

# **CA ARCserve® Backup**

**Client Agent Benutzerhandbuch**

**r15**



Diese Dokumentation und die dazugehörigen Software-Hilfeprogramme (nachfolgend als die "Dokumentation" bezeichnet) dienen ausschließlich zu Informationszwecken des Nutzers und können jederzeit durch CA geändert oder zurückgenommen werden.

Diese Dokumentation darf ohne vorherige schriftliche Genehmigung von CA weder vollständig noch auszugsweise kopiert, übertragen, vervielfältigt, veröffentlicht, geändert oder dupliziert werden. Diese Dokumentation ist vertraulich und geistiges Eigentum von CA und darf vom Benutzer weder veröffentlicht noch zu anderen Zwecken verwendet werden als solchen, die in einem separaten Vertraulichkeitsabkommen zwischen dem Nutzer und CA erlaubt sind.

Ungeachtet der oben genannten Bestimmungen ist der Nutzer, der über eine Lizenz verfügt, berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen Gebrauch für sich und seine Angestellten im Zusammenhang mit der betreffenden Software auszudrucken, vorausgesetzt, dass jedes kopierte Exemplar diesen Urheberrechtsvermerk und sonstige Hinweise von CA enthält.

Das Recht zum Anfertigen einer Kopie der Dokumentation beschränkt sich auf den Zeitraum der vollen Wirksamkeit der Produktlizenzen. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Nutzer gegenüber CA schriftlich, dass alle Kopien oder Teilkopien der Dokumentation an CA zurückgegeben oder vernichtet worden sind.

SOWEIT NACH ANWENDBAREM RECHT ERLAUBT, STELLT CA DIESE DOKUMENTATION IM VORLIEGENDEN ZUSTAND OHNE JEGLICHE GEWÄHRLEISTUNG ZUR VERFÜGUNG; DAZU GEHÖREN INSbesondere STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTTAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET CA GEGENÜBER DEM NUTZER ODER DRITTEN FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER VERWENDUNG DIESER DOKUMENTATION ENTSTEHEN; DAZU GEHÖREN INSbesondere ENTGANGENE GEWINNE, VERLORENGEGANGENE INVESTITIONEN, BETRIEBSUNTERBRECHUNG, VERLUST VON GOODWILL ODER DATENVERLUST, SELBST WENN CA ÜBER DIE MÖGLICHKEIT DIESES VERLUSTES ODER SCHADENS INFORMIERT WURDE.