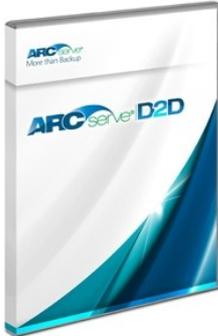
- Hochverfügbarkeit des gesamten Systems schützt das Windows-Betriebssystem, den Systemstatus, die Anwendungen und die Daten durch Replikation "physisch zu virtuell" bzw. "virtuell zu virtuell" und Failover.
- Die LAN- und WAN-optimierte Replikation gewährleistet kontinuierlichen Schutz interner und 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 Availability

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 Wiederherstellung 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

- Unbegrenzt, 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.



The screenshot shows the web interface for an Iomega IQSHNAS01 NAS device. The header is red and contains the Iomega logo (an EMC company), a small image of the device, and the model number IQSHNAS01. Below the header, the page is titled "Anmelden" (Login). There is a checkbox labeled "Auf nicht gesicherte Inhalte ohne vorherige Anmeldung zugreifen" (Access non-secured content without previous login). Below this are two input fields: "Benutzername:" (Username) and "Kennwort:" (Password). On the right side, there is a grey box with the title "Anmelden" and the following text: "Geben Sie einen gültigen Benutzernamen und ein gültiges Kennwort ein, und klicken Sie auf Einloggen. Klicken Sie auf **Auf nicht gesicherte Inhalte ohne vorherige Anmeldung zugreifen**, um anonym auf eingeschränkten öffentlichen Inhalt zuzugreifen."

5.1.1.1 Anlegen eines Backup-Benutzers



Benutzer hinzufügen

Benutzername:

Beschreibender Name:

Kennwort:

Kennwort bestätigen:

Administrator

Sicherer Ordner für diesen Benutzer hinzufügen

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.



Benutzer hinzufügen



Die Informationen zum Benutzer 'ca-backup' wurden erfolgreich aktualisiert.

Beschreibender Name: **ca-backup**
Administrator: **Ja**

5.1.1.2 Anlegen eines Backup-Ordners



Gemeinsamen Speicher hinzufügen - Schritt 1 von 2

Ordnername:

Sicherheit aktivieren
 Bei Aktivierung dieses Kontrollkästchens können Sie festlegen, welche Benutzer Zugriff erhalten sollen.



Gemeinsamen Speicher hinzufügen - Schritt 2 von 2

Ungesicherten Lesezugriff erlauben

Legen Sie den Benutzerzugriff auf den sicheren Ordner 'ca-backup' fest:

Benutzername	Lesen/Schreiben	Lesen	Ohne
 administrator	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
 ca-backup	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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



Gemeinsamen Speicher hinzufügen



Ordner 'ca-backup' wurde erfolgreich hinzugefügt.

Sicherheit: Sicheres Lesen/Schreiben

Ordner 'ca-backup' sind folgende Zugriffsrechte zugeordnet:

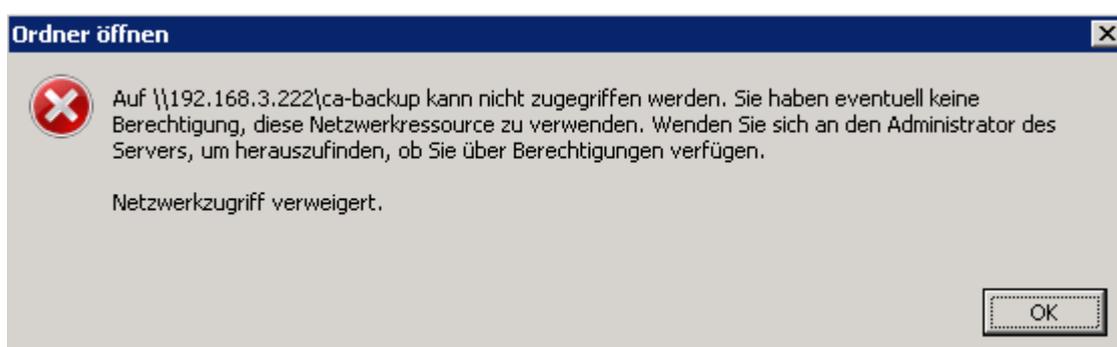
Benutzer	Zugriff
 ca-backup	Lesen/Schreiben

Zusammenfassung

5.1.1.3 Prüfung der Datensicherheit

Seitens des Backupserver 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

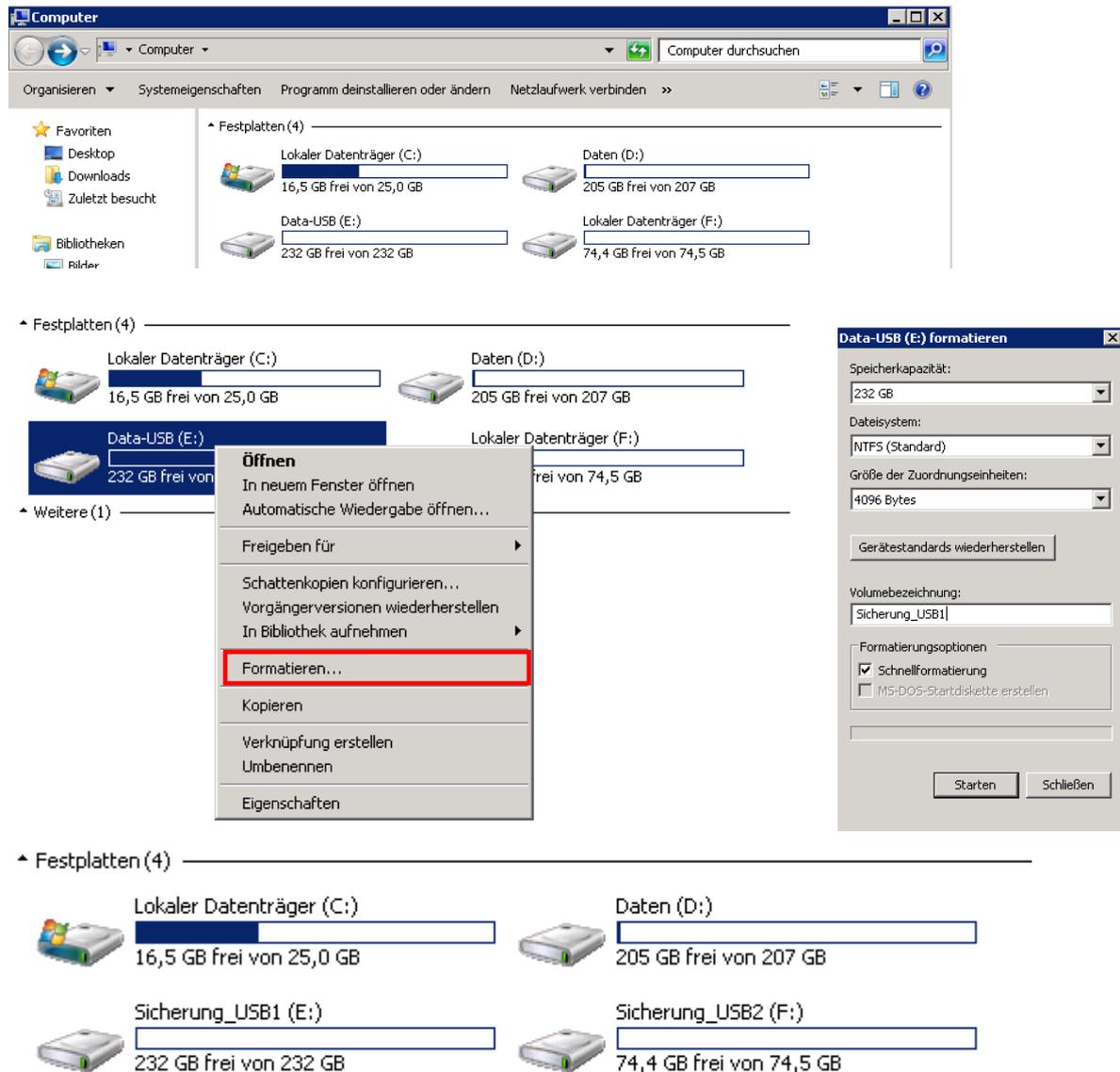


Durch den Zugriff eines nicht authentifizierten Benutzers erfolgt eine Verweigerung.

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)



The screenshot shows the Windows 'Computer' window with four drives listed: Lokaler Datenträger (C:), Daten (D:), Data-USB (E:), and Lokaler Datenträger (F:). The 'Data-USB (E:)' drive is selected, and a context menu is open with 'Formatieren...' highlighted. To the right, the 'Data-USB (E:) formatieren' dialog box is shown with the following settings:

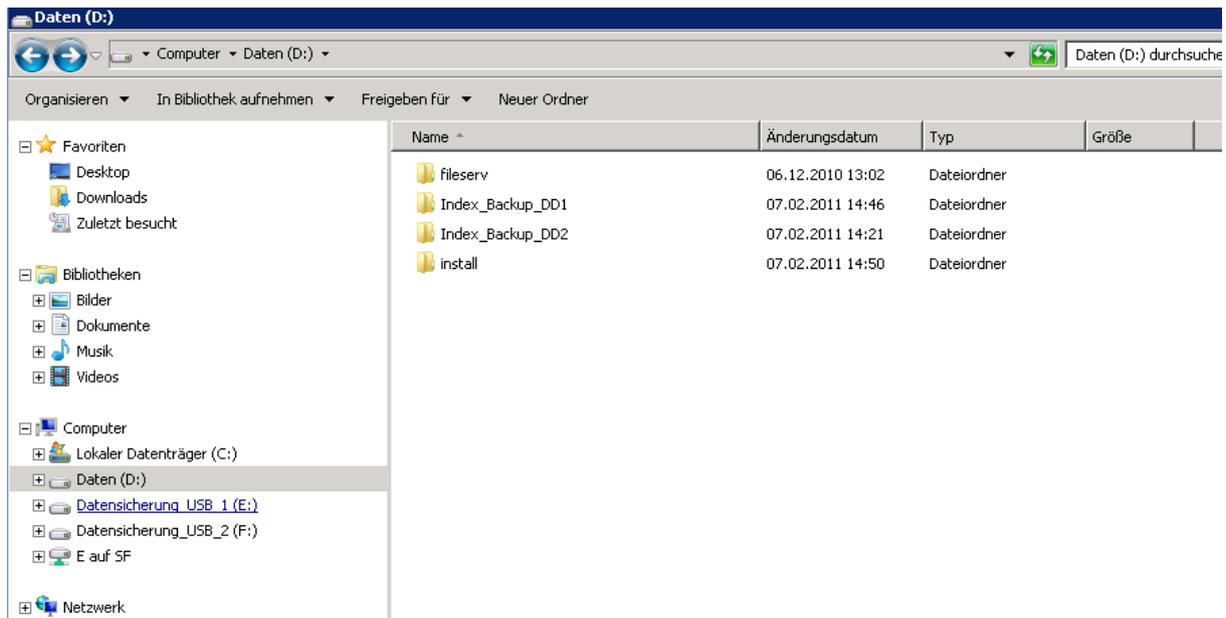
- Speicherkapazität: 232 GB
- Dateisystem: NTFS (Standard)
- Größe der Zuordnungseinheiten: 4096 Bytes
- Gerätestandards wiederherstellen (button)
- Volumebezeichnung: Sicherung_USB1
- Formatierungsoptionen:
 - Schnellformatierung
 - MS-DOS-Startdiskette erstellen
- Buttons: Starten, Schließen

Below the dialog, the drive list is updated to show 'Sicherung_USB1 (E:)' and 'Sicherung_USB2 (F:)'.

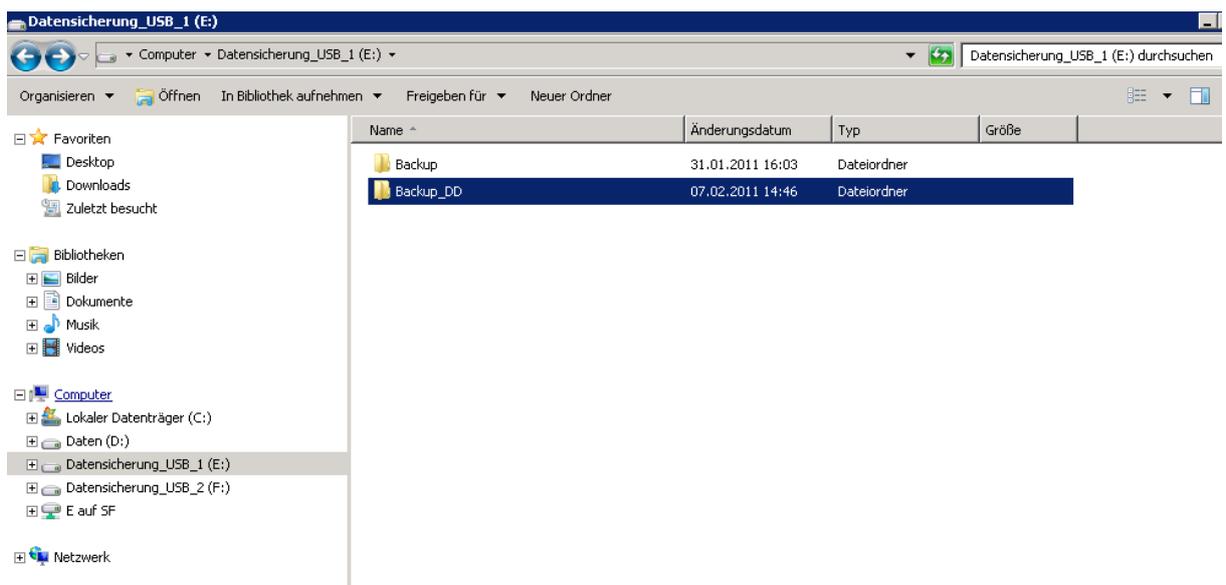
Nachdem die externen USB Laufwerke an den Server angeschlossen wurden, sollten diese im Vorwege formatiert und namentlich benannt werden.

5.2.1 Anlage der Sicherungs- und Index Dateiordner

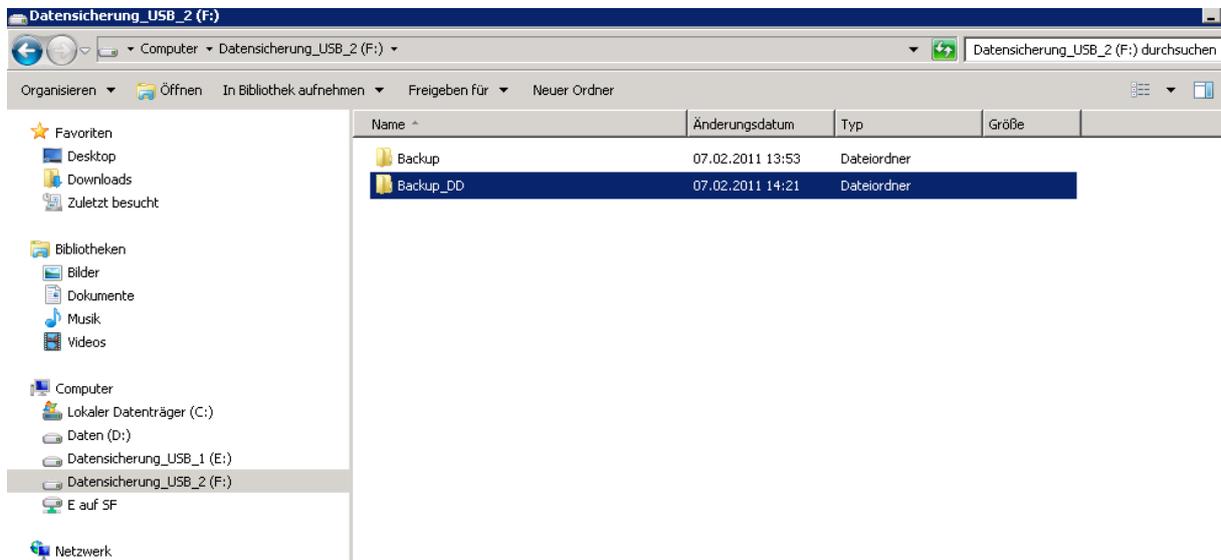
Vor Anlage der Sicherungsjobs ist es erforderlich entsprechende Ordner auf den Sicherungsdatenträgern zu erstellen.



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



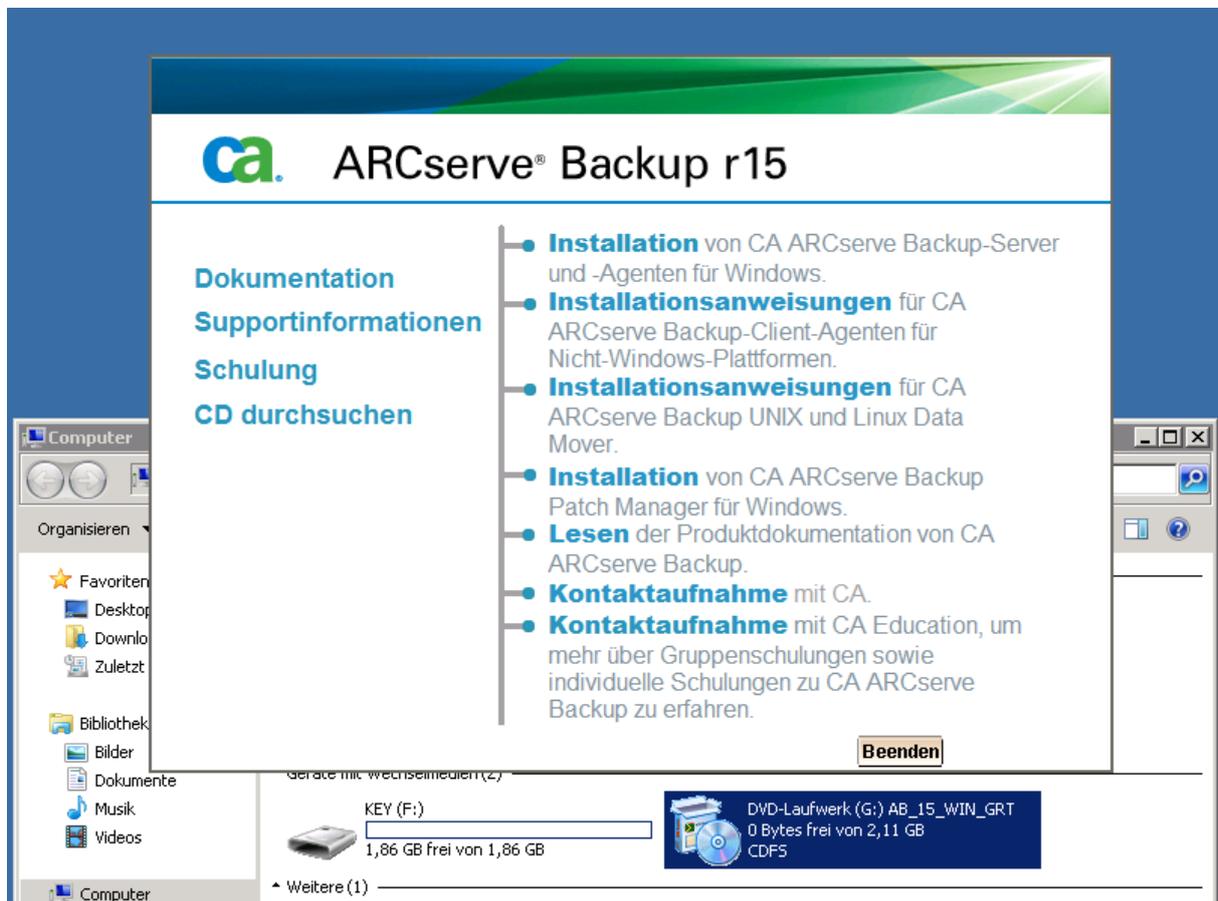
Anlage des Sicherungsordners für die Deduplizierungssicherung (Auf USB1 HDD)



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.

Erforderliche Komponenten



→ Erforderliche Komponenten

Setup benötigt die unten aufgeführten erforderlichen Komponenten, um CA ARCserve Backup zu installieren.

Komponentenname	Status
Windows Installer 3.1 Redistributable (v2)	Installiert
Microsoft Visual C++ 2005 SP1 Redistributable Package (x86)	Ausstehend
Microsoft Visual C++ 2005 SP1 Redistributable Package (x64)	Ausstehend



Wählen Sie eine der folgenden Möglichkeiten:

- Klicken Sie auf 'Installieren', um die erforderlichen Komponenten zu installieren. Diese Option ermöglicht Ihnen die Installation von CA ARCserve Backup.
- Klicken Sie auf 'Abbrechen', wenn Sie die erforderlichen Komponenten nicht installieren möchten. Setup wird dann beendet, ohne CA ARCserve Backup zu installieren.

[Produktinformationen](#)

[Readme anzeigen](#)

Installieren

Abbrechen

Installation Erforderlicher Komponenten

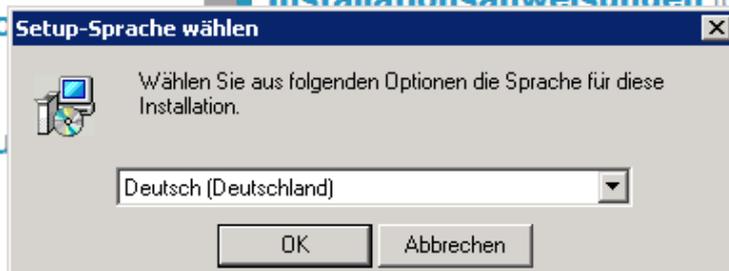
ca. ARCserve® Backup r15

Dokumentation

Supportinfo

Schulung

CD durchsu



- **Installation** von CA ARCserve Backup-Server und -Agenten für Windows.

- **Installationsanweisungen** für CA

- **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

CA ARCserve Backup-Setup

Lizenzschlüssel



- ✓ Lizenzvereinbarung
- **Lizenzschlüssel**
- Methoden
- Konfiguration
- Setup-Übersicht

Geben Sie an, wie Sie die Agenten und Optionen von CA ARCserve Backup lizenzieren möchten.

einen 25-stelligen Schlüssel (d. h. ABCDE - FGHIJ - KLMNO - PQRST - UVWXYZ)

Wenn Sie mehrere Komponenten installieren und daher mehrere Schlüsselcodes haben, geben Sie den Schlüsselcode für das Basisprodukt oder die Aktualisierung ein. Sie werden später während der Installation aufgefordert, die anderen Schlüssel einzugeben.



ein ALP-Zertifikat. Stellen Sie sicher, dass die Lizenz ordnungsgemäß angewendet wurde, um die Installation fortzusetzen.

eine Testversion. Wenn Sie keinen Schlüssel besitzen, klicken Sie auf 'Testversion' (<http://www.ca.com/trial>), um zu erfahren, wie Sie einen Schlüssel erhalten.

Um weitere Informationen zur Lizenzierung und Registrierung zu erhalten, klicken Sie [hier](#).

[Produktinformationen](#)
[Readme anzeigen](#)

Eingabe des gültigen Lizenzschlüssels für das Windows Standard Modul

CA ARCserve Backup-Setup

Methoden 

✓ Lizenzvereinbarung
✓ Lizenzschlüssel
➔ **Methoden**
Konfiguration
Setup-Übersicht

Geben Sie die Installationsmethode an, die Ihren Bedürfnissen entspricht.

 Lokal
Ermöglicht Ihnen die Installation und Aktualisierung von CA ARCserve Backup-Produkten auf diesem Computer.

 Remote
Ermöglicht Ihnen die Installation und Aktualisierung von CA ARCserve Backup-Produkten auf einem Remote-Computer.

 Antwortdatei erstellen
Ermöglicht Ihnen die Erstellung einer Antwortdatei, die bei einer eingabefreien, automatischen Installation verwendet wird.

[Produktinformationen](#)
[Readme anzeigen](#)

<Zurück Weiter> Abbrechen

Angabe der lokalen Installationsmethode

CA ARCserve Backup-Setup

Installationstyp 

- ✓ Lizenzvereinbarung
- ✓ Lizenzschlüssel
- ✓ Methoden
- **Konfiguration**
 - **Installationstyp**
 - Komponenten
 - Meldungen
 - Setup-Übersicht
 - Status der Installation
 - Installationsbericht

Ziel-Host: [IQSHBU01]

Geben Sie einen Installationstyp an

Express

Benutzerdefiniert

- ARCserve-Manager (Konsole)
- ARCserve-Standalone-Server 
- ARCserve-Primärserver 
- ARCserve-Mitgliedserver
- Anderer

Diese Option installiert einen ARCserve-Standalone-Server. Mit Hilfe eines ARCserve-Standalone-Servers können Sie lokale Jobs ausführen, verwalten und überwachen.

[Produktinformationen](#)
[Readme anzeigen](#)

<Zurück Weiter> Abbrechen

Angabe des Installationstyps (Standalone Server)

CA ARCserve Backup-Setup

Komponenten

Lizenzvereinbarung
 Lizenzschlüssel
 Methoden
 Konfiguration
 Installationstyp
 Komponenten
 Konten
 Datenbankeinstellungen
 Meldungen
 Setup-Übersicht
 Status der Installation
 Installationsbericht

[Produktinformationen](#)
[Readme anzeigen](#)

Ziel-Host: [IQSHBU01]

Komponenten:	Beschreibung:
<ul style="list-style-type: none"> CA ARCserve Backup <ul style="list-style-type: none"> Manager (Konsole) Server <ul style="list-style-type: none"> Standalone-Server <ul style="list-style-type: none"> Basis Tape Library Option Enterprise-Modul Disaster Recovery Option NDMP NAS Option Global Dashboard Client Agent für Windows für x64-basierte Systeme Agent für virtuelle Rechner für x64-basierte Systeme Agent for Open Files für Windows für x64-basierte Sys Setup-Dateien für die Agent-Bereitstellung Agent für Microsoft SQL Server für x64-basierte System Agent für Microsoft SharePoint für x64-basierte System Agent für Microsoft Exchange Server für x64-basierte : Agent für Oracle für x64-basierte Systeme 	<p>☀</p> <p>Installiert die Benutzeroberfläche (UI), um lokale Server und Remote-Server von CA ARCserve Backup auf Windows zu verwalten. Sie kann unabhängig von den Serverkomponenten installiert werden.</p> <p>Installiert die ARCserve-Dokumente. Zum Anzeigen der Dokumente benötigen Sie Adobe Acrobat.</p>

Für diese Funktion sind 448MB auf der Festplatte erforderlich. Info zur Festplatte

Installationspfad: Ordner ändern

Auswahl der entscheidenden Komponenten.

CA ARCserve Backup - Setup

Konten



- ✓ Lizenzvereinbarung
- ✓ Lizenzschlüssel
- ✓ Verfahren
- **Konfiguration**
 - ✓ Installationstyp
 - ✓ Komponenten
 - **Konten**
 - Meldungen
 - Setup-Übersicht
 - Status der Installation
 - Installationsbericht

[Produktinformationen](#)

[Readme anzeigen](#)

Ziel-Host: [IQSHBU01]

Geben Sie ein Windows-Administratorkonto an

Microsoft Windows-Domäne: [IQSHBU01]

Microsoft Windows-Benutzername: [Administrator]

Kennwort: [*****]

Geben Sie ein CA ARCserve Backup-Domänenkonto an

CA ARCserve Backup-Domäne: [IQSHBU01]

CA ARCserve Backup-Server: [IQSHBU01]

Benutzername: [caroot]

Kennwort: [*****]

Kennwort bestätigen: [*****]

Kennwort speichern

<Zurück Weiter Abbrechen

Angabe der Sicherungskonten.

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

CA ARCserve Backup - Setup

Datenbankeinstellungen



- ✓ Lizenzvereinbarung
- ✓ Lizenzschlüssel
- ✓ Verfahren
- **Konfiguration**
 - ✓ Installationstyp
 - ✓ Komponenten
 - ✓ Konten
 - **Datenbankeinstellungen**
- Meldungen
- Setup-Übersicht
- Status der Installation
- Installationsbericht

[Produktinformationen](#)
[Readme anzeigen](#)

Ziel-Host: [IQSHBU01]

Wählen Sie einen Datenbanktyp: **ARCserve-Standarddatenbank**

Installationspfad für die Standarddatenbank von CA ARCserve [ASDB] angeben

Standardinstallationspfad: C:\Program Files (x86)\Microsoft SQL Server
 Benutzerdef. Pfad: []

Datendateipfad für ARCserve-Standarddatenbank

Standardinstallationspfad: C:\Program Files (x86)\Microsoft SQL Server\MSSQL10.ARCSEVERE_DB\MSSQL\DATA
 Benutzerdef. Pfad: []

Einstellung für SQL-Sprachensortierung

Standardsortierung
 Ostasiatische Sprachen: Chinese_PRC

Inst.-Pfad für Katalogdateien: C:\Program Files (x86)\CA\ARCserve Backup\CATALOG.DB\

<Zurück Weiter Abbrechen

Angabe der Datenbankeinstellungen

CA ARCserve Backup-Setup

Meldungen 

- ✓ Lizenzvereinbarung
- ✓ Lizenzschlüssel
- ✓ Methoden
- **Konfiguration**
 - ✓ Installationstyp
 - ✓ Komponenten
 - ✓ Konten
 - ✓ Datenbankeinstellungen
 - **Meldungen**
- Setup-Übersicht
- Status der Installation
- Installationsbericht

[Produktinformationen](#)
[Readme anzeigen](#)

Ziel-Host: [IQSHBU01]

 Lesen Sie vor der Installation die folgenden Warnhinweise:

- Setup installiert die folgenden Komponenten:
 - Microsoft SQL Server Express Edition
 - Microsoft .NET Framework 3.5 Service Pack 1
 - Microsoft XML Core Services (MSXML)
 - Java Runtime Environment (JRE)
 - eTrust Threat Management Agent 8.1 (x64)
- Das vorhandene Produkt "Microsoft SQL Server Native Client" auf dem Zielrechner führt möglicherweise dazu, dass das Setup für "Microsoft SQL Server 2008 Express Edition" fehlschlägt. Um dieses Problem zu vermeiden, deinstallieren Sie "Microsoft SQL Server Native Client" über "Programme hinzufügen/entfernen".

[Drucken](#)

<Zurück Weiter> Abbrechen

Zusammenfassung

CA ARCserve Backup-Setup

Status der Installation
Setup kopiert die Dateien auf die Festplatte. Bitte warten.

[Lizenzvereinbarung](#)
[Lizenzschlüssel](#)
[Methoden](#)
[Konfiguration](#)
 [Installationstyp](#)
 [Komponenten](#)
 [Konten](#)
 [Datenbankeinstellungen](#)
 [Meldungen](#)
[Setup-Übersicht](#)
 → Status der Installation
 Installationsbericht

Setup installiert die folgenden Komponenten auf Ihrem Rechner, um CA ARCserve Backup installieren zu können.

Komponentenname	Status
CA-Lizenz 1.9.1	Installation wird durchg...
Microsoft SQL Server 2008 Express Edition	Ausstehend
eTrust Threat Management Agent 8.1 (x64)	Ausstehend
CA ARCserve Backup - Setup-Unterstützungsdateien	Ausstehend
CAPKI (x86)	Ausstehend
CAPKI (x64)	Ausstehend
CA ARCserve Discovery Service	Ausstehend
CA ARCserve Universal Agent (x64)	Ausstehend

Setup installiert CA-Lizenz 1.9.1 auf Ihrem Rechner.

[Produktinformationen](#)
[Readme anzeigen](#)

Durchführung der Installation.

CA ARCserve Backup-Setup

Firewall-Registrierung 

→ Firewall-Registrierung

ARCserve muss die folgenden Dienste/Programme als Ausnahmen in Windows Firewall registrieren.

Dienst und Programm	Status	Pfad
CASDBEngine	wird als Firewall-Ausnahme hinzugefügt	C:\Program Files (x86)\CA\ARCserve Bac...
CASDiscovery	wird als Firewall-Ausnahme hinzugefügt	C:\Program Files (x86)\CA\SharedCompo...
CASJobEngine	wird als Firewall-Ausnahme hinzugefügt	C:\Program Files (x86)\CA\ARCserve Bac...
CASMessageEngine	wird als Firewall-Ausnahme hinzugefügt	C:\Program Files (x86)\CA\ARCserve Bac...
CASMgmtSvc	wird als Firewall-Ausnahme hinzugefügt	C:\Program Files (x86)\CA\ARCserve Bac...
CASportmapper	wird als Firewall-Ausnahme hinzugefügt	C:\Program Files (x86)\CA\SharedCompo...
CASvcControlSvr	wird als Firewall-Ausnahme hinzugefügt	C:\Program Files (x86)\CA\ARCserve Bac...
CASTaskEngine	wird als Firewall-Ausnahme hinzugefügt	C:\Program Files (x86)\CA\ARCserve Bac...

Setup darf ARCserve-Dienste/-Programme als Ausnahmen in Windows Firewall registrieren.

Wählen Sie den Netzwerkstandorttyp:

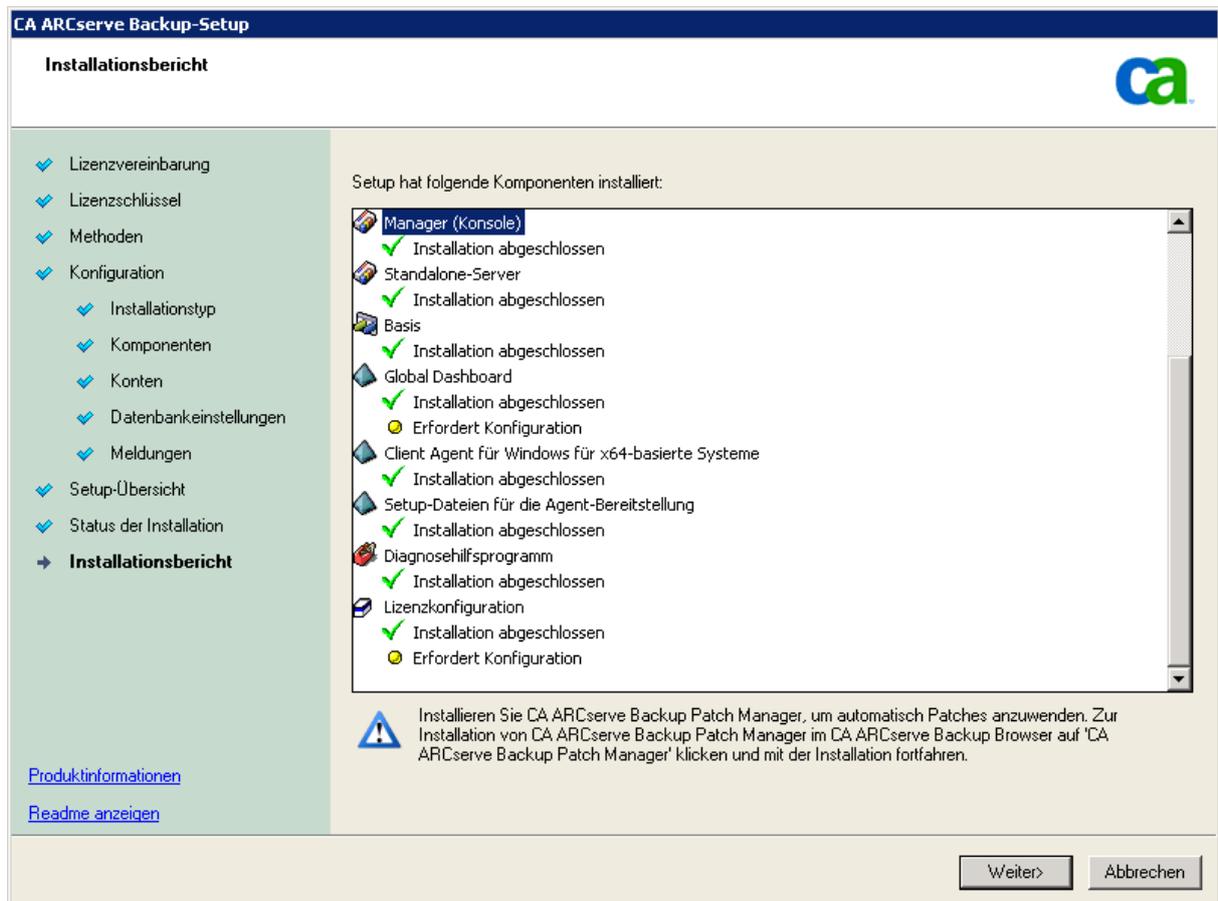
Domäne: Netzwerke am Arbeitsplatz, die zu einer Domäne gehören
 Heim/Arbeit (Privat): Heim- oder Arbeitsplatznetzwerke mit Personen und Geräten, die bekannt und vertrauenswürdig sind
 Öffentlich: Netzwerke an öffentlichen Orten, beispielsweise Flughäfen oder Cafés

Registrieren der ARCserve-Dienste/-Programme als Ausnahmen in Windows Firewall überspringen.

 **Vorsicht!** Wenn Sie diesen Schritt überspringen, wird CA ARCserve Backup möglicherweise nicht ordnungsgemäß kommunizieren.

[Produktinformationen](#)
[Readme anzeigen](#)

Registrierung in der Windows Firewall



CA ARCserve Backup-Setup

Installationsbericht

Setup hat folgende Komponenten installiert:

- Manager (Konsole)
 - ✓ Installation abgeschlossen
- Standalone-Server
 - ✓ Installation abgeschlossen
- Basis
 - ✓ Installation abgeschlossen
- Global Dashboard
 - ✓ Installation abgeschlossen
 - Erfordert Konfiguration
- Client Agent für Windows für x64-basierte Systeme
 - ✓ Installation abgeschlossen
- Setup-Dateien für die Agent-Bereitstellung
 - ✓ Installation abgeschlossen
- Diagnosehilfsprogramm
 - ✓ Installation abgeschlossen
- Lizenzkonfiguration
 - ✓ Installation abgeschlossen
 - Erfordert Konfiguration

⚠ Installieren Sie CA ARCserve Backup Patch Manager, um automatisch Patches anzuwenden. Zur Installation von CA ARCserve Backup Patch Manager im CA ARCserve Backup Browser auf 'CA ARCserve Backup Patch Manager' klicken und mit der Installation fortfahren.

[Produktinformationen](#)
[Readme anzeigen](#)

Weiter> Abbrechen

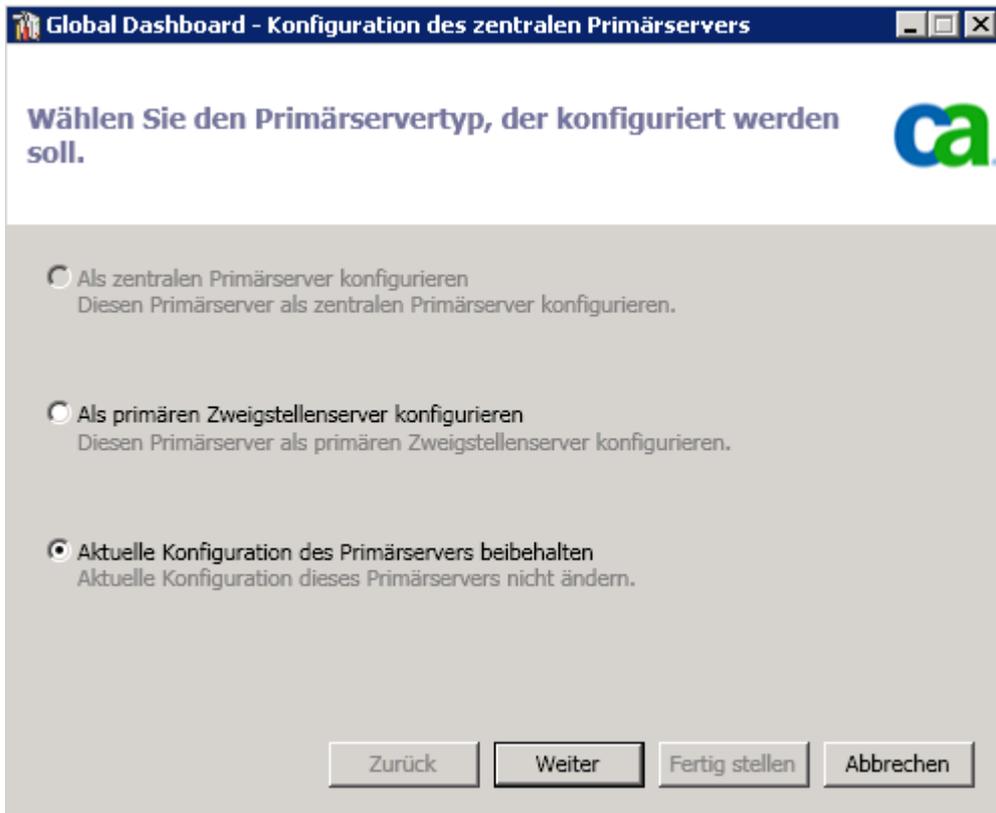
Installationsbericht

(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



Global Dashboard - Konfiguration des zentralen Primärserver

Wählen Sie den Primärservertyp, der konfiguriert werden soll.

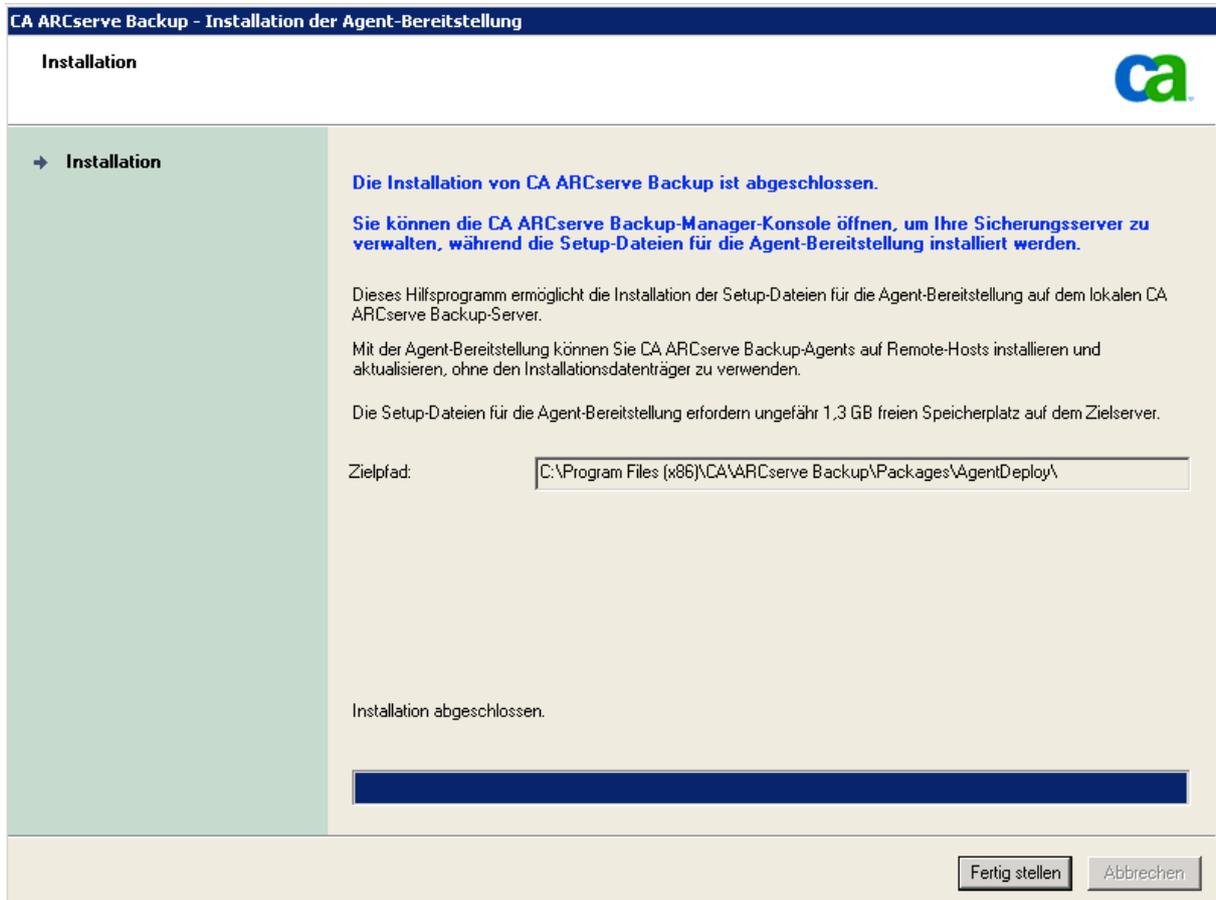
Als zentralen Primärserver konfigurieren
Diesen Primärserver als zentralen Primärserver konfigurieren.

Als primären Zweigstellenserver konfigurieren
Diesen Primärserver als primären Zweigstellenserver konfigurieren.

Aktuelle Konfiguration des Primärserver beibehalten
Aktuelle Konfiguration dieses Primärserver nicht ändern.

Zurück Weiter Fertig stellen Abbrechen

6.2.3 Abschluss der Installation



The screenshot shows a Windows-style dialog box titled "CA ARCserve Backup - Installation der Agent-Bereitstellung". The window has a dark blue header bar with the title. Below the header, the word "Installation" is displayed in the top left corner, and the CA logo is in the top right corner. A vertical sidebar on the left contains a green arrow pointing to the word "Installation". The main content area has a light beige background and contains the following text:

Die Installation von CA ARCserve Backup ist abgeschlossen.

Sie können die CA ARCserve Backup-Manager-Konsole öffnen, um Ihre Sicherungsserver zu verwalten, während die Setup-Dateien für die Agent-Bereitstellung installiert werden.

Dieses Hilfsprogramm ermöglicht die Installation der Setup-Dateien für die Agent-Bereitstellung auf dem lokalen CA ARCserve Backup-Server.

Mit der Agent-Bereitstellung können Sie CA ARCserve Backup-Agents auf Remote-Hosts installieren und aktualisieren, ohne den Installationsdatenträger zu verwenden.

Die Setup-Dateien für die Agent-Bereitstellung erfordern ungefähr 1,3 GB freien Speicherplatz auf dem Zielsystem.

Zielpfad:

Installation abgeschlossen.

At the bottom right of the dialog box, there are two buttons: "Fertig stellen" and "Abbrechen".

6.3 Installation ARCserve Backup r15 auf Server 2003 // R2

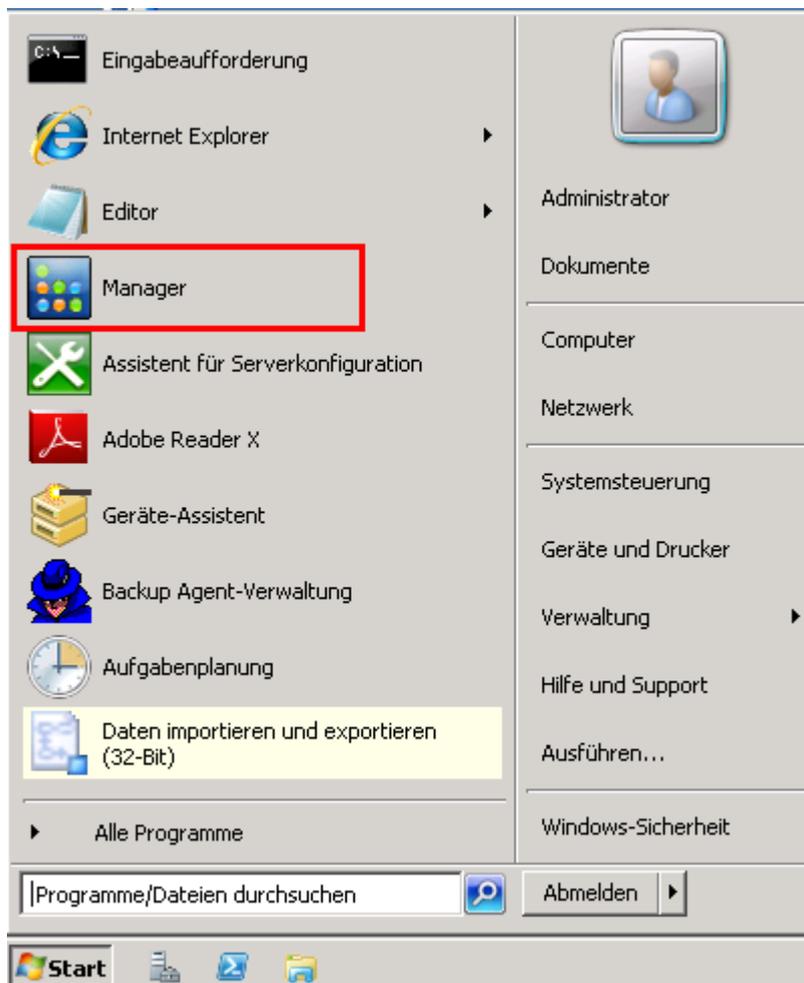
Die Installation unter Server 2003 / R2 unterscheidet sich nicht. Voraussetzung ist ein aktueller Updatestand des Hostsystems.

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



CA ARCserve Backup - [Startseite]

Datei Schnellstart Ansicht Fenster Hilfe

ARCserve® BACKUP Meine erste Sicherung

Willkommen Grundlagen **Geräte** Erste Sicherung Erste Wiederherstellung Fertig stellen

Willkommen!

Willkommen beim Lernprogramm **Meine erste Sicherung**. Dieses Lernprogramm vermittelt grundlegende Informationen zu CA ARCserve® Backup und bietet eine erste Annäherung an den CA ARCserve Backup-Manager, mit dem Sie Ihre erste Sicherung einstellen werden.

Dieses Lernprogramm enthält die folgenden Themen, die am oberen Rand Ihres Bildschirms in Form von Registerkarten angeordnet sind:

- **Grundlagen** - Erläuterung der Konzepte zur Datensicherung
- **Geräte** - Ermöglicht die Erstellung von datenträgerbasierten Geräten zur Sicherung von Daten
- **Erste Sicherung** - Erläuterung des Sicherungs-Managers, mit dem Sie Ihren ersten Sicherungsjob erstellen
- **Erste Wiederherstellung** - Erläuterung der Wiederherstellung von gesicherten Daten

Mit diesem Lernprogramm können Sie ein Gerät erstellen und anschließend in nur wenigen Minuten einen normalen Sicherungsjob aufbauend auf die Standardeinstellungen festlegen.

Verwenden Sie die Schaltflächen 'Zurück' und 'Weiter', um im Lernprogramm zu navigieren. Klicken Sie auf die Schaltfläche 'Lernprogramm beenden', um auf die **Startseite** von CA ARCserve Backup zurückzukehren.

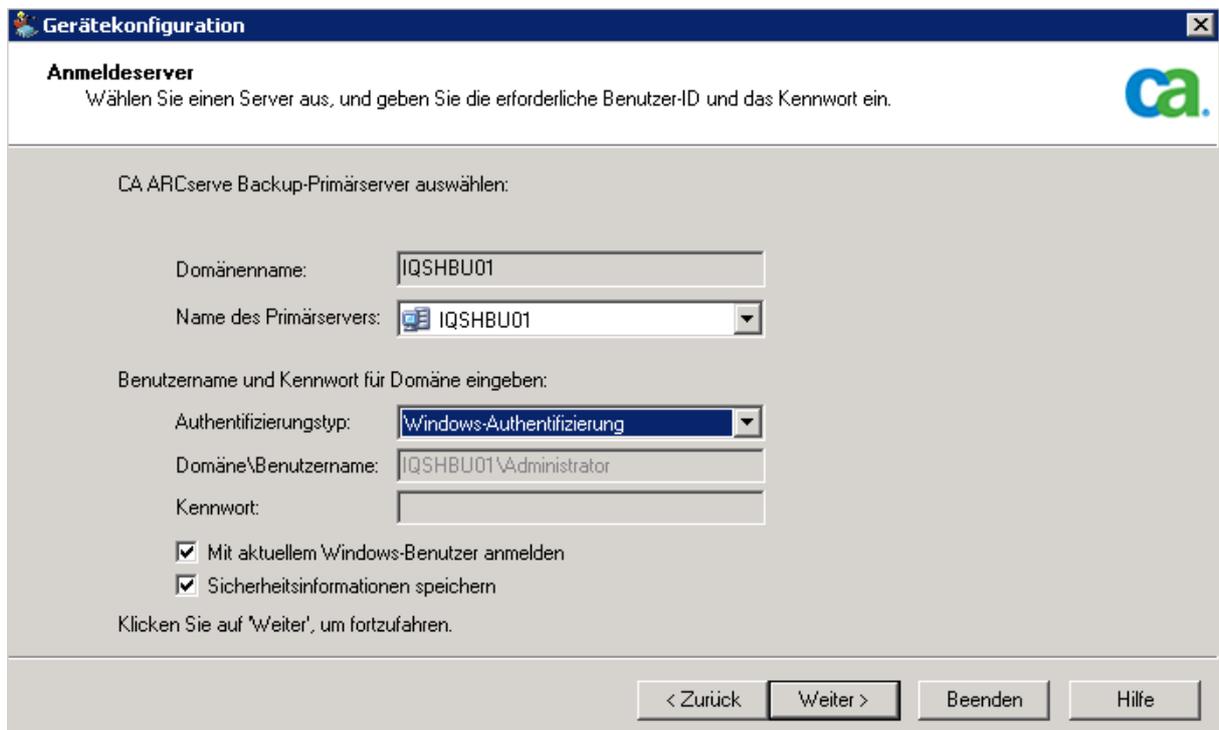
Zeigen Sie mit dem Mauszeiger auf die **grün markierten und kursiv formatierten** Wörter, um die Definition eines Begriffs anzuzeigen.

Klicken Sie in den Fenstern des Lernprogramms auf die Links im Abschnitt 'Erfahren Sie mehr', die sich am rechten Rand Ihres Bildschirms befinden, um mehr Informationen zum Thema zu erhalten.

Erfahren Sie mehr:

- Was ist CA ARCserve Backup?
- Lernen Sie mehr über die Funktionen des Produkts

Start der Sicherungseinrichtung (Einrichtung der Geräte / des Gerätes)



Gerätekonfiguration

Anmeldeserver

Wählen Sie einen Server aus, und geben Sie die erforderliche Benutzer-ID und das Kennwort ein.

CA ARCserve Backup-Primärservers auswählen:

Domänenname:

Name des Primärservers:

Benutzername und Kennwort für Domäne eingeben:

Authentifizierungstyp:

Domäne\Benutzername:

Kennwort:

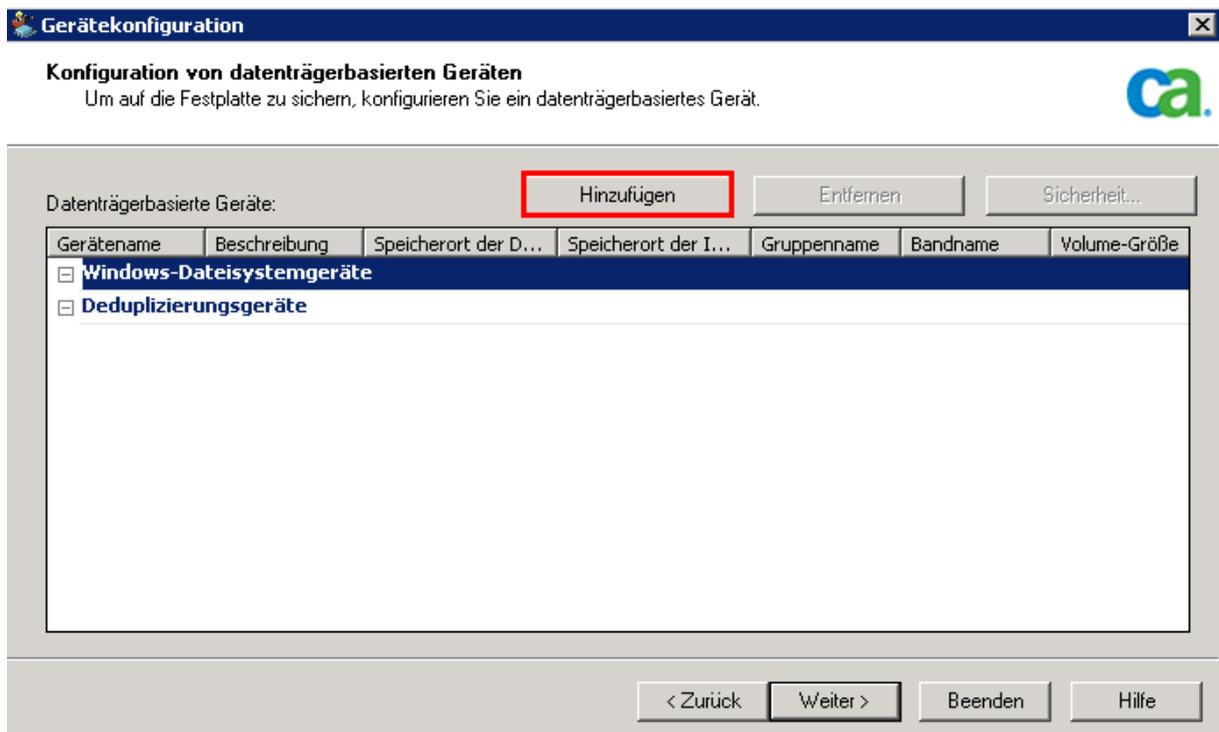
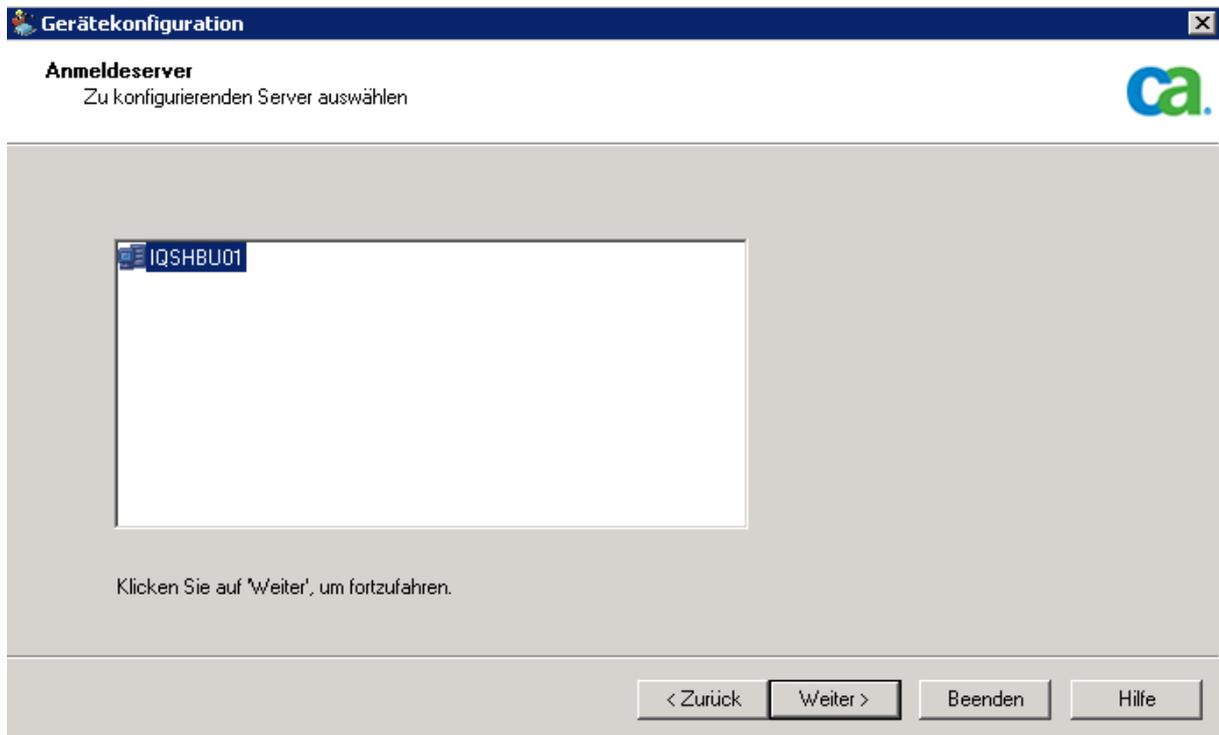
Mit aktuellem Windows-Benutzer anmelden

Sicherheitsinformationen speichern

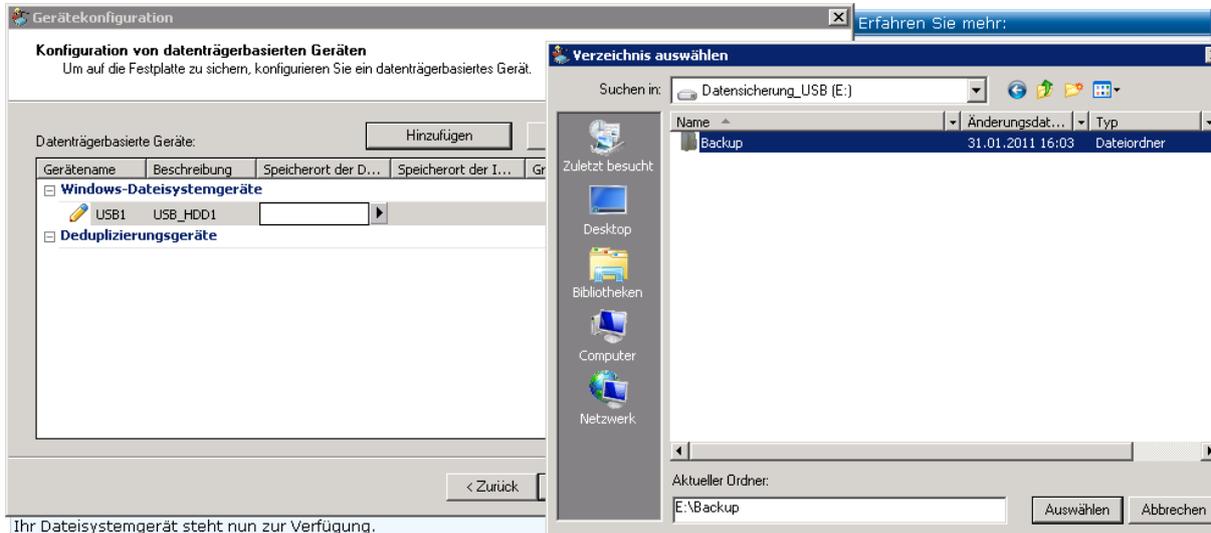
Klicken Sie auf 'Weiter', um fortzufahren.

< Zurück Weiter > Beenden Hilfe

Festlegend der Anmeldeinformation



Ersteinrichtung des Datensicherungsgerätes



Konfiguration von datenträgerbasierten Geräten
Um auf die Festplatte zu sichern, konfigurieren Sie ein datenträgerbasiertes Gerät.

Datenträgerbasierte Geräte: Hinzufügen

Gerätename	Beschreibung	Speicherort der D...	Speicherort der I...	Gr...
Windows-Dateisystemgeräte				
USB1	USB_HDD1			
Deduplizierungsgeräte				

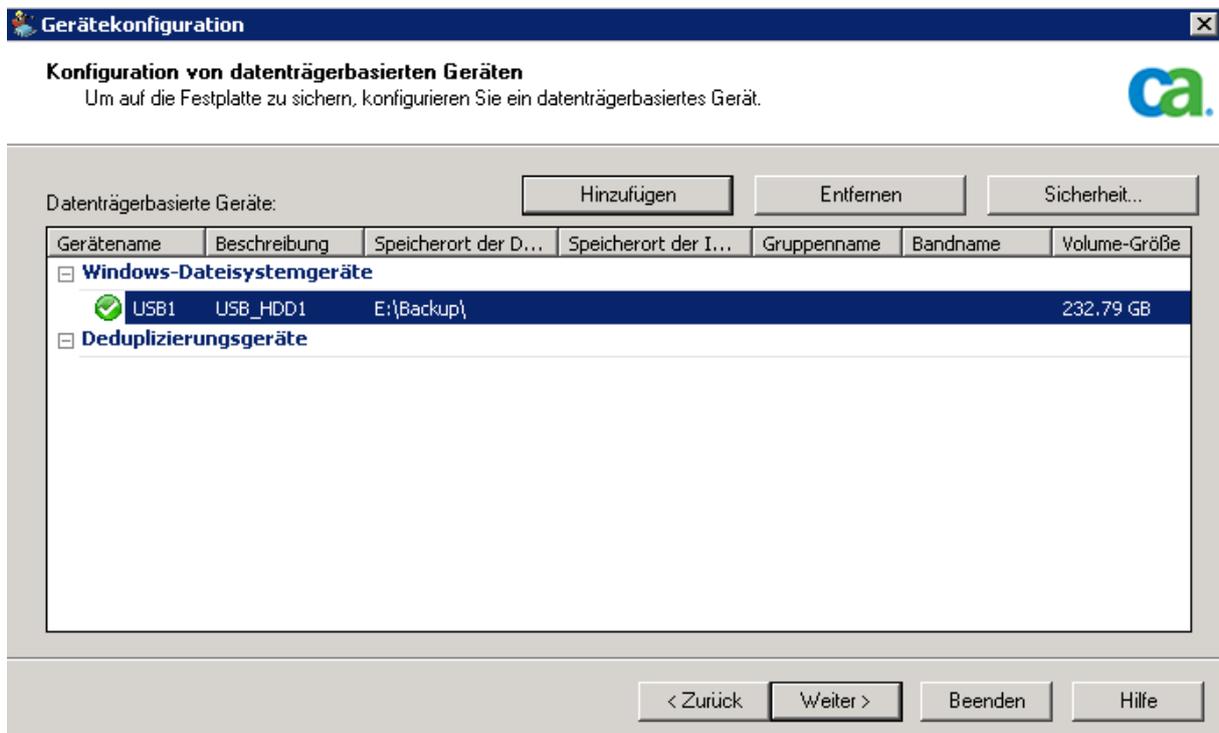
Ihr Dateisystemgerät steht nun zur Verfügung.

Verzeichnis auswählen
Suchen in: Datensicherung_USB (E:)

Name	Änderungsdat...	Typ
Backup	31.01.2011 16:03	Dateiordner

Aktueller Ordner: E:\Backup Auswählen Abbrechen

Beschreibung und Auswahl des Speicherortes auf der USB Festplatte.

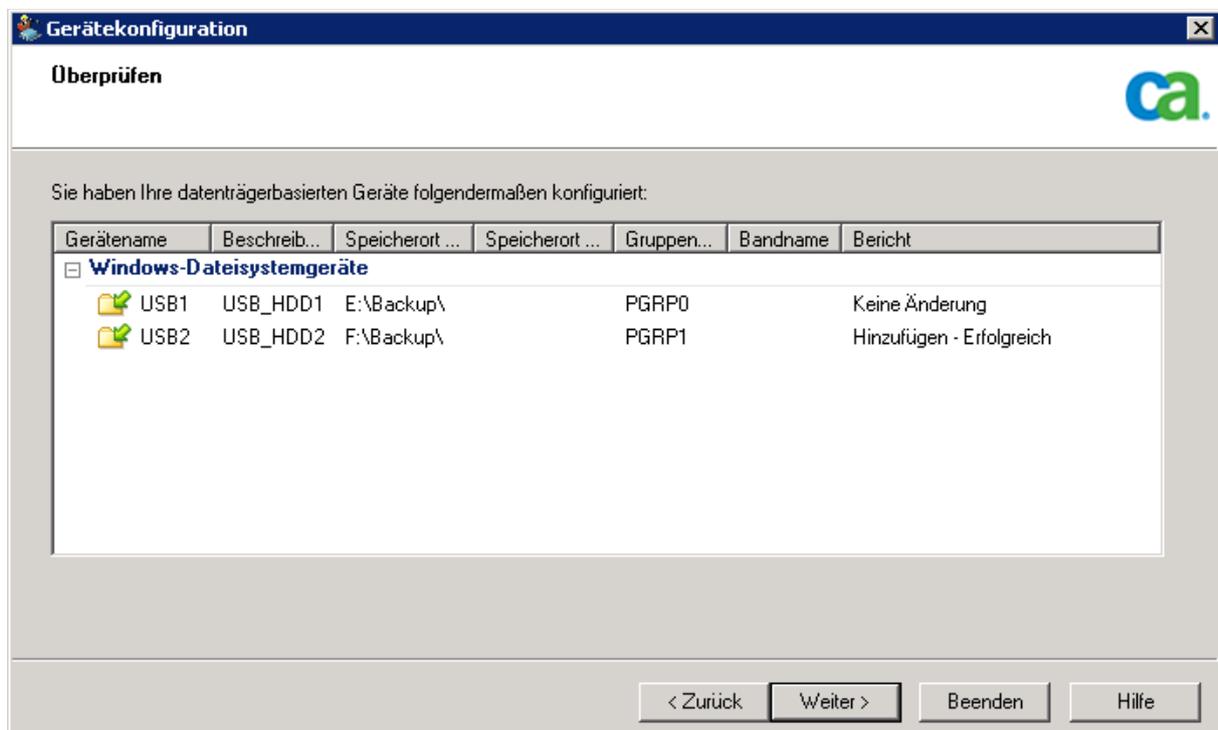
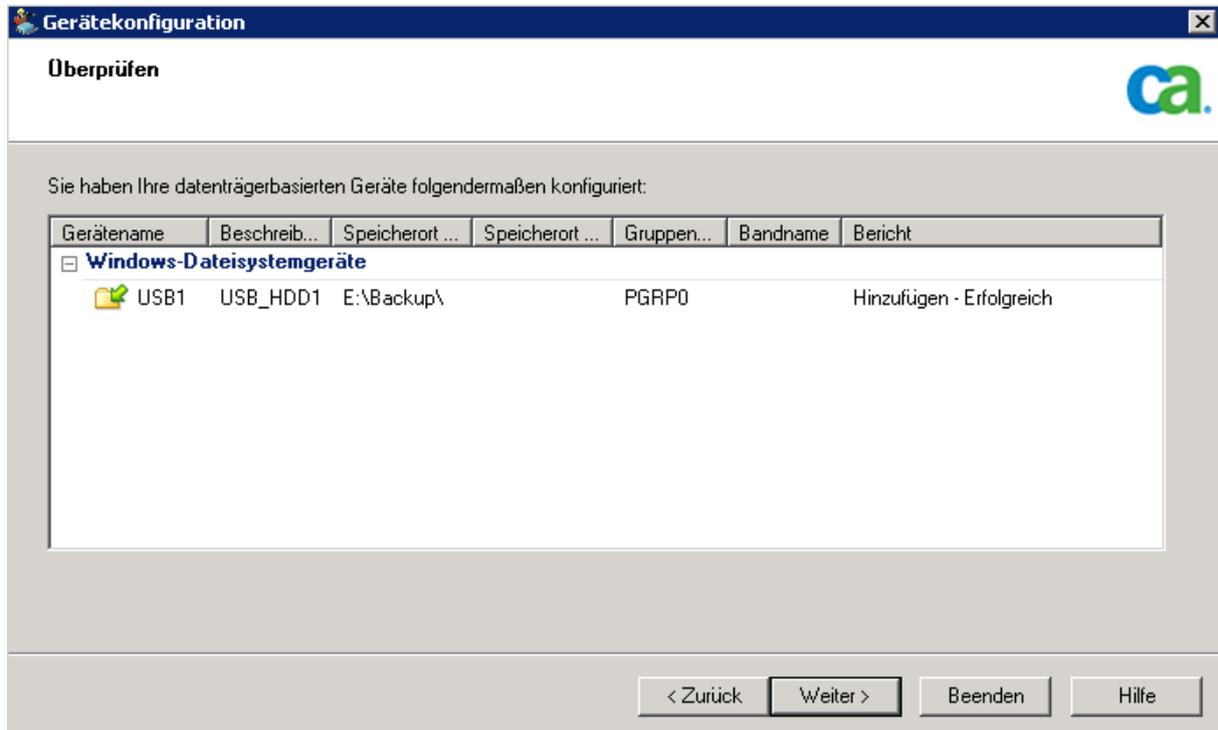


Konfiguration von datenträgerbasierten Geräten
Um auf die Festplatte zu sichern, konfigurieren Sie ein datenträgerbasiertes Gerät.

Datenträgerbasierte Geräte: Hinzufügen Entfernen Sicherheit...

Gerätename	Beschreibung	Speicherort der D...	Speicherort der I...	Gruppenname	Bandname	Volume-Größe
Windows-Dateisystemgeräte						
✓ USB1	USB_HDD1	E:\Backup\				232.79 GB
Deduplizierungsgeräte						

< Zurück Weiter > Beenden Hilfe



Hinzufügen einer weiteren USB Festplatte. Die Schritte sind indentisch.

Job Band DB
Übergeben Optionen Filter Ansicht

Starten Quelle Ablaufplan Ziel

Sicherungstyp auswählen
 Normale Sicherung
 Deduplizierungssicherung
 UNIX/Linux Data Mover-Sicherung

Staging aktivieren
 Ermöglicht die Konfiguration von Staging-Sicherungsjobs. Wenn Sie diese Option aktivieren, werden die Registerkarten 'Staging-Speicherort' und 'Migrationsrichtlinie' angezeigt.

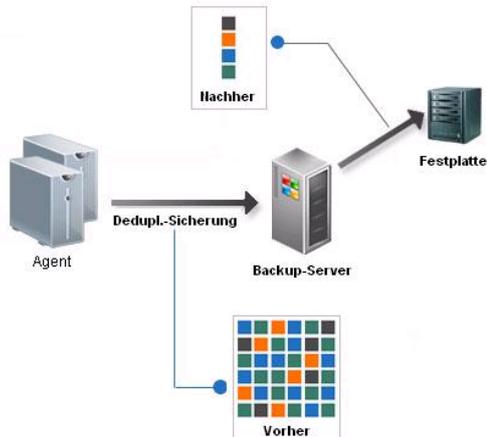



Funktionsweise der Dateneduplizierung

Die Technologie der *Dateneduplizierung* ermöglicht es Ihnen, mehr Sicherungen auf demselben physischen Datenträger unterzubringen, Sicherungen über einen längeren Zeitraum hinweg aufzubewahren und die Wiederherstellung von Daten zu beschleunigen. Die Deduplizierung analysiert die zu sichernden Datenströme, sucht nach doppelten Datenblöcken und speichert nur die einfach vorkommenden Datenblöcke auf dem Datenträger. Die Duplikate werden in speziellen Indexdateien nachverfolgt.

Die Deduplizierung wird in CA ARCserve Backup als Inline-Vorgang in einer zusammenhängenden Sitzung auf dem Sicherungsserver ausgeführt. Wenn Sie Redundanzen zwischen Sicherungsjobs ermitteln möchten, die von den Stammverzeichnissen zweier verschiedener Computer durchgeführt wurden, verwenden Sie die *globale Deduplizierung*.

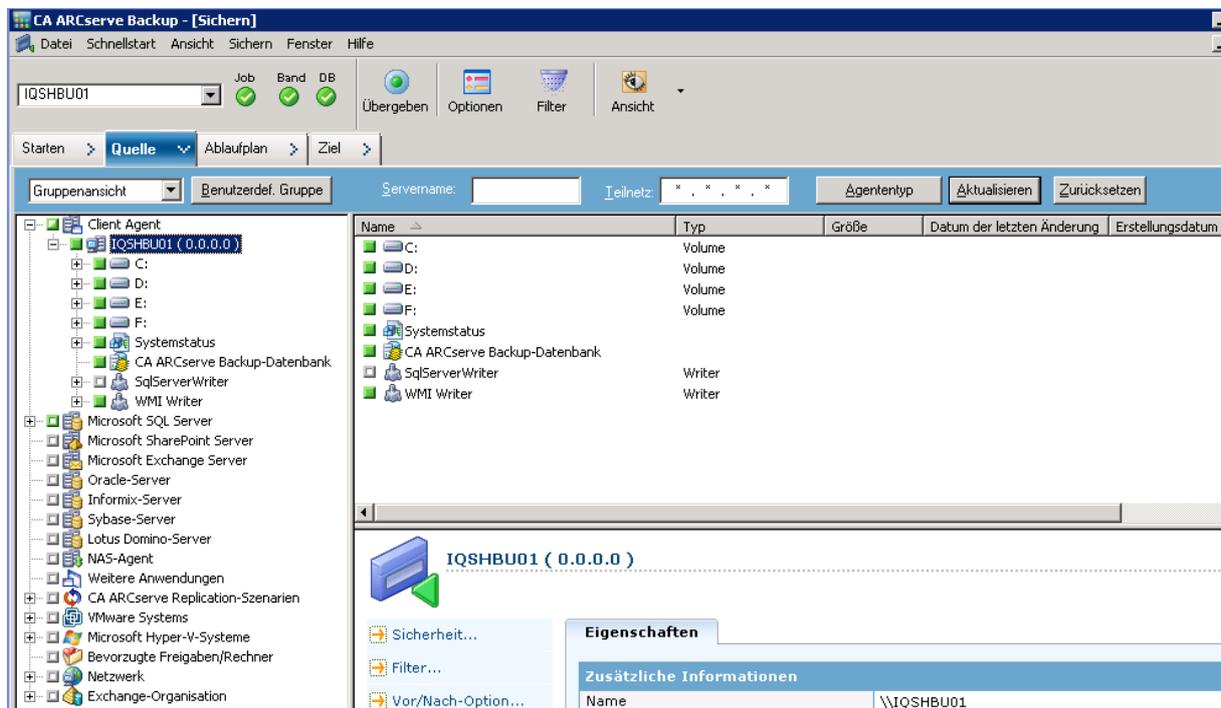
Durch die Deduplizierung werden für jede Sicherungssitzung drei Dateien erstellt:



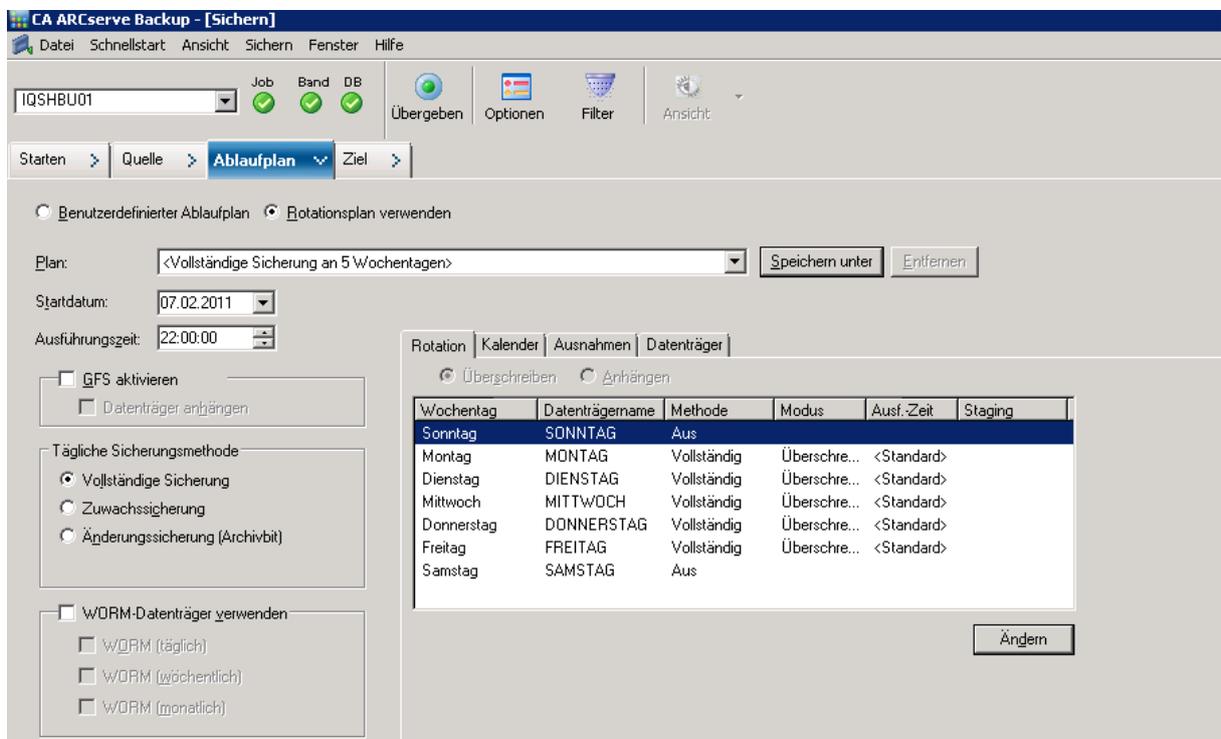
Auswahl der Dateneduplizierung* (Eine Optimierungsmöglichkeit für die Schulen)

*Deduplizierungssicherung

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

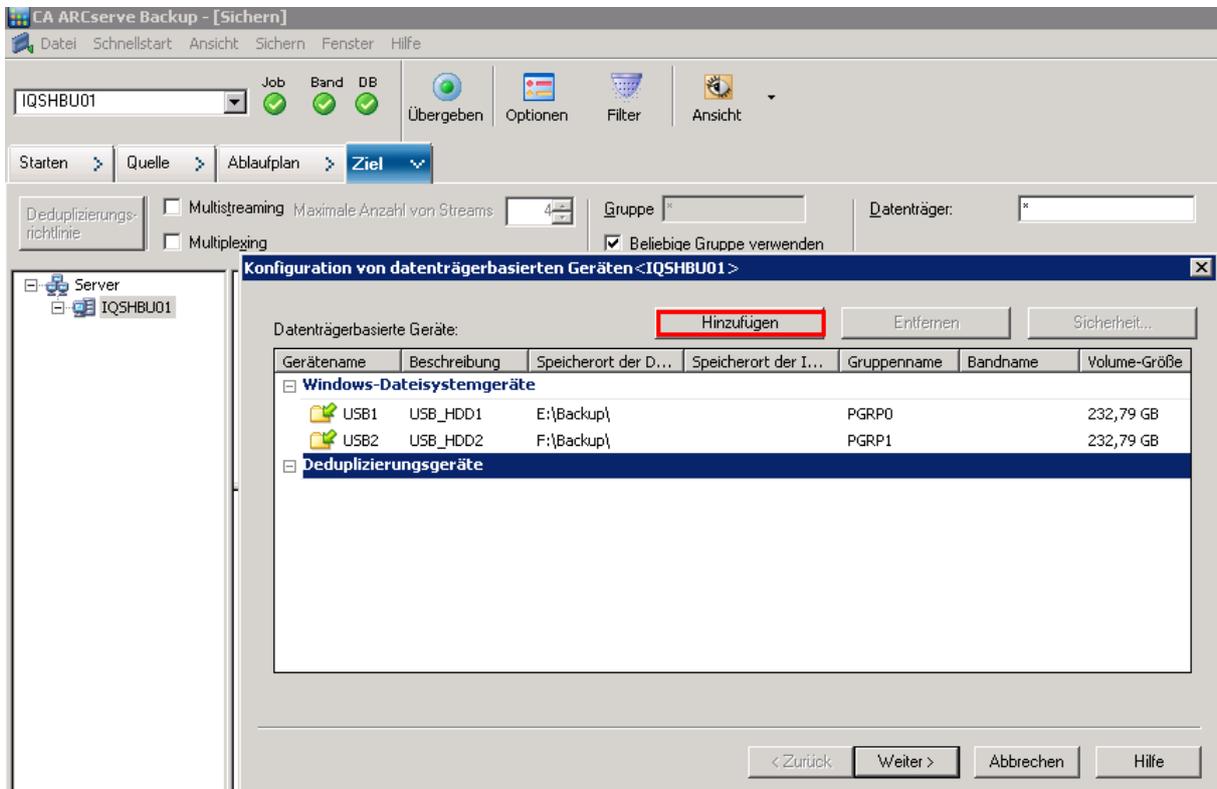


Individuelle Auswahl der zu sichernden Dateien. (Beispiel: Gesamtsicherung)

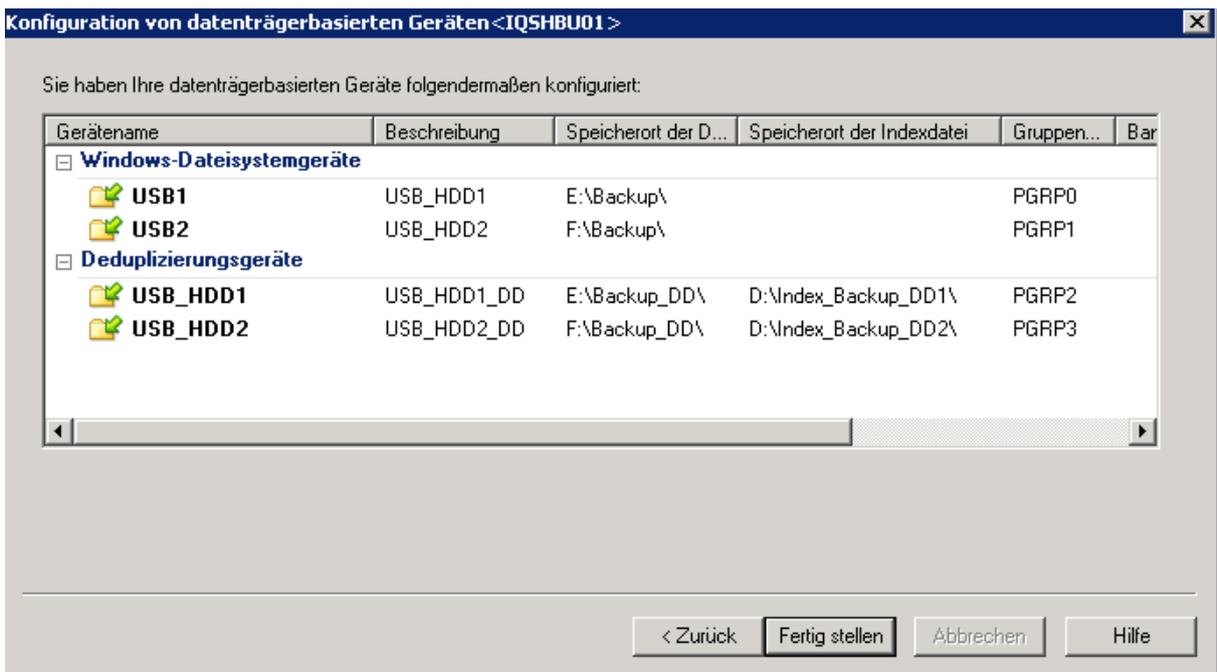


Wochentag	Datenträgername	Methode	Modus	Ausf.-Zeit	Staging
Sonntag	SONNTAG	Aus			
Montag	MONTAG	Vollständig	Überschre...	<Standard>	
Dienstag	DIENSTAG	Vollständig	Überschre...	<Standard>	
Mittwoch	MITTWOCH	Vollständig	Überschre...	<Standard>	
Donnerstag	DONNERSTAG	Vollständig	Überschre...	<Standard>	
Freitag	FREITAG	Vollständig	Überschre...	<Standard>	
Samstag	SAMSTAG	Aus			

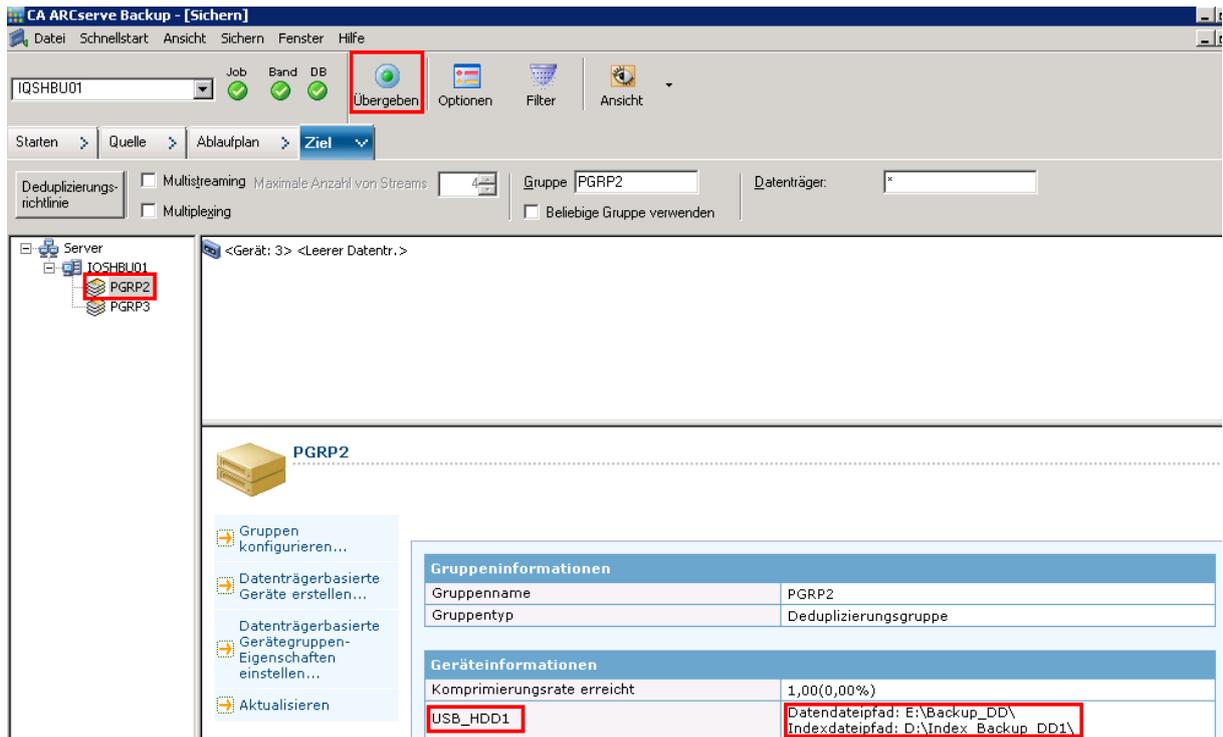
Erstellen eines Rotations- Sicherungszeitplans. (Auswahl der Vollständigen Sicherung)



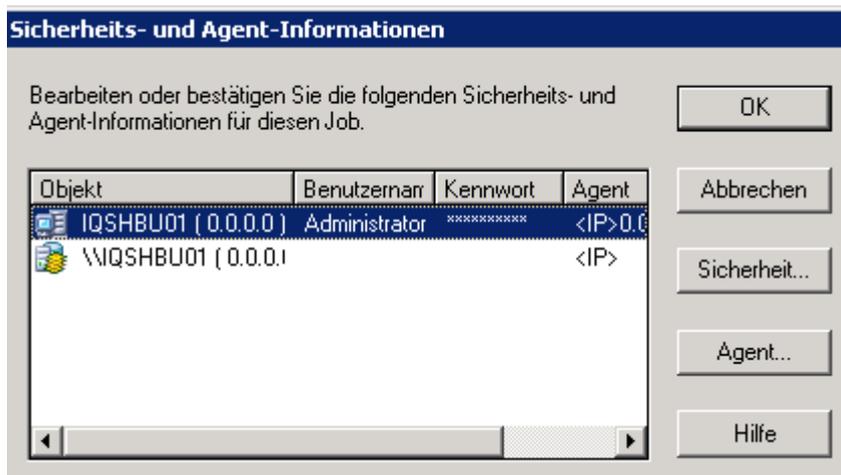
Hinzufügen der Deduplizierungsgeräte



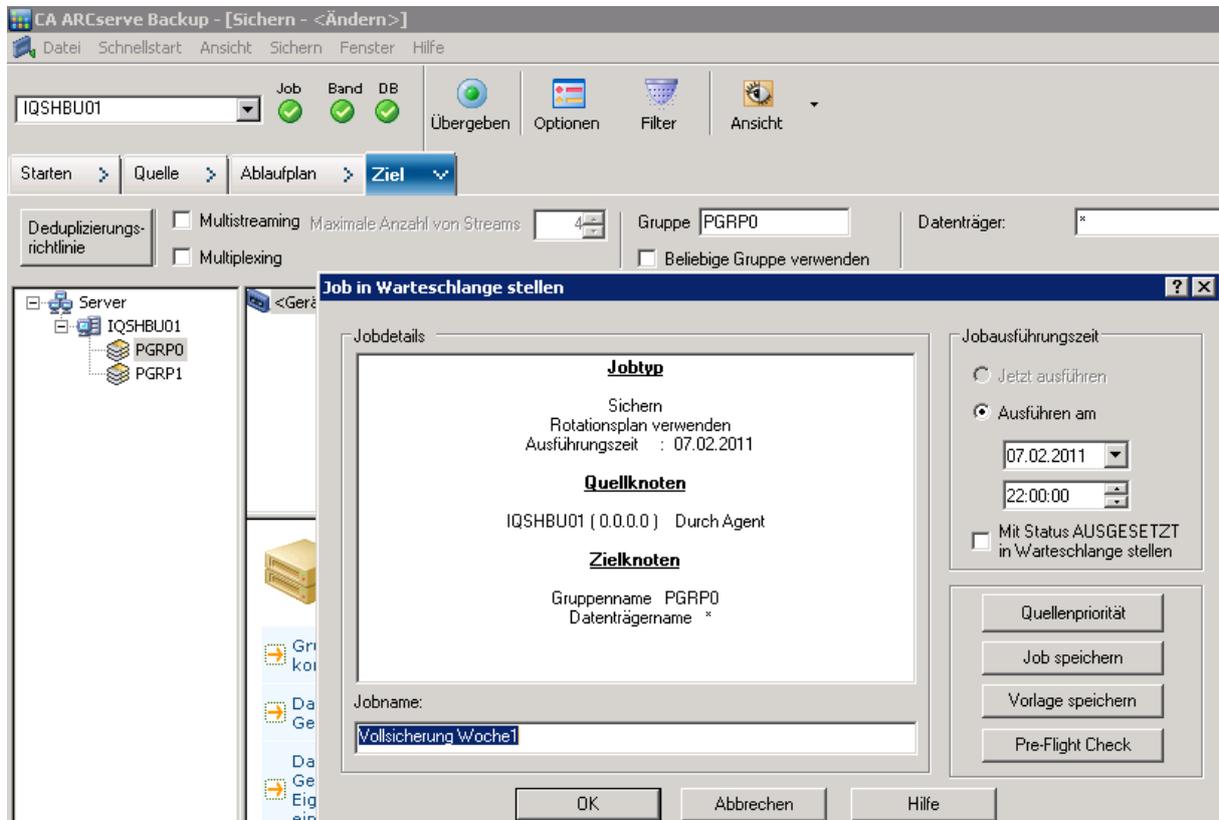
Zusammenfassung der erstellten Deduplizierungsorte. Die gewählten Ordner werden im Vorwege auf den USB Festplatten angelegt. **(Siehe 4.2.1)**



Übergabe des ersten Sicherungsjobs auf angelegter USB_HDD1

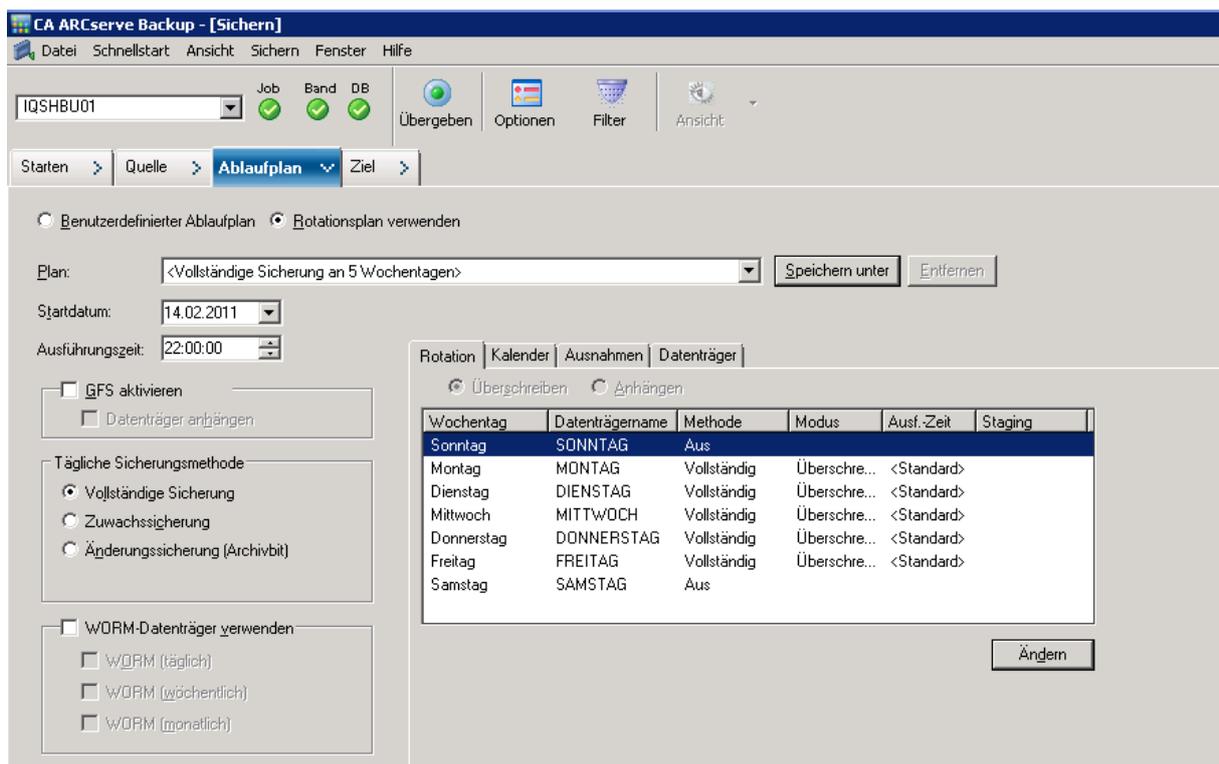


Auswahl des Sicherungsoperators.



The screenshot shows the 'Job in Warteschlange stellen' (Queue Job) dialog box in the CA ARCserve Backup software. The 'Jobtyp' (Job Type) is 'Sichern' (Backup) with 'Rotationsplan verwenden' (Use rotation plan) selected. The execution date is set to 07.02.2011 at 22:00:00. The 'Quellknoten' (Source node) is 'IQSHBU01 (0.0.0.0) Durch Agent' and the 'Zielknoten' (Target node) is 'Gruppenname PGRP0, Datenträgername *'. The 'Jobname' is 'Vollsicherung Woche1'. The 'Jobausführungszeit' (Job execution time) options are 'Jetzt ausführen' (Execute now) and 'Ausführen am' (Execute on), with the latter selected. Other options include 'Mit Status AUSGESETZT in Warteschlange stellen' (Queue with status OUT) and buttons for 'Quellenpriorität', 'Job speichern', 'Vorlage speichern', and 'Pre-Flight Check'. The 'OK', 'Abbrechen', and 'Hilfe' buttons are at the bottom.

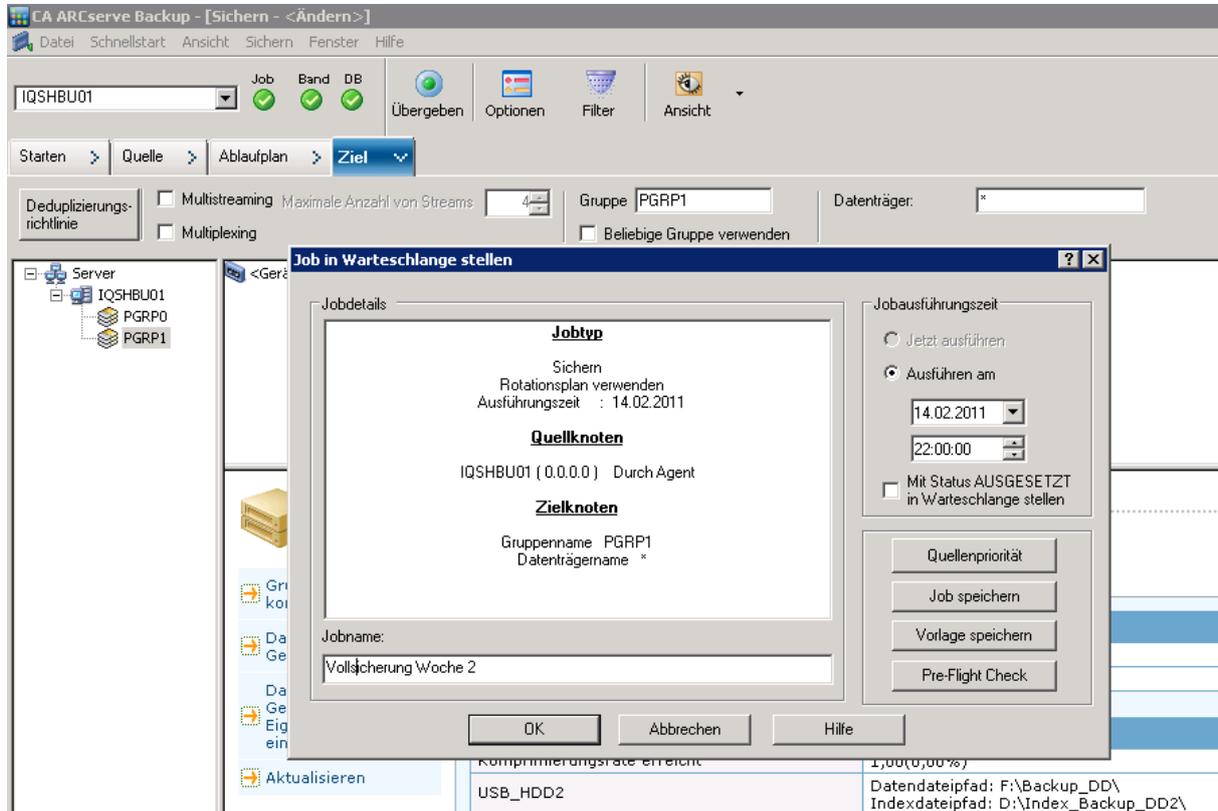
Sicherungszeitplan übergeben und in Warteschlange stellen.



The screenshot shows the 'Ablaufplan' (Schedule) configuration screen in the CA ARCserve Backup software. The 'Plan' is '<Vollständige Sicherung an 5 Wochentagen>' (Full backup on 5 weekdays). The 'Startdatum' (Start date) is 14.02.2011 and the 'Ausführungszeit' (Execution time) is 22:00:00. The 'Tägliche Sicherungsmethode' (Daily backup method) is 'Vollständige Sicherung' (Full backup). The 'WORM-Datenträger verwenden' (Use WORM media) options are 'WORM (täglich)', 'WORM (wöchentlich)', and 'WORM (monatlich)'. The 'Rotation' tab is active, showing a table of backup rotation details.

Wochentag	Datenträgername	Methode	Modus	Ausf.-Zeit	Staging
Sonntag	SONNTAG	Aus			
Montag	MONTAG	Vollständig	Überschre...	<Standard>	
Dienstag	DIENSTAG	Vollständig	Überschre...	<Standard>	
Mittwoch	MITTWOCH	Vollständig	Überschre...	<Standard>	
Donnerstag	DONNERSTAG	Vollständig	Überschre...	<Standard>	
Freitag	FREITAG	Vollständig	Überschre...	<Standard>	
Samstag	SAMSTAG	Aus			

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



Job in Warteschlange stellen

Jobtyp
Sichern
Rotationsplan verwenden
Ausführungszeit : 14.02.2011

Quellknoten
IQSHBU01 (0.0.0.0) Durch Agent

Zielknoten
Gruppenname PGRP1
Datenträgername *

Jobname:
Vollsicherung Woche 2

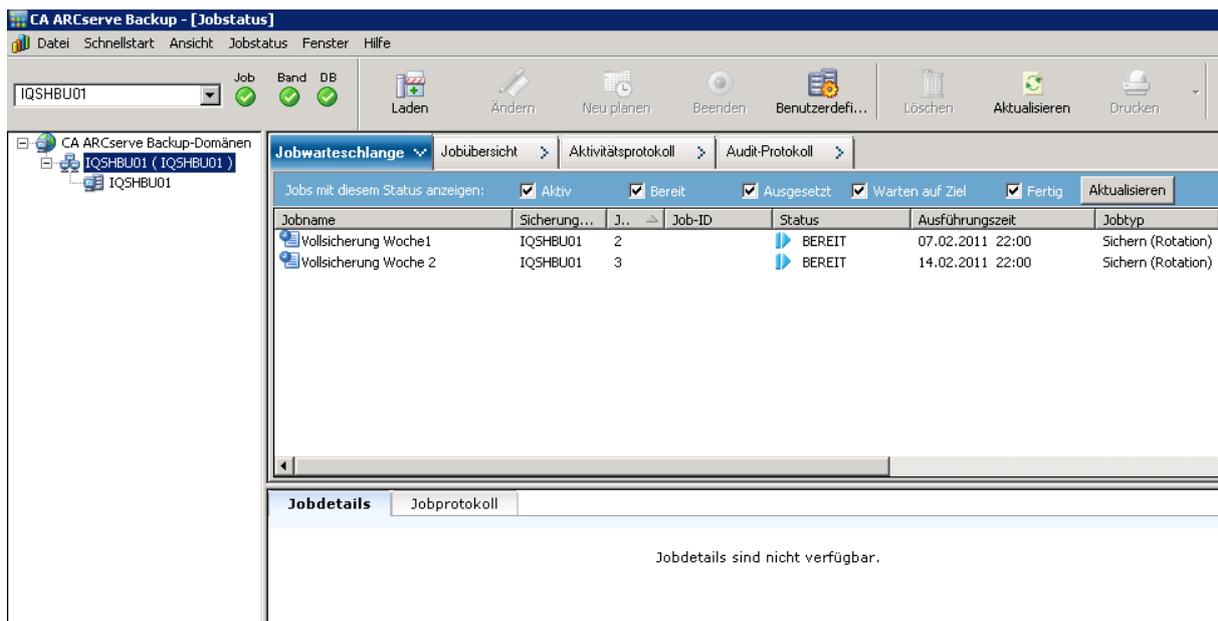
Jobausführungszeit
 Jetzt ausführen
 Ausführen am
 14.02.2011
 22:00:00
 Mit Status AUSGESETZT in Warteschlange stellen

Quellenpriorität
Job speichern
Vorlage speichern
Pre-Flight Check

OK Abbrechen Hilfe

Komprimierungsrate erreicht 1,00(0,00%)
 USB_HDD2 Datendateipfad: F:\Backup_DD\
 Indexdateipfad: D:\Index_Backup_DD\

Übergabe an Festplatte 2



CA ARCserve Backup - [Jobstatus]

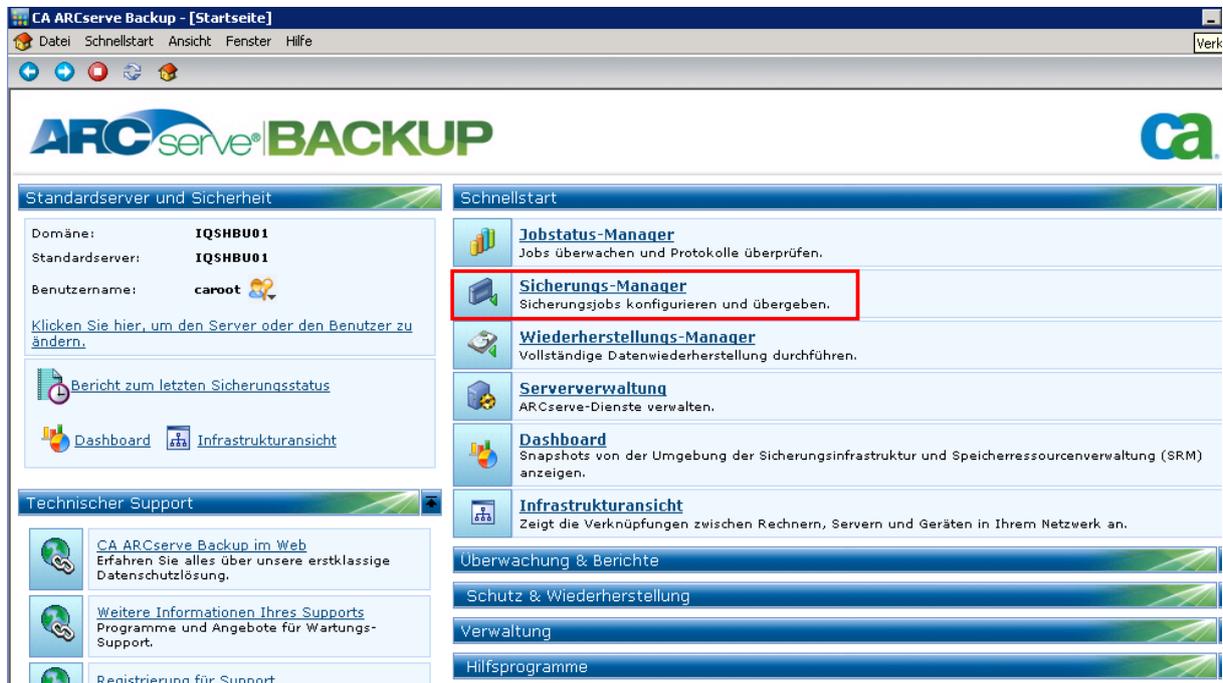
Jobs mit diesem Status anzeigen: Aktiv Bereit Ausgesetzt Warten auf Ziel Fertig Aktualisieren

Jobname	Sicherung...	J..	Job-ID	Status	Ausführungszeit	Jobtyp
Vollsicherung Woche1	IQSHBU01	2		BEREIT	07.02.2011 22:00	Sichern (Rotation)
Vollsicherung Woche 2	IQSHBU01	3		BEREIT	14.02.2011 22:00	Sichern (Rotation)

Jobdetails sind nicht verfügbar.

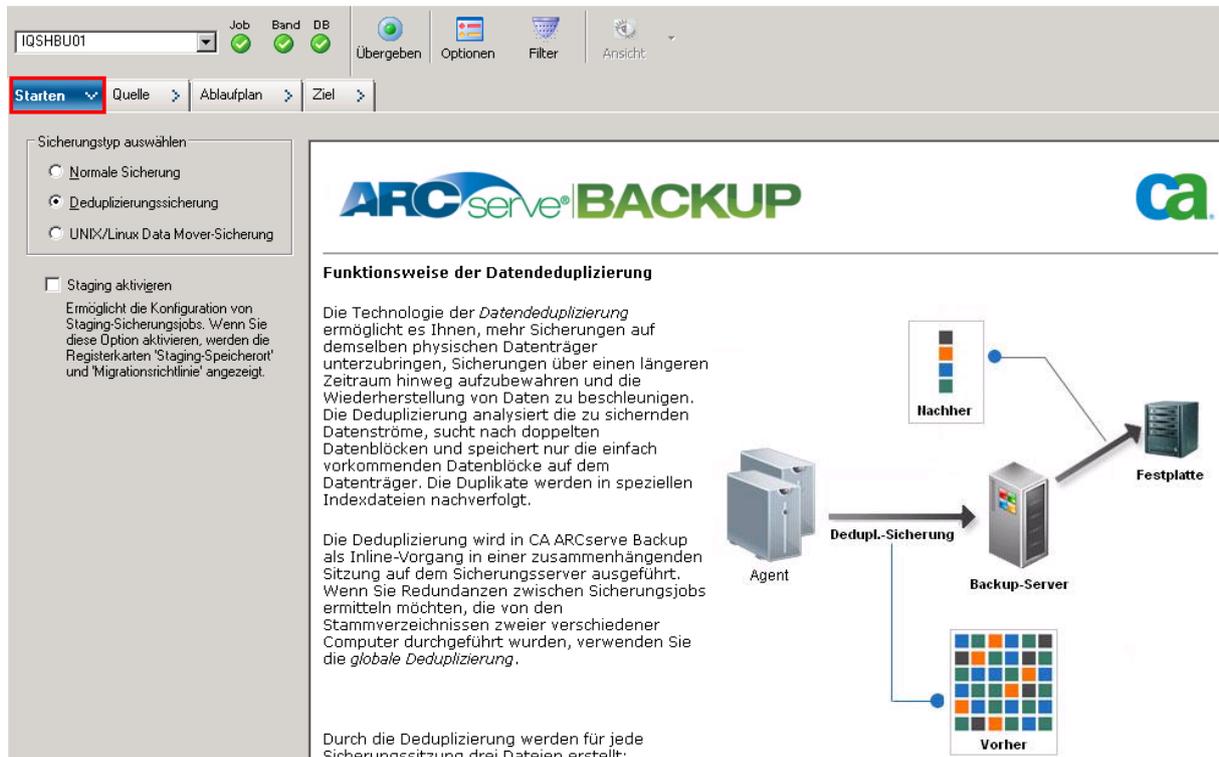
Übersicht der angelegten Sicherungen.

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



The screenshot shows the CA ARCserve Backup web interface. The 'Schnellstart' (Quick Start) section contains several links: 'Jobstatus-Manager', 'Sicherungs-Manager' (highlighted with a red box), 'Wiederherstellungs-Manager', 'Serververwaltung', 'Dashboard', and 'Infrastruktursicht'. The 'Sicherungs-Manager' link is described as 'Sicherungsjobs konfigurieren und übergeben.' Below this, there are navigation tabs for 'Überwachung & Berichte', 'Schutz & Wiederherstellung', 'Verwaltung', and 'Hilfsprogramme'.

Auswahl des Sicherungsmanagers



The screenshot shows the configuration interface for deduplication. The 'Starten' button is highlighted with a red box. The 'Sicherungstyp auswählen' (Select backup type) section has 'Deduplizierungssicherung' (Deduplication backup) selected. The 'Funktionsweise der Dateneduplizierung' (How data deduplication works) section contains the following text:

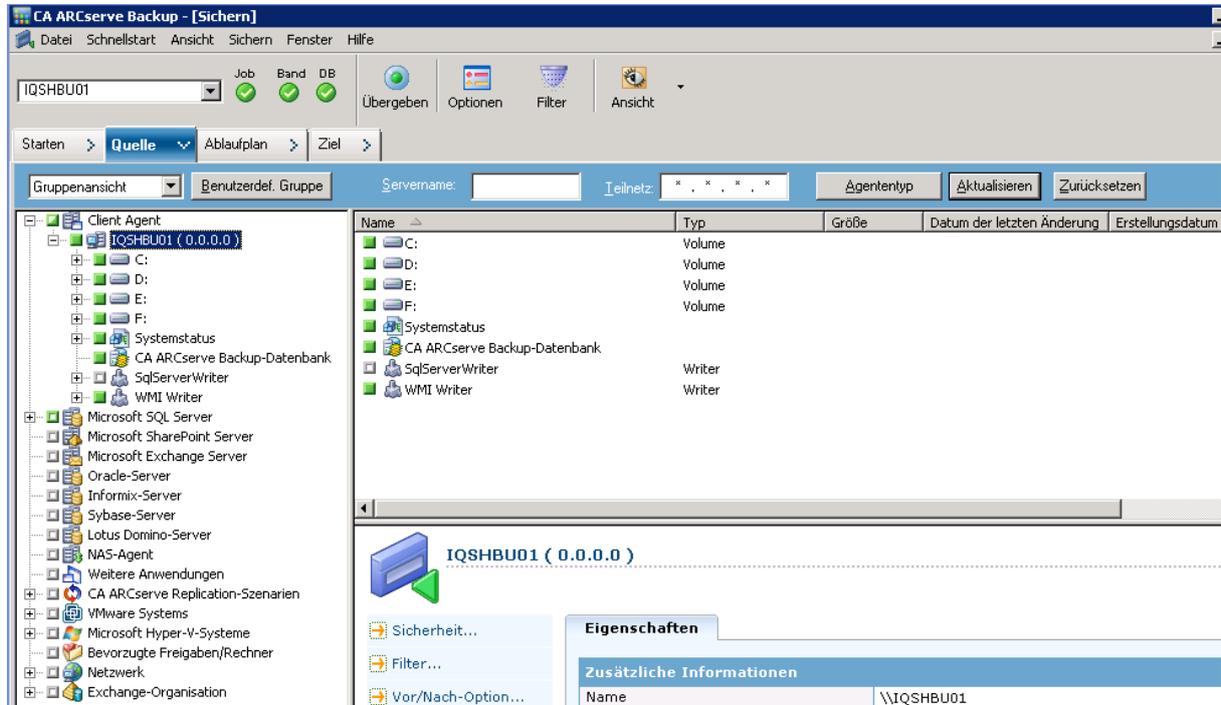
Die Technologie der *Dateneduplizierung* ermöglicht es Ihnen, mehr Sicherungen auf demselben physischen Datenträger unterzubringen, Sicherungen über einen längeren Zeitraum hinweg aufzubewahren und die Wiederherstellung von Daten zu beschleunigen. Die Deduplizierung analysiert die zu sichernden Datenströme, sucht nach doppelten Datenblöcken und speichert nur die einfach vorkommenden Datenblöcke auf dem Datenträger. Die Duplikate werden in speziellen Indexdateien nachverfolgt.

Die Deduplizierung wird in CA ARCserve Backup als Inline-Vorgang in einer zusammenhängenden Sitzung auf dem Sicherungsserver ausgeführt. Wenn Sie Redundanzen zwischen Sicherungsjobs ermitteln möchten, die von den Stammverzeichnissen zweier verschiedener Computer durchgeführt wurden, verwenden Sie die *globale Deduplizierung*.

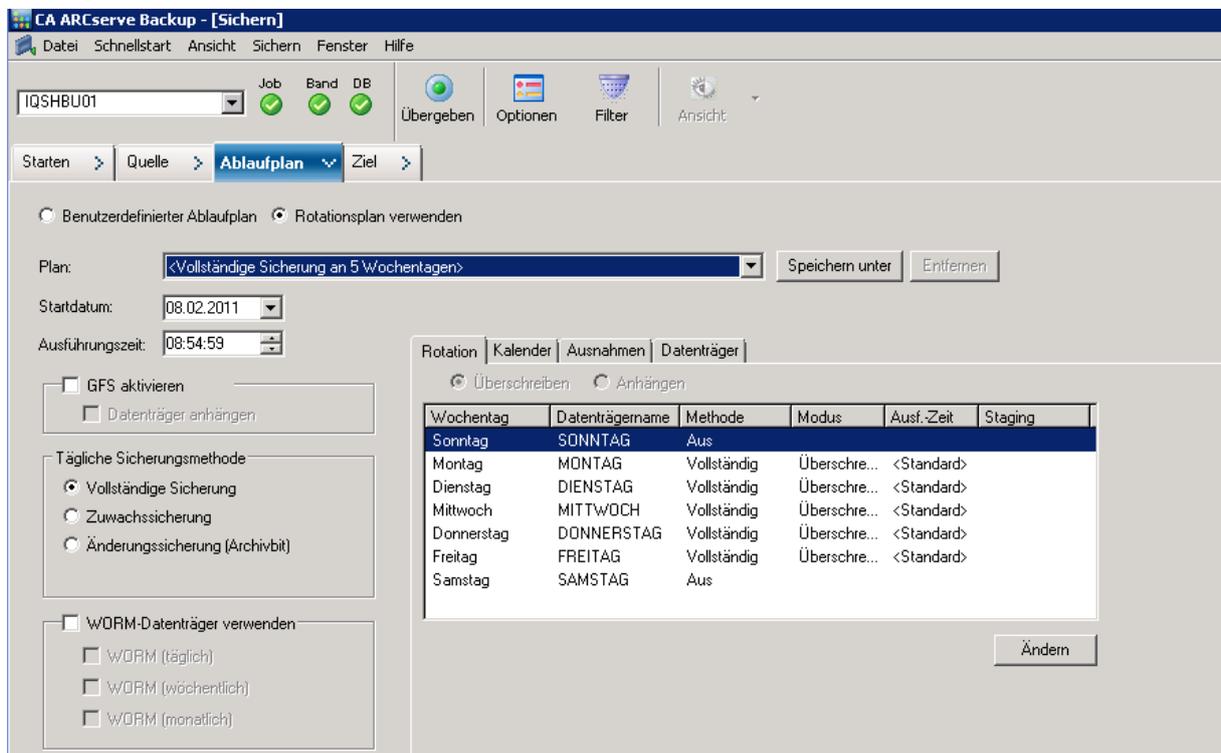
Durch die Deduplizierung werden für jede Sicherungssitzung drei Dateien erstellt:

The diagram illustrates the deduplication process. It shows an 'Agent' connected to a 'Backup-Server'. The 'Backup-Server' is connected to a 'Festplatte' (hard drive). The process is labeled 'Dedupl.-Sicherung'. A 'Hasher' component is shown above the Backup-Server, and a 'Vorher' (Before) component is shown below it, indicating the state of the data before deduplication.

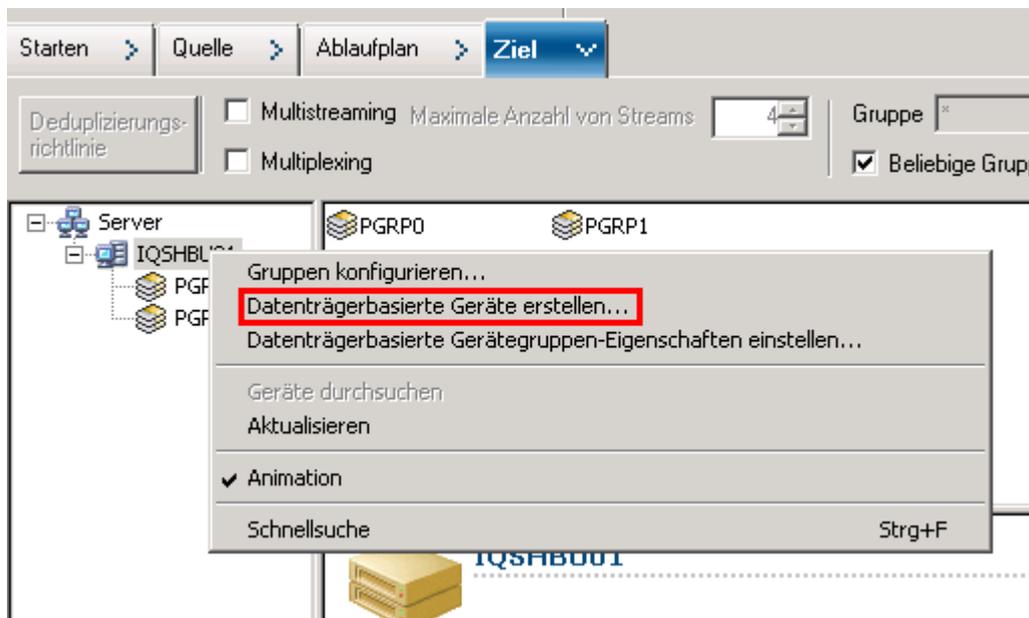
Erneute Wahl der Deduplizierungssicherung



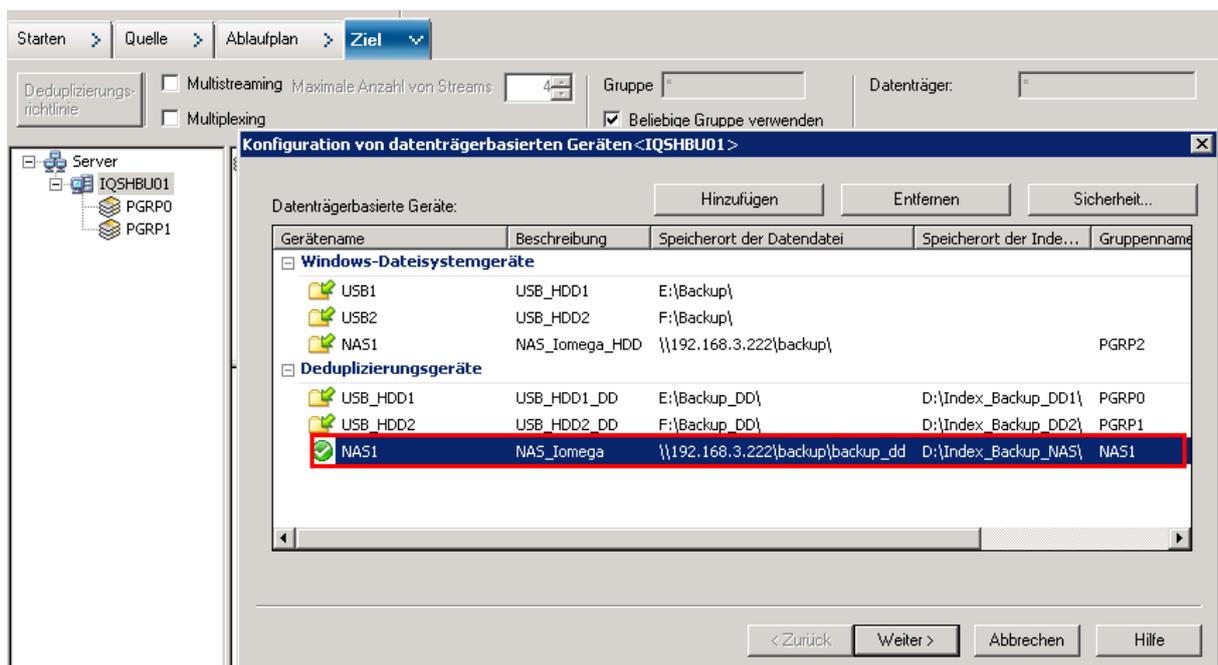
Auswahl der zu Sichernden Dateien (Hier Vollsicherung)



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.

Starten > Quelle > Ablaufplan > Ziel

Deduplizierungsrichtlinie: Multistreaming Maximale Anzahl von Streams: 4 Multiplexing Gruppe: NAS1 Datenträger: *

Beliebige Gruppe verwenden

Server
 IQSHBU01
 NAS1
 PGRP0
 PGRP1

<Gerät: 6> <Leerer Datentr.>

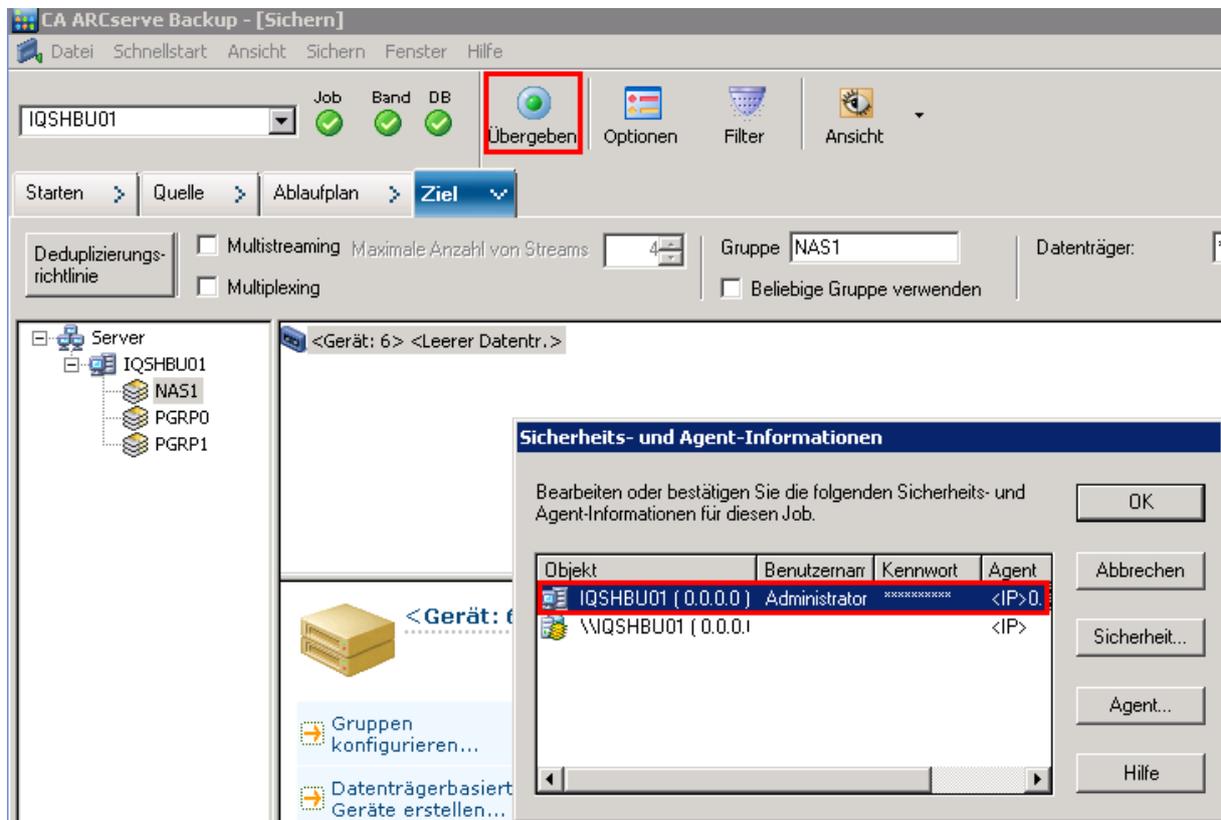
NAS1

- Gruppen konfigurieren...
- Datenträgerbasierte Geräte erstellen...
- Datenträgerbasierte Gerätegruppen-Eigenschaften einstellen...
- Aktualisieren

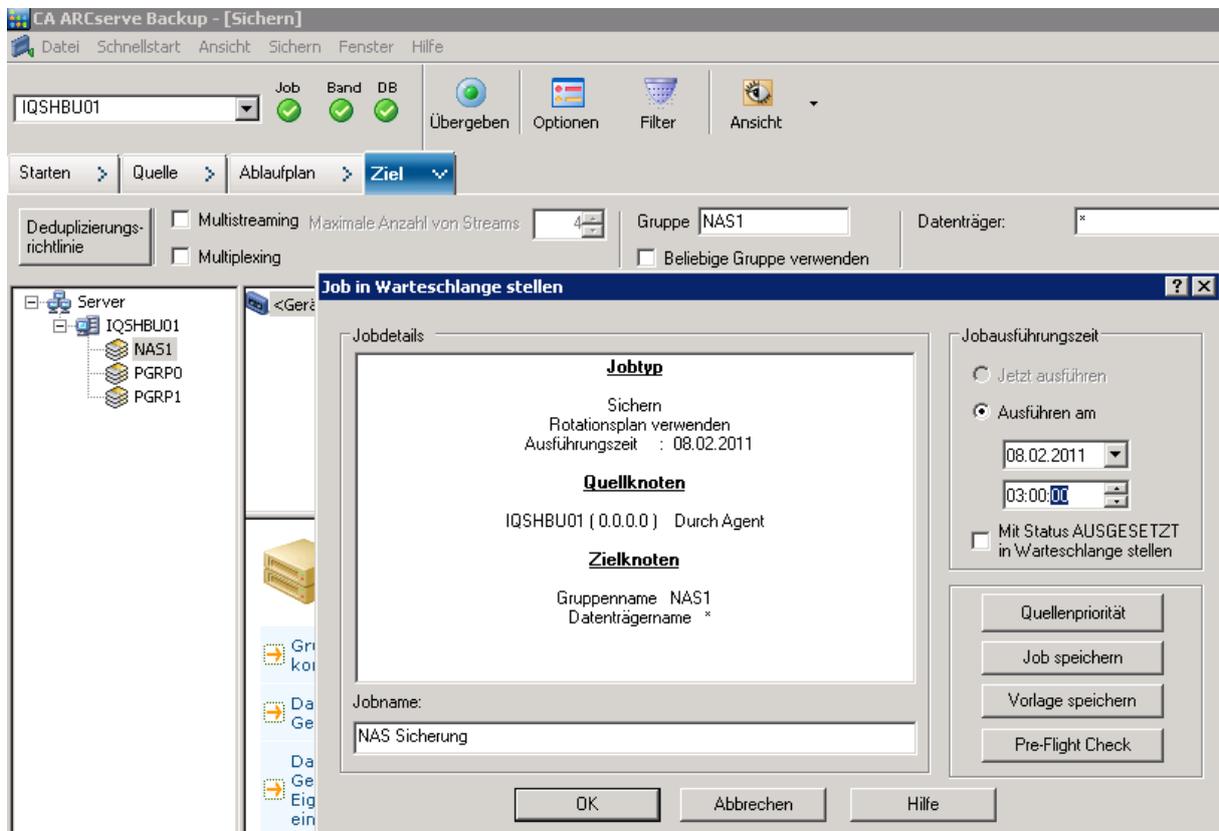
Gruppeninformationen	
Gruppenname	NAS1
Gruppentyp	Deduplizierungsgruppe

Geräteinformationen	
Komprimierungsrate erreicht	1,00(0,00%)
NAS1	Datendateipfad: \\192.168.3.222\backup\backup_dd\ Indexdateipfad: D:\Index_Backup_NAS\

Ein neu erstelltes Datenträger basiertes Gerät.



Übergabe des Datensicherungsjobs inkl. Angabe des Sicherungsoperators.



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)

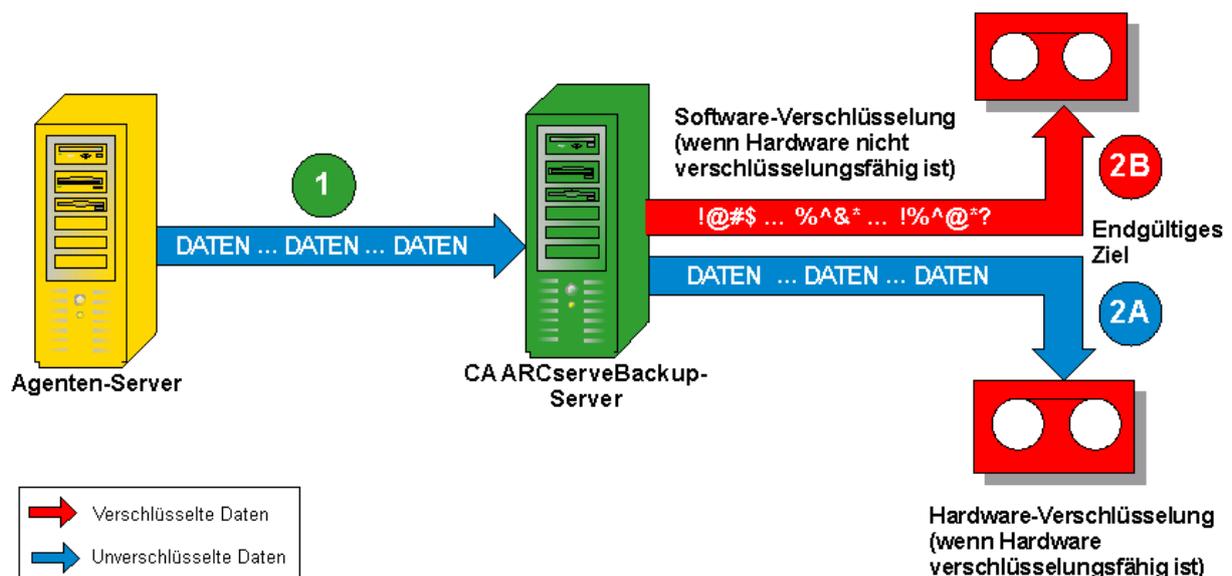
Die Installation und die Handhabung zwischen Server 2008 / R2 und Server 2003 / R2 unterscheiden sich nicht.

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)

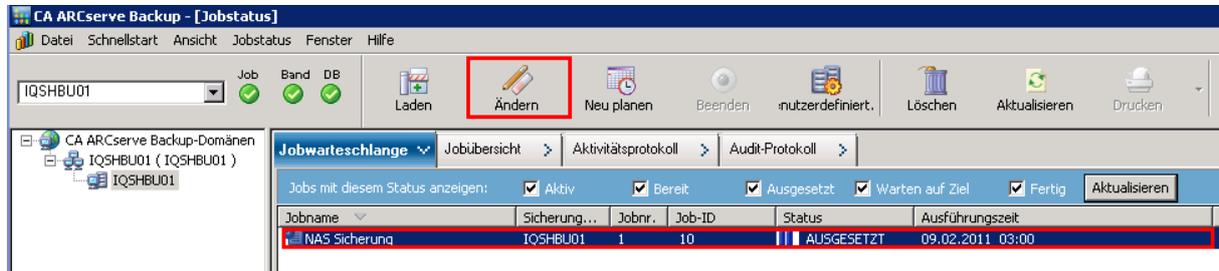
Wenn CA ARCserve Backup feststellt, dass der endgültige Zieldatenträger keine Hardware-Verschlüsselung unterstützt, verwendet CA ARCserve Backup Software-Verschlüsselung zum Verschlüsseln der Daten vor deren Übertragung an den endgültigen Zieldatenträger.



8.1 Festlegen der Verschlüsselungsfunktion

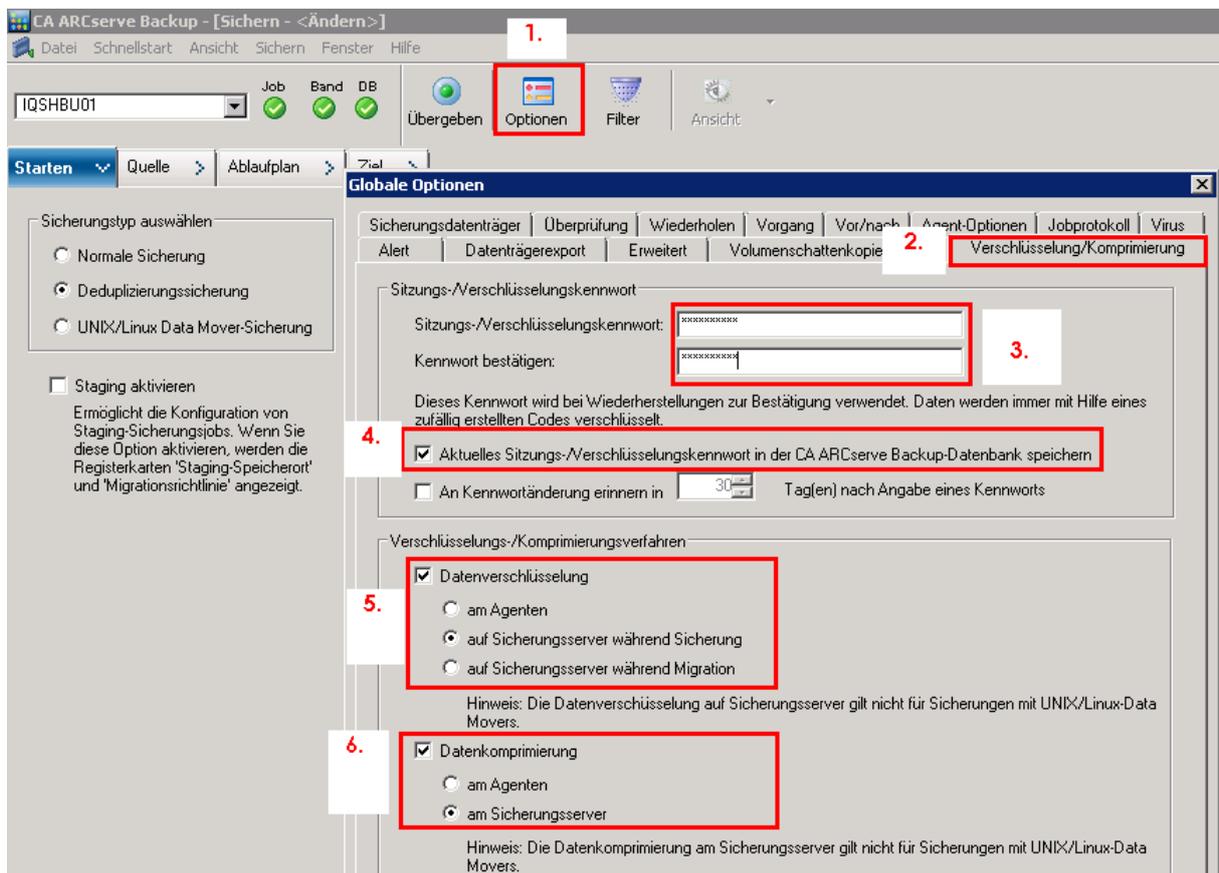
Über die Registerkarte "Verschlüsselung/Komprimierung" im Dialogfeld "Globale Optionen" des Sicherungs-Managers, kann auf die Verschlüsselungsoptionen zugegriffen werden. In diesem Dialogfeld kann die Datenverschlüsselung auf dem Agenten, auf dem Sicherungsserver während der Sicherung, oder auf dem Sicherungsserver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

8.1.1 Einstellen der Verschlüsselung für einen bestehenden Sicherungsjob



Beispiel NAS-Sicherung (Selektieren und Ändern wählen)

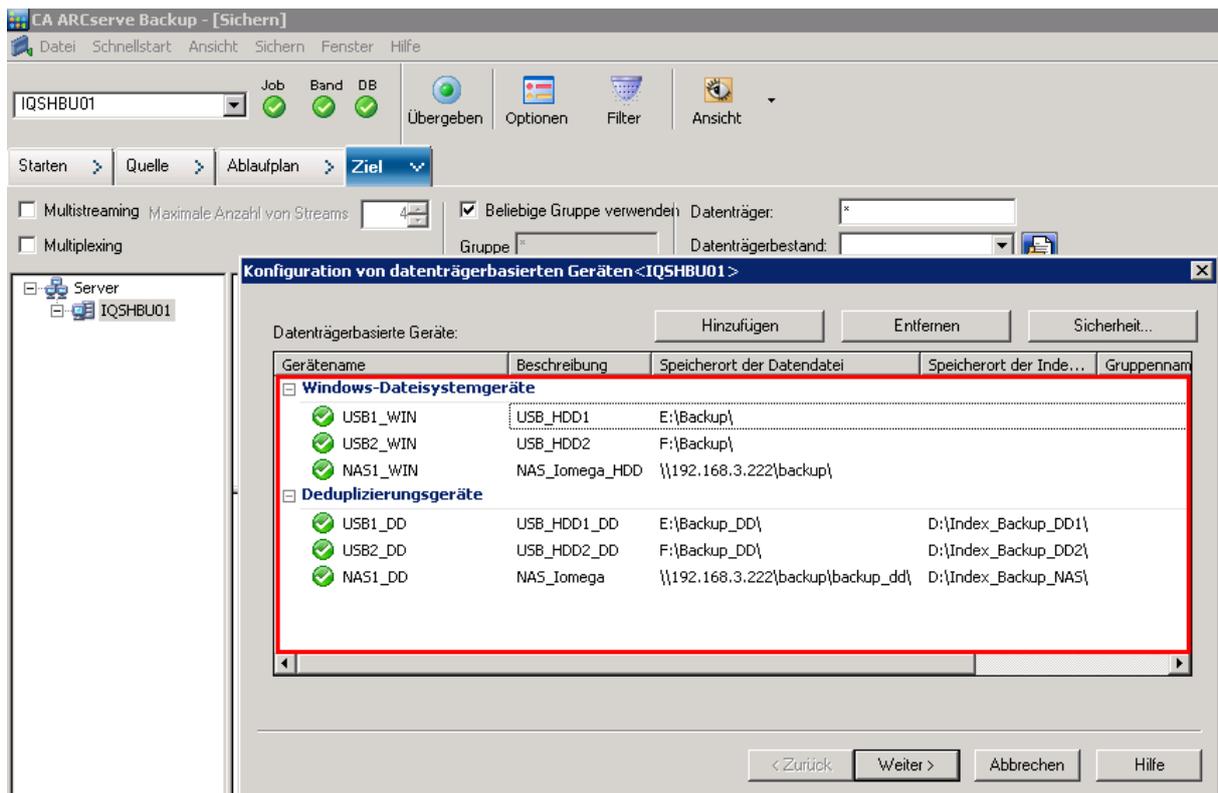
8.1.2 Einstellungen



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

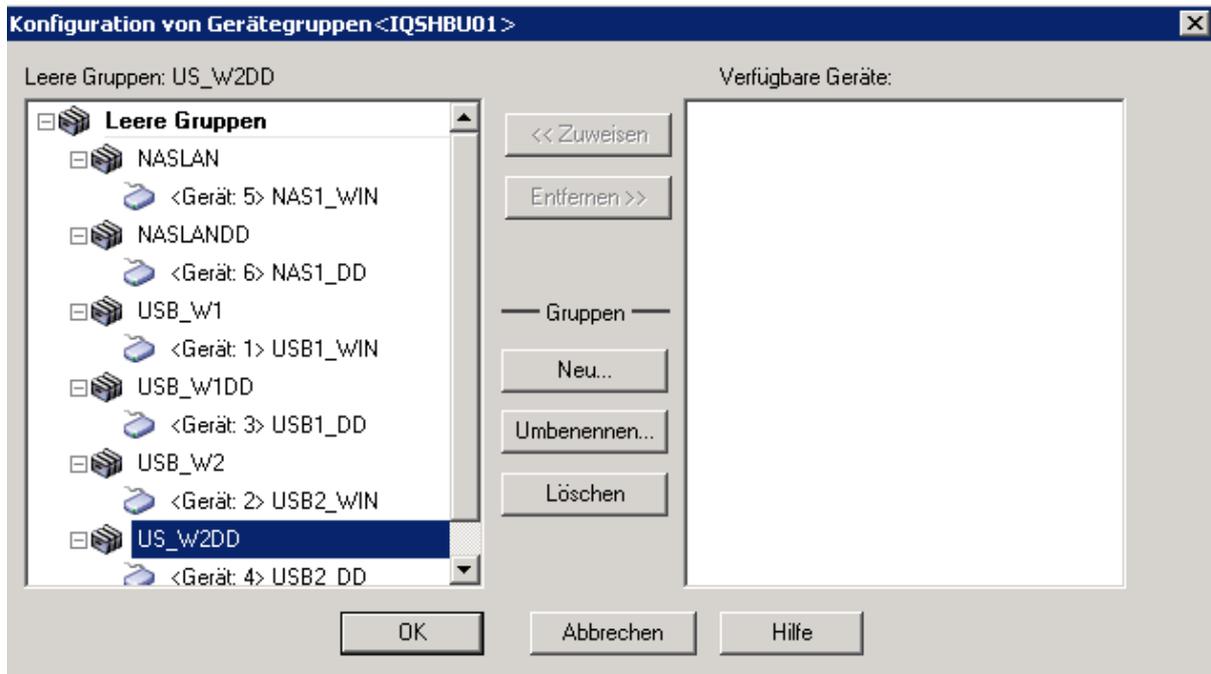
8.2 Einrichtung einer normalen Sicherung mit Verschlüsselung

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

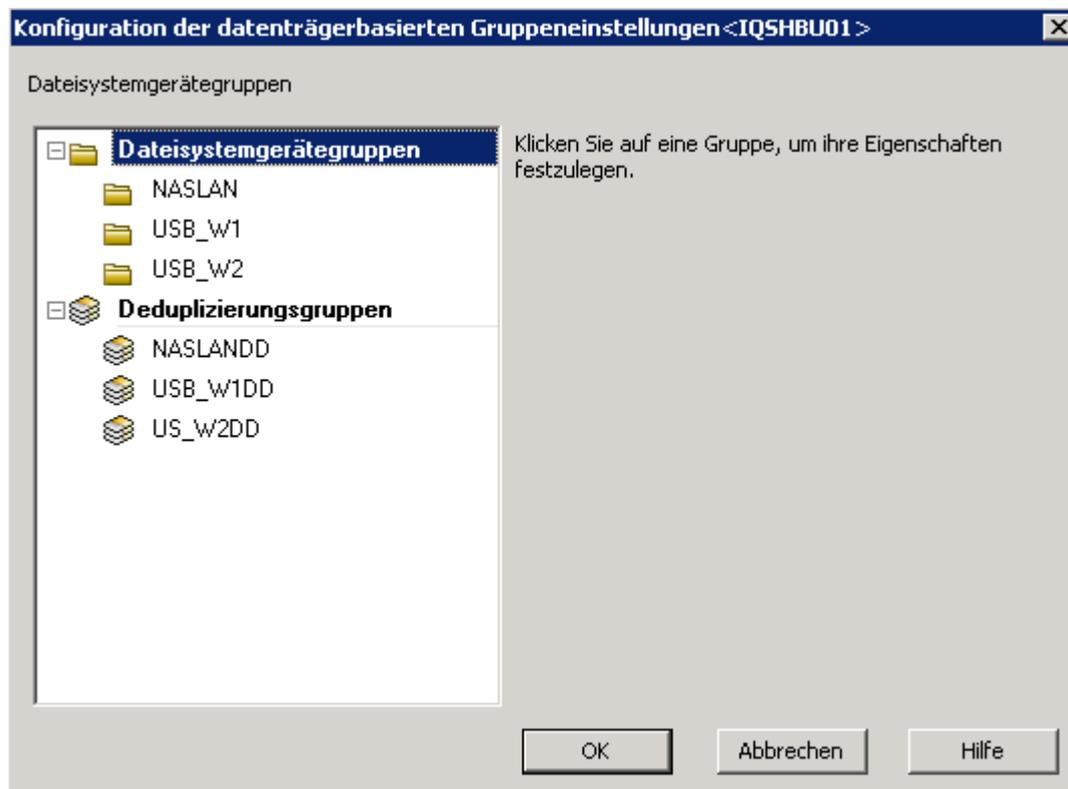


Angelegte Datenträgerbasierte Geräte
(Unterscheidung für Windows (NTFS)- und Sicherungen mit Deduplizierung)

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 Verschlüsselung.

Starten > Quelle > Ablaufplan > Ziel >

Sicherungstyp auswählen

- Normale Sicherung
- Deduplizierungssicherung
- UNIX/Linux Data Mover-Sicherung

Staging aktivieren
Ermöglicht die Konfiguration von Staging-Sicherungsjobs. Wenn Sie diese Option aktivieren, werden die Registerkarten 'Staging-Speicherort' und 'Migrationsrichtlinie' angezeigt.

ARCserve® BACKUP **ca**

Sichern von Daten

Sie können CA ARCserve Backup verwenden, um alle Ihre Clients auf einmal zu sichern, nur Ihren lokalen Host zu sichern, oder ausgewählte Hosts, einschließlich einzelner Data Mover-Server, zu sichern.

Hinweis: Um Objekte auszuwählen, die sich auf Servern für Sicherungen befinden, geben Sie zunächst die Server in der Client-Datenbank an. Die CA ARCserve Backup-Software muss aktiv sein, um Server zur Datenbank hinzuzufügen.

Mit dem Sicherungs-Manager können Sie folgende Aufgaben durchführen:

- Sichern von Clients auf verschiedenen Datenträgern oder Erstellen eines benutzerdefinierten Sicherungsplans

Diagramm: Ein Agent (links) führt einen Backup (Pfeil) zu einem Backup-Server (rechts), der an ein Bandgerät (rechts unten) angeschlossen ist.

1. Optionen

2. Verschlüsselung/Komprimierung

Sitzungs-/Verschlüsselungskennwort

Sitzungs-/Verschlüsselungskennwort: []

Kennwort bestätigen: [] **3.**

Dieses Kennwort wird bei Wiederherstellungen zur Bestätigung verwendet. Daten werden immer mit Hilfe eines zufällig erstellten Codes verschlüsselt.

4. Aktuelles Sitzungs-/Verschlüsselungskennwort in der CA ARCserve Backup-Datenbank speichern

An Kennwortänderung erinnern in 30 Tag(en) nach Angabe eines Kennworts

Verschlüsselungs-/Komprimierungsverfahren

5. Datenverschlüsselung

- am Agenten
- auf Sicherungsserver während Sicherung
- auf Sicherungsserver während Migration

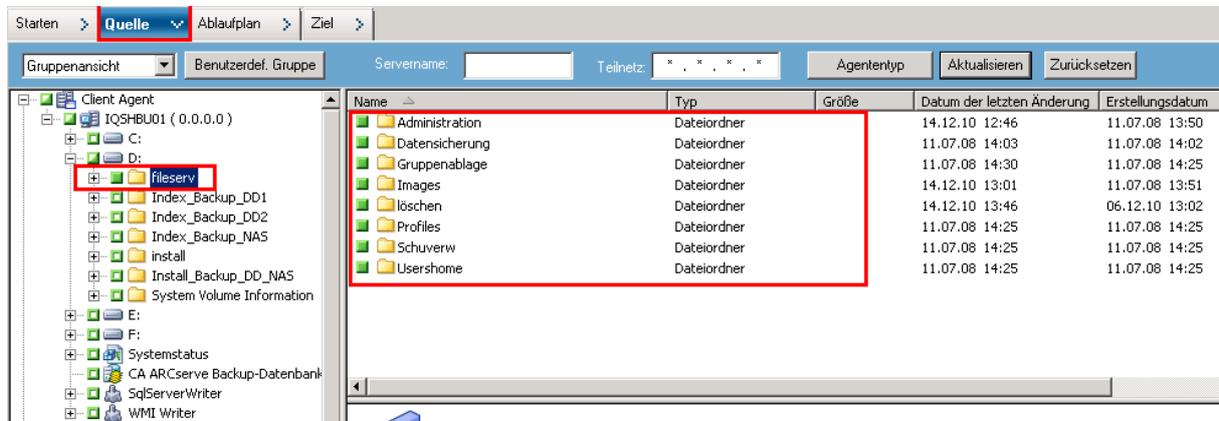
Hinweis: Die Datenverschlüsselung auf Sicherungsserver gilt nicht für Sicherungen mit UNIX/Linux-Data Movers.

6. Datenkomprimierung

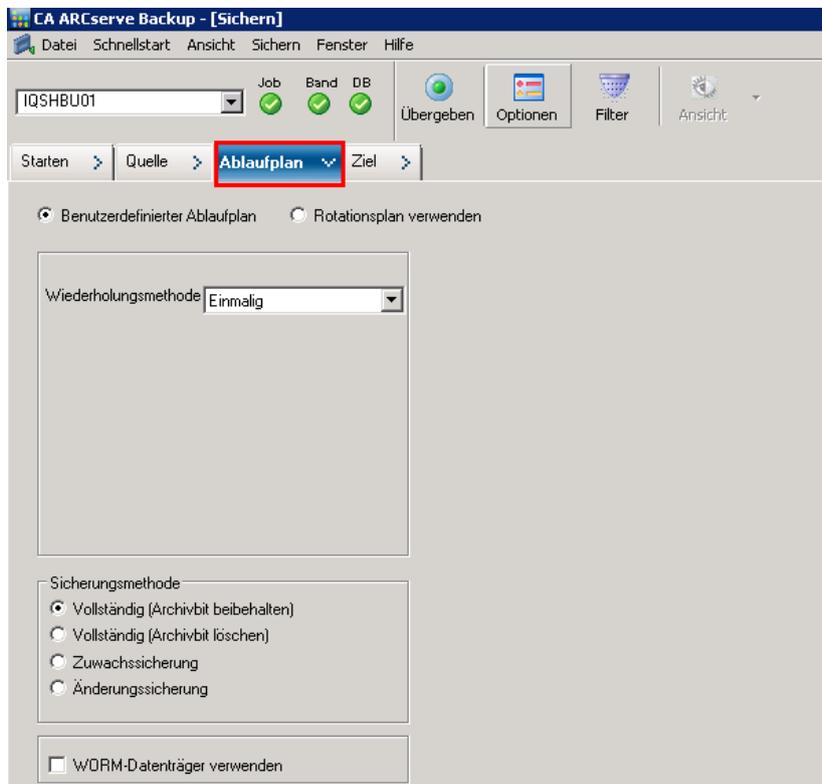
- am Agenten
- am Sicherungsserver

Hinweis: Die Datenkomprimierung am Sicherungsserver gilt nicht für Sicherungen mit UNIX/Linux-Data Movers.

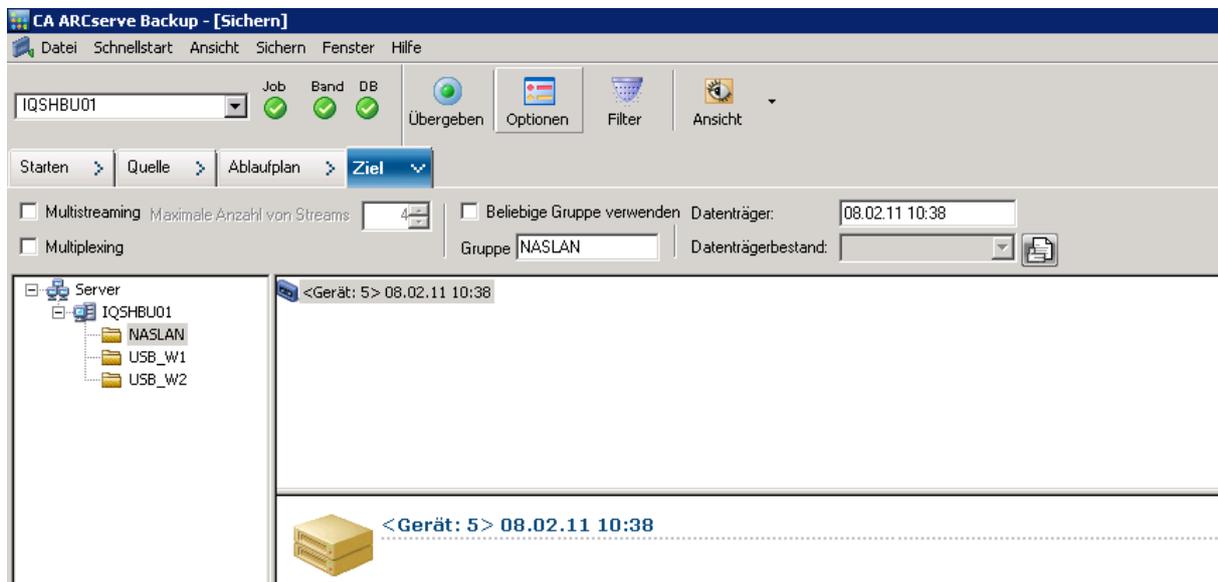
Anwenden der Verschlüsselungsfunktionen



Beispielauswahl des Ordners „fileserv“

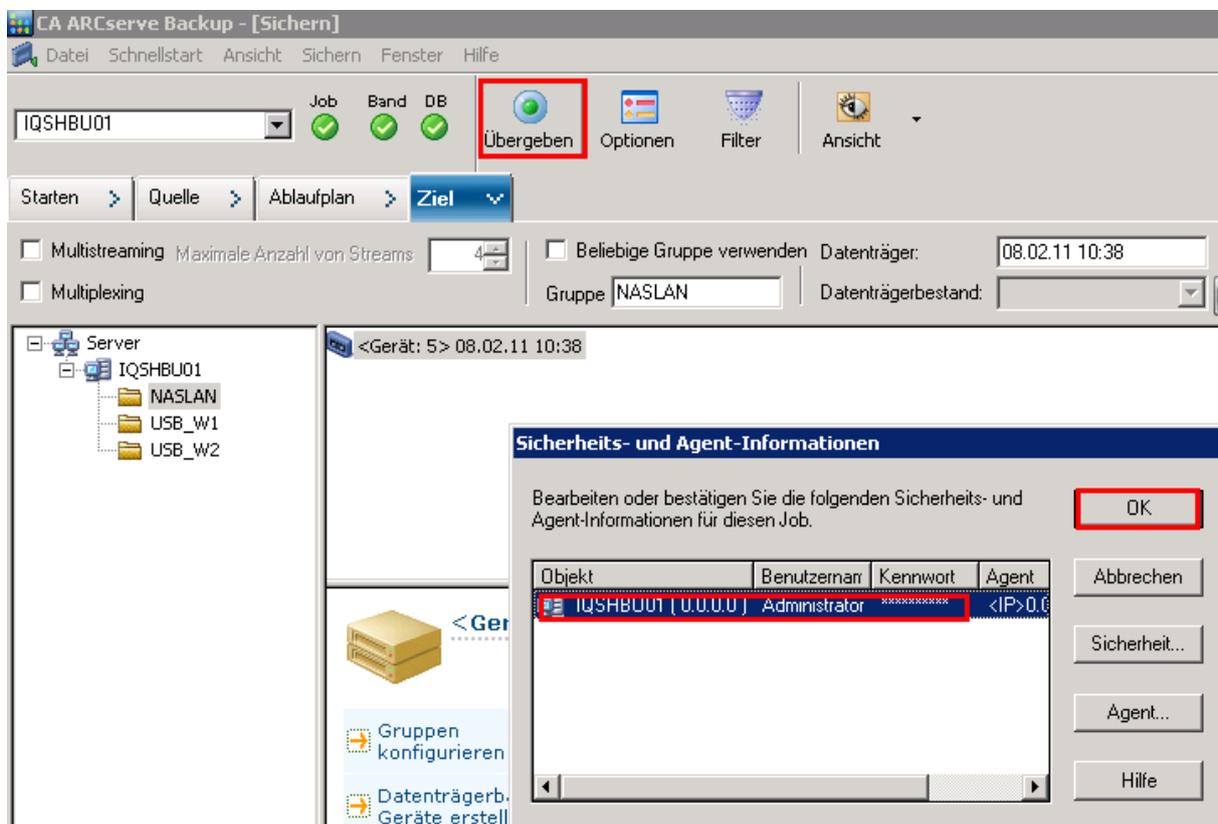


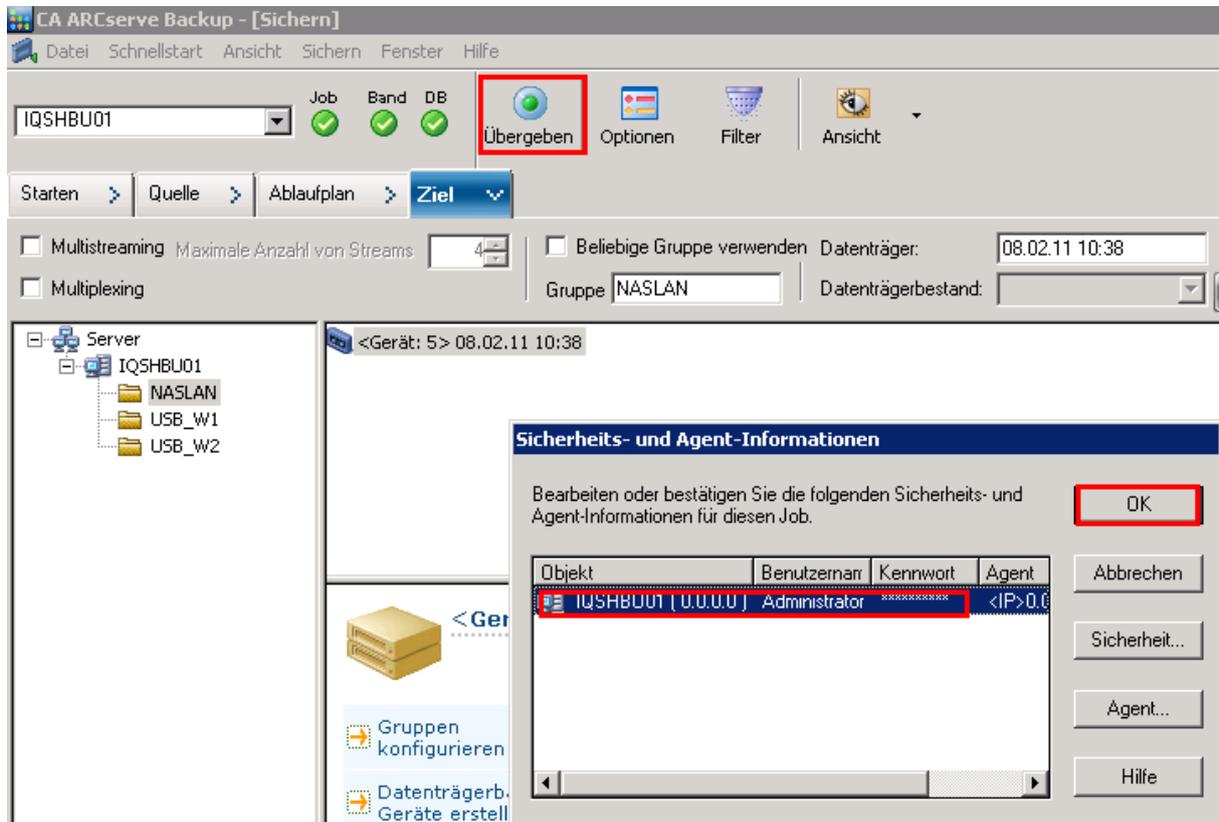
Bestimmen des Ablaufplans (Hier einmalig)



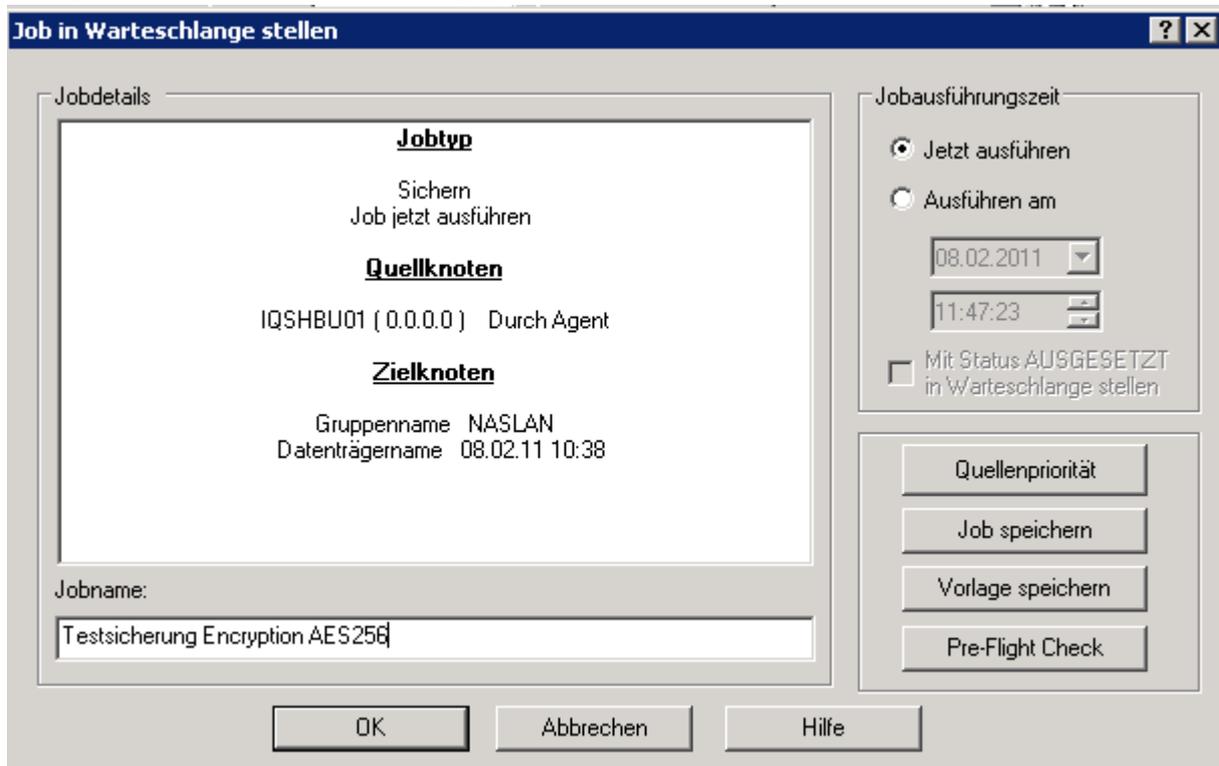
Auswahl des Ziels. (Hier NASLAN)

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.





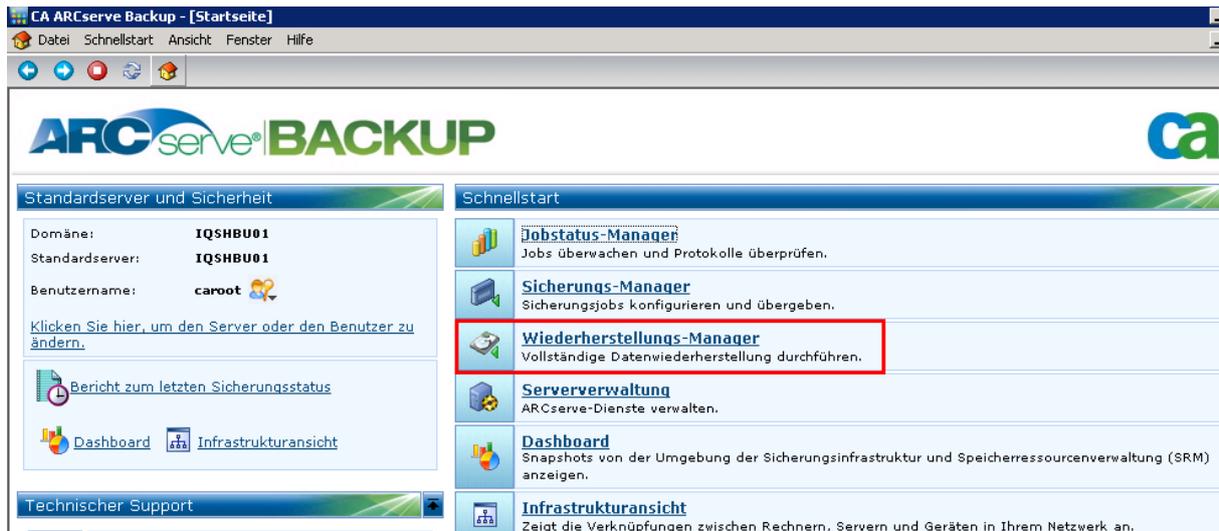
Übergabe des definierten Sicherungsjobs.



Testsicherung Encryption AES256 IQSHBU01 1 20 AKTIV Dateien werden gesichert... Sichern

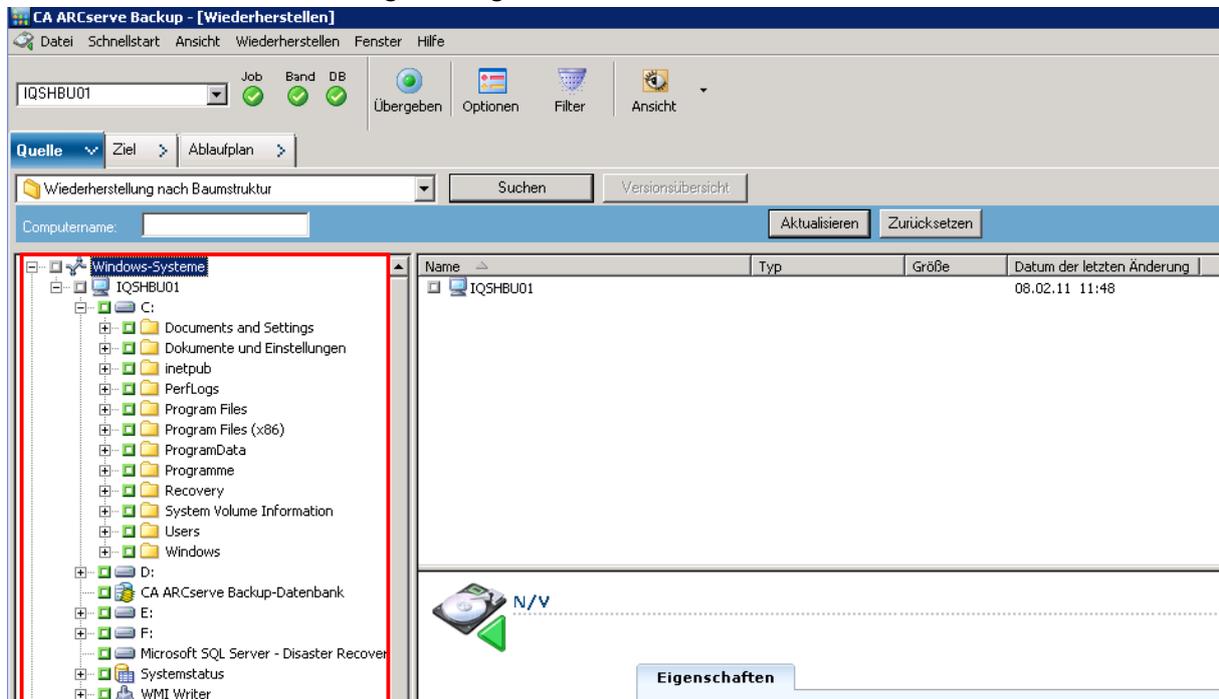
9. Wiederherstellung

9.1 Wiederherstellen von Daten (Ordner und Dateien)



The screenshot shows the CA ARCserve Backup main interface. The 'Schnellstart' (Quick Start) section contains several options, with 'Wiederherstellungs-Manager' (Recovery Manager) highlighted by a red box. The interface also displays server information for domain 'IQSHBU01' and user 'caroot'.

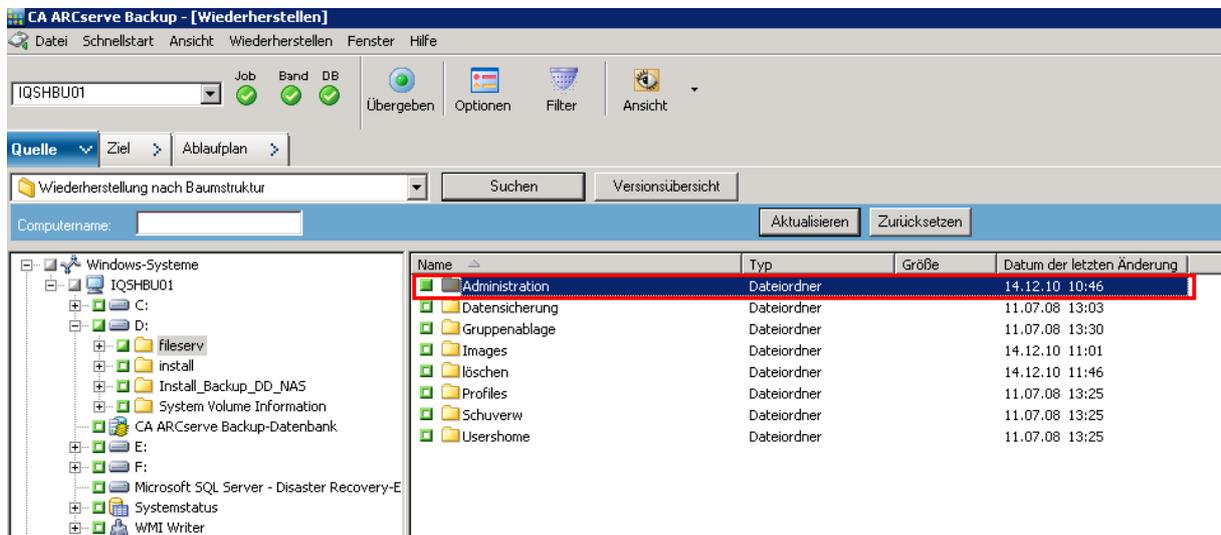
Wählen des Wiederherstellungsmanagers



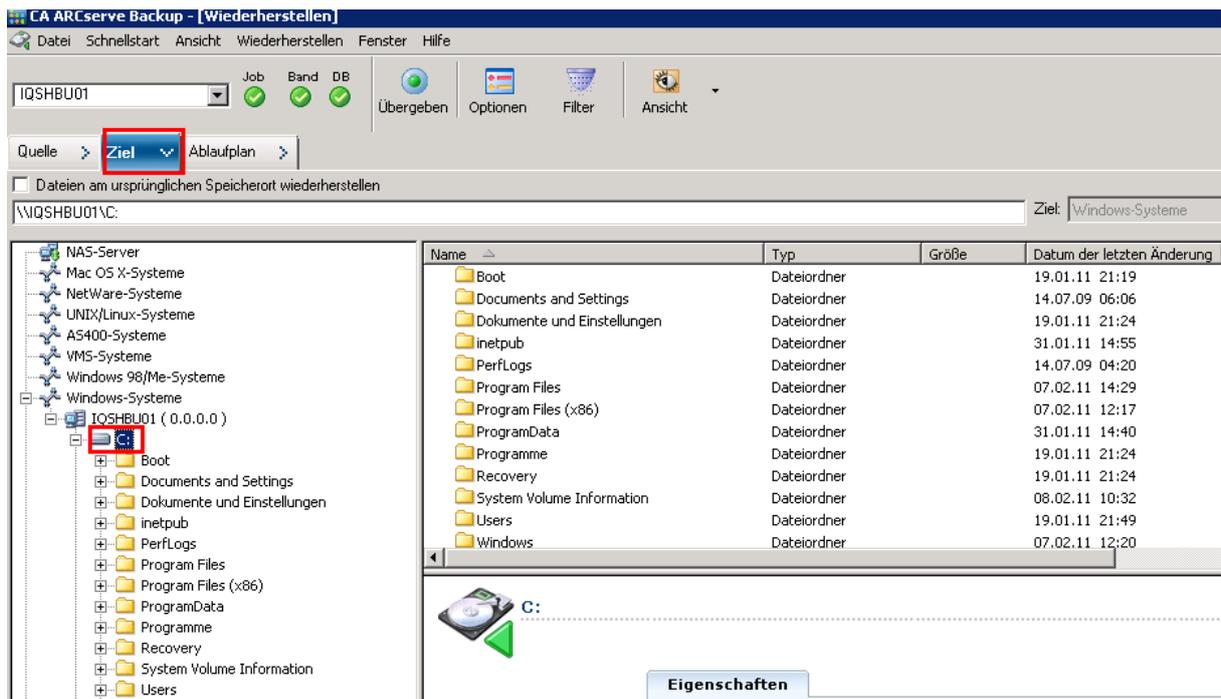
The screenshot shows the 'Wiederherstellen' (Recovery) window. The 'Quelle' (Source) is set to 'Wiederherstellung nach Baumstruktur' (Recovery by tree structure). The file tree on the left shows the path 'Windows-Systeme > IQSHBU01 > C:' highlighted with a red box. The right pane shows a table of files to be recovered.

Name	Typ	Größe	Datum der letzten Änderung
IQSHBU01			08.02.11 11:48

Auswahl des Pfades



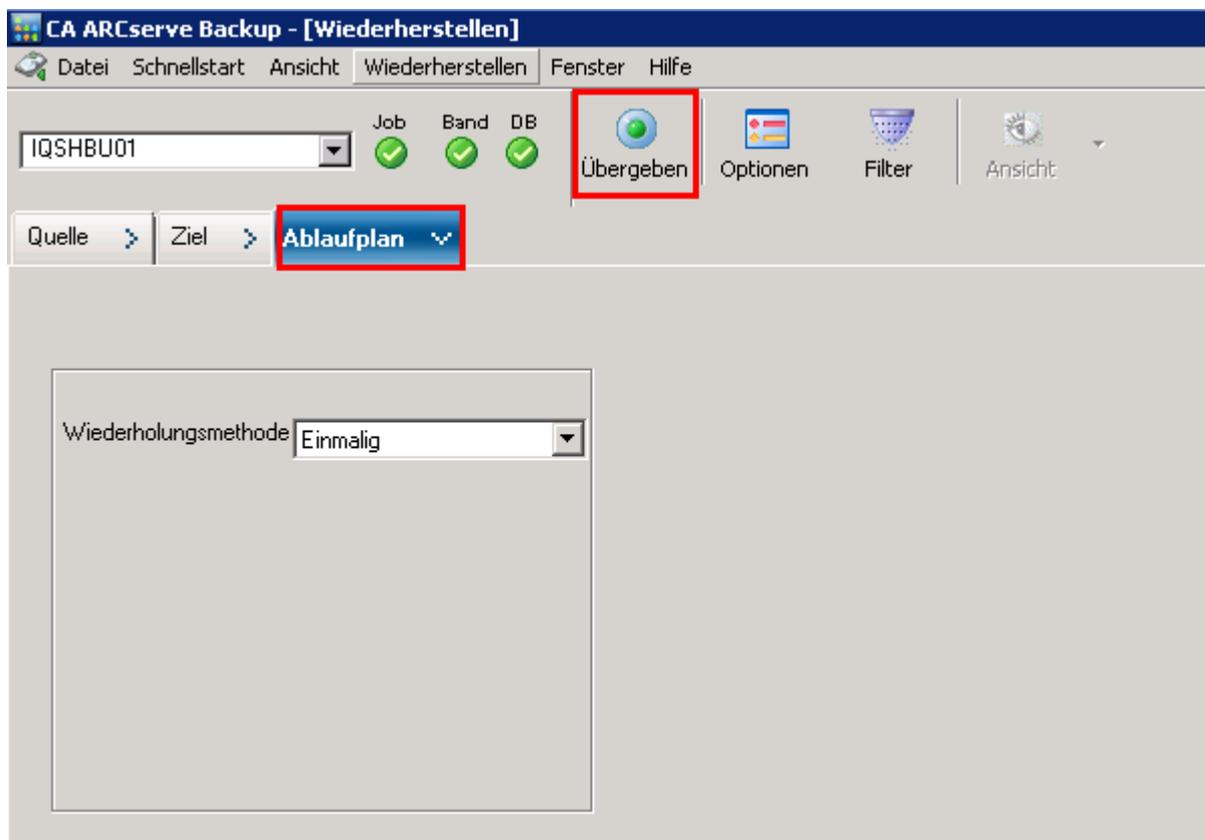
Beispielordner „Administration“



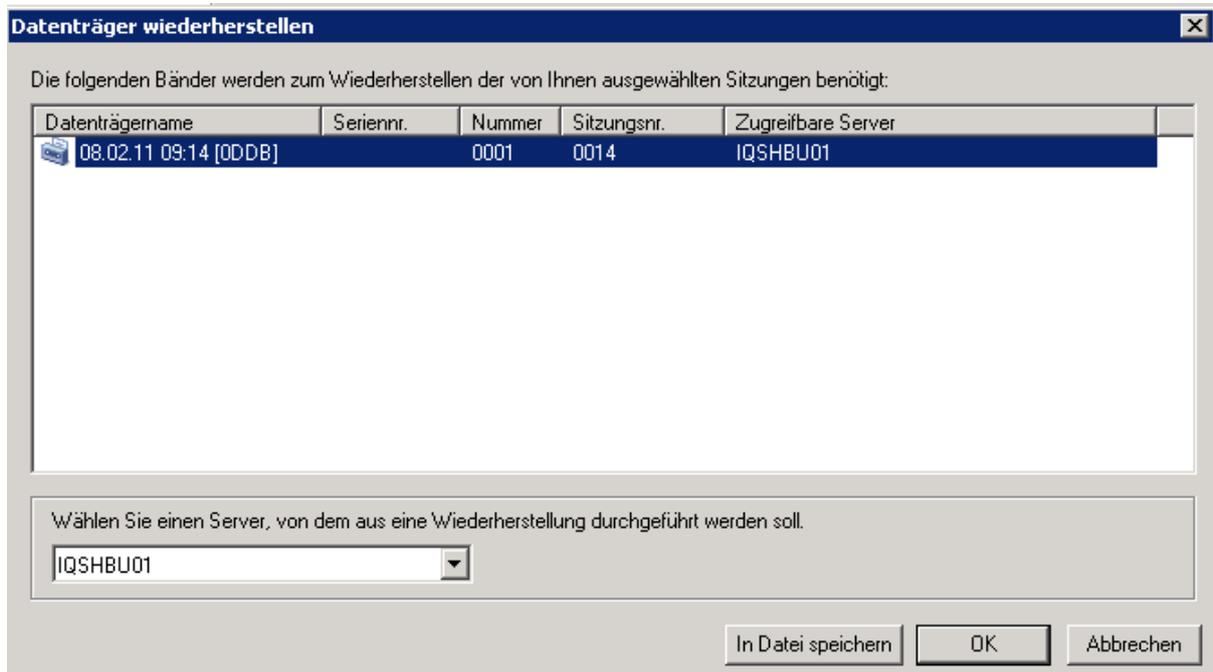
Wiederherstellung nach C:\ (Beispiel)



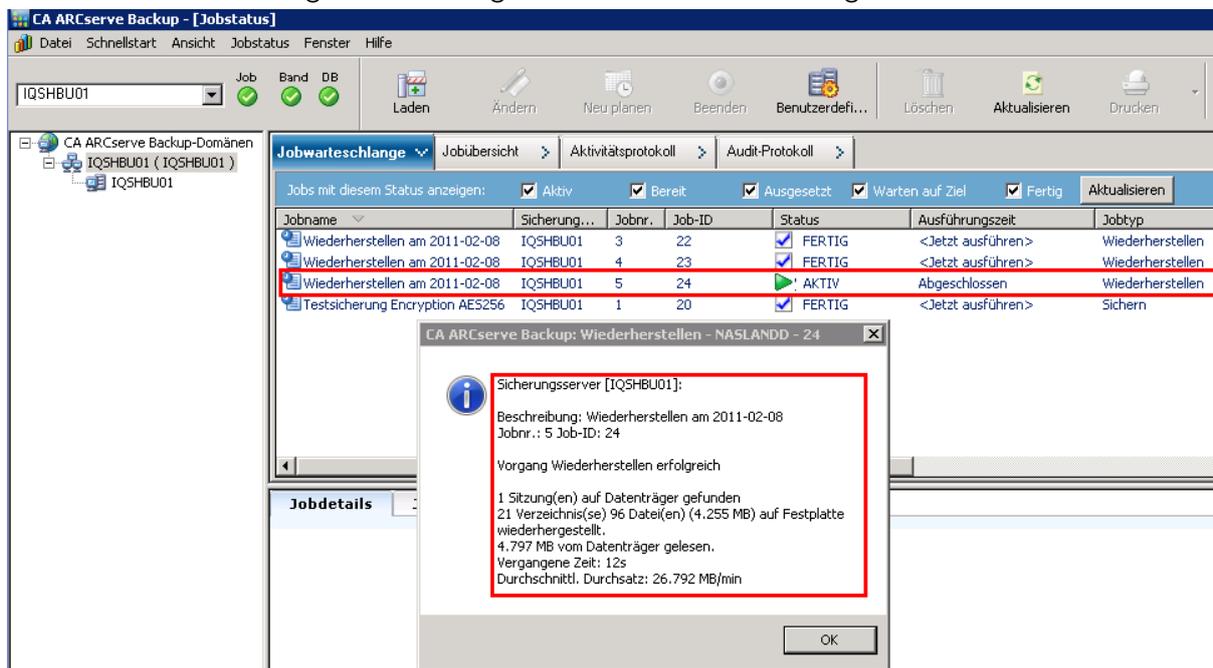
Option: „Dateien am ursprünglichen Speicherort wiederherstellen“



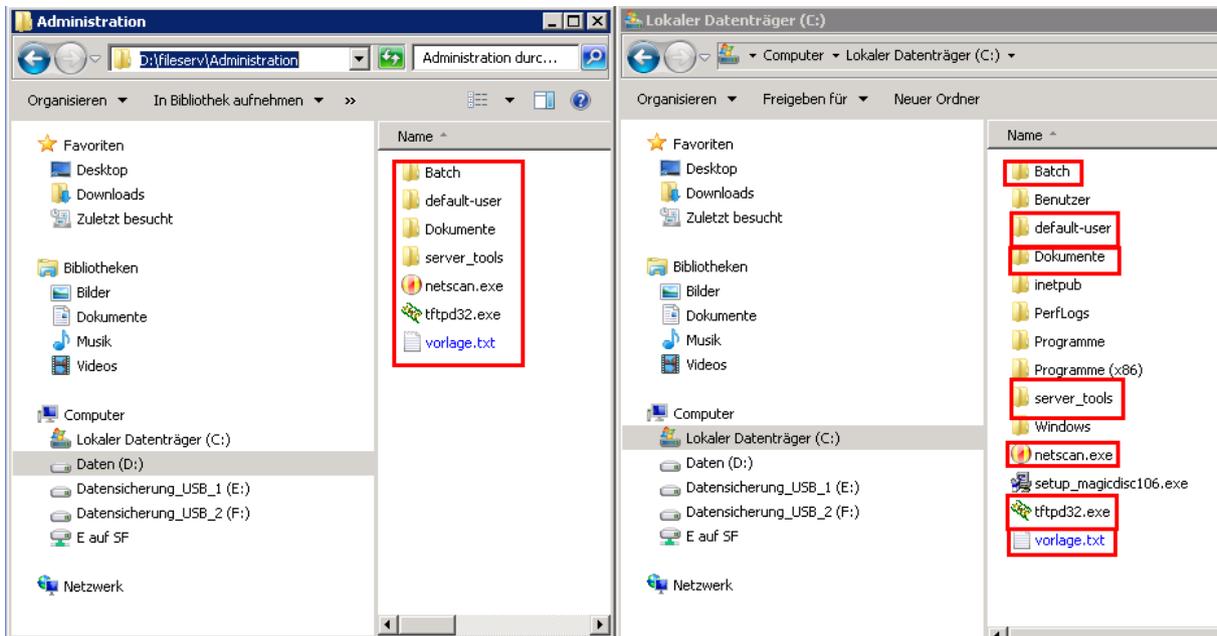
Übergabe an das System



Hinweis auf den benötigten Datenträger für die Wiederherstellung.

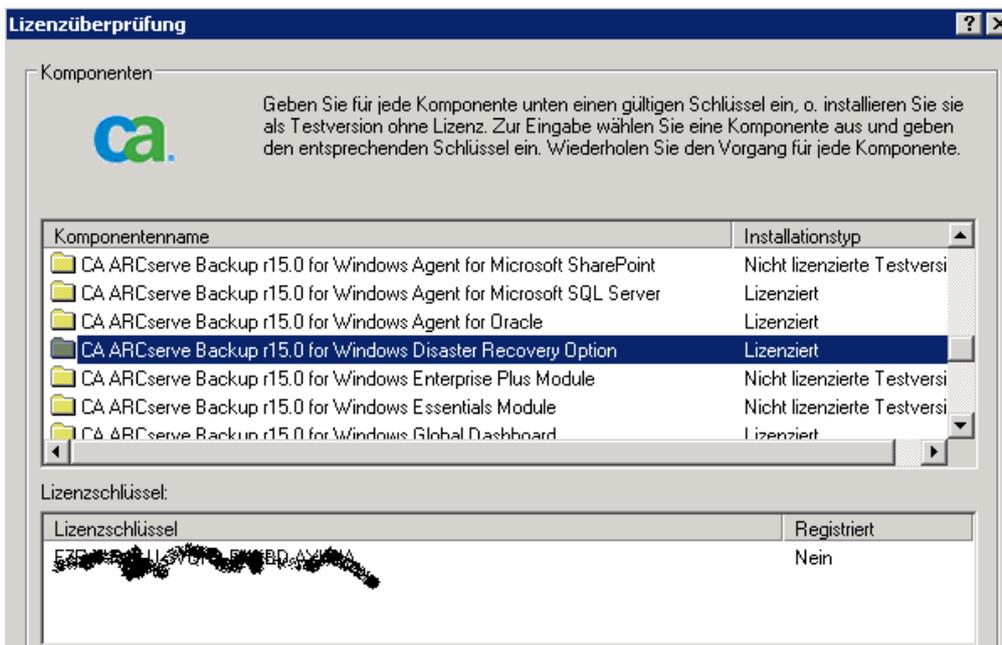


Fertigstellung der Wiederherstellung



Ergebnis

9.2 Wiederherstellung von Datenträgern



Hinweis: Um eine Gesamtwiederherstellung eines Systems oder einer Partition zu gewährleisten ist die Disaster-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 Disaster Recovery Option zusätzlich lizenziert und eingesetzt werden. Es hat sich jedoch als praktikabler erwiesen, das Backup R15 parallel mit dem D2D Produkt zu vereinen.

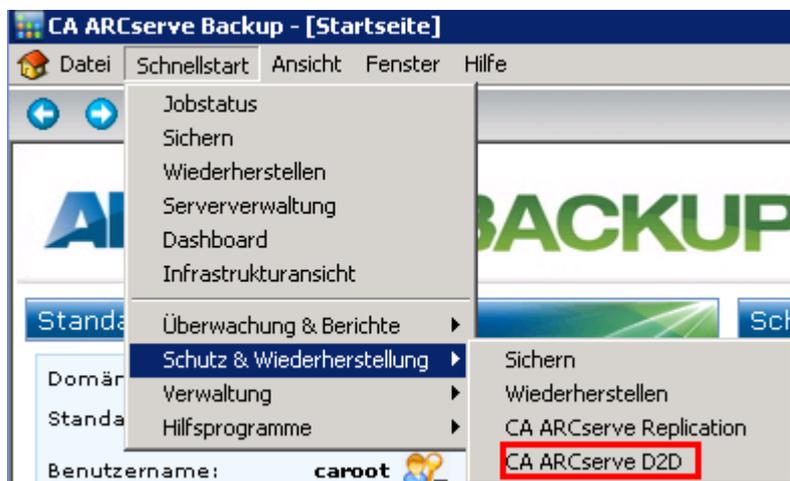
Hinweis: In dieser Empfehlung wird kurz beschrieben, wie ein Server mit der Image Funktion D2D wiederhergestellt wird. Diese Funktion ist anwendbar auf Server 2003 sowie Server 2008.

9.2.3 Parallele Installation zur CA ARCserve Backup R15

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

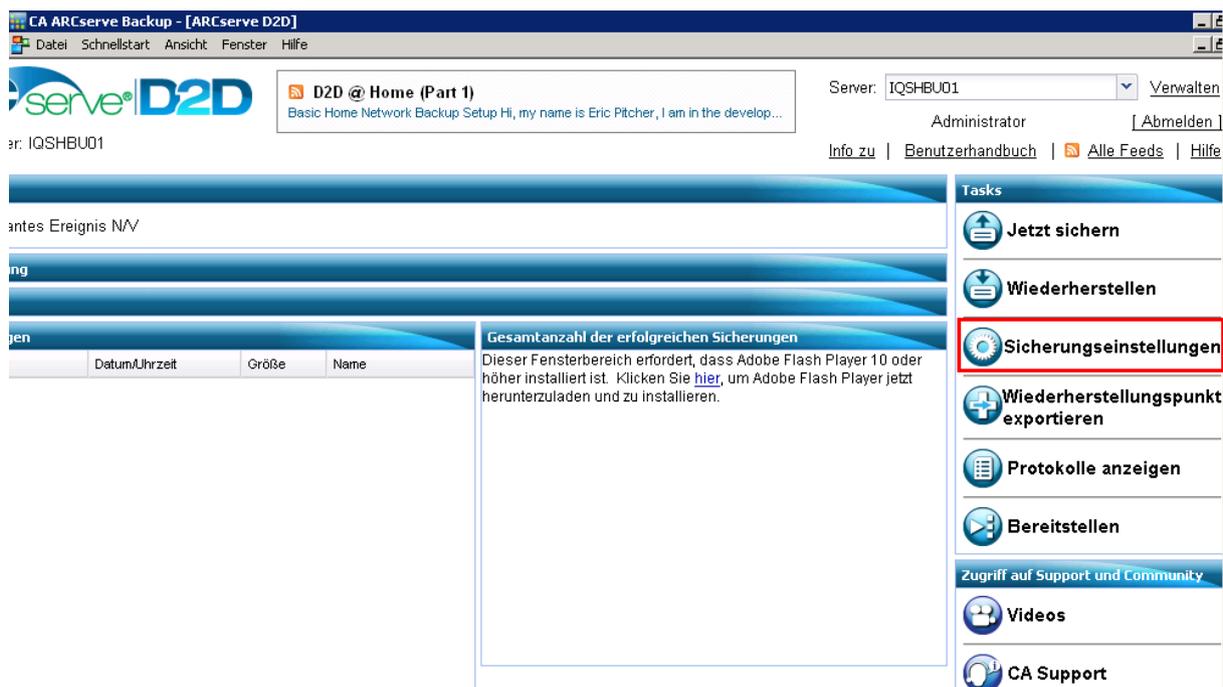
9.2.4 Voreinstellung D2D

Nach erfolgter Installation ist im ersten Schritt das D2D zu konfigurieren. D2D implementiert sich vollständig in das Backup R15 Produkt.

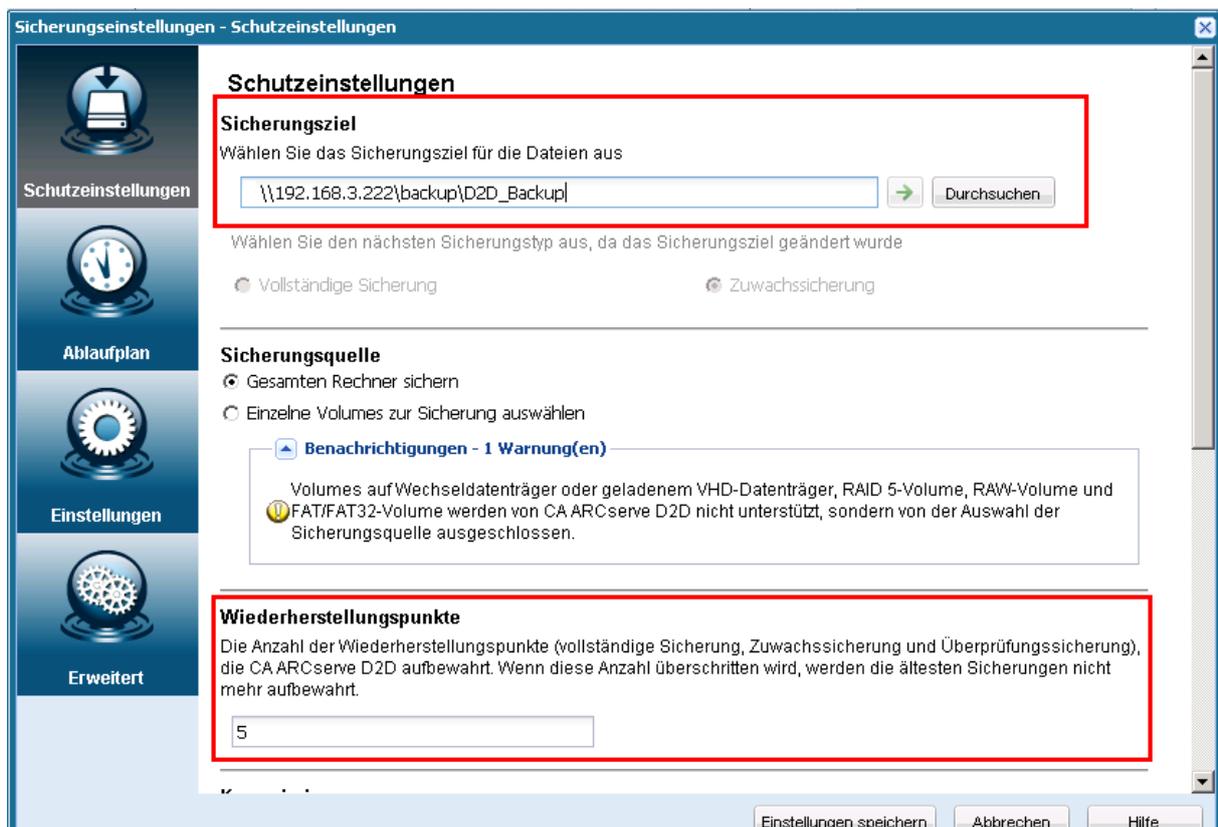




Anmeldung an der Weboberfläche



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 Wiederherstellungspunkte.

(In diesem Beispiel 5 Tage)

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

Verwaltungsserver: IQSHBU01

Job-Monitor

16 % (6,21 GB von 38,28 GB)

Typ:	Vollständige Sicherung	Startzeit:	09.02.11 10:08:42
Phase:	Volumes werden gesichert	Vergangene Zeit:	00:10:24
Durchsatz:	610,20 MB/Minute	Geschätzte verbleibende Zeit:	00:53:49

Zusammenfassung

- Letzte Sicherung - N/V**
N/V
- Wiederherstellungspunkte**
0 Wiederherstellungspunkte von 5
- Zielkapazität**
Ziel hat 425,29 GB an freiem Speicher
Pfad: \\192.168.3.222\D2D_Backup\iqshbu01

■ Sicherung 0 Byte ■ Andere 38,40 GB ■ Frei 425,29 GB

Laufendes vollständiges Backup.

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

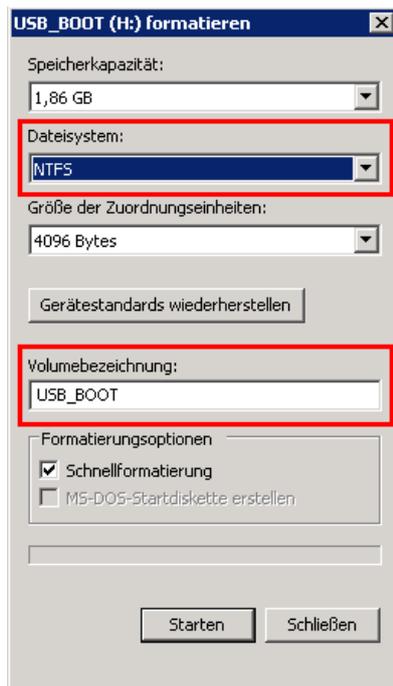
Da es sich bei den Schulservern um Geräte handelt, die kein integriertes CD / DVD Laufwerk haben, ist es erforderlich den Startvorgang von einem Wechseldatenträger zu Gewährleisten.

* BMR = Bare Metal Recovery

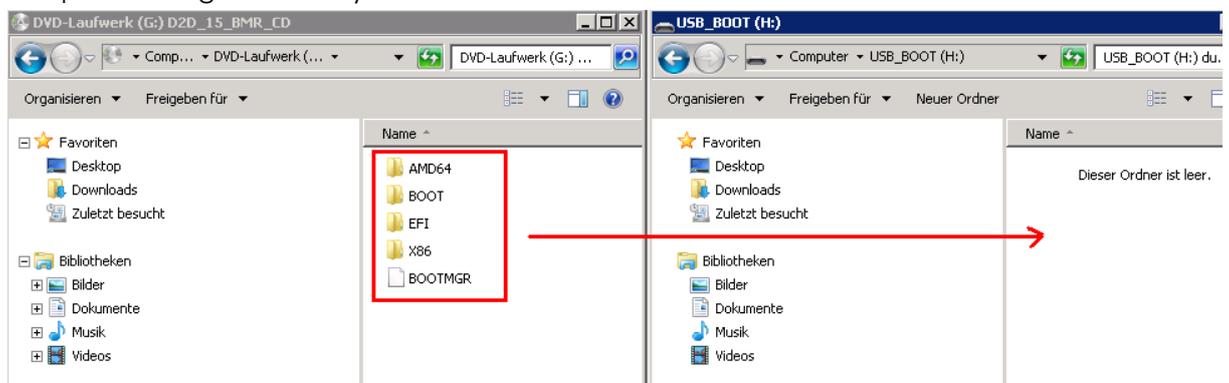
9.2.5.1 Herstellung eines USB Notfallmediums für die Komplettwiederherstellung.

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.

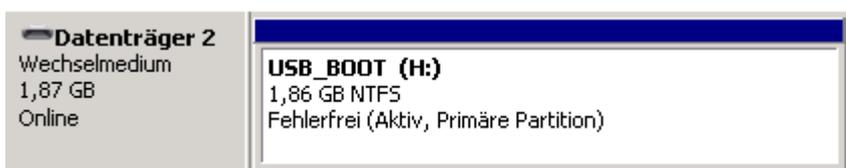
DISKPART> active

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. Einlegen 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.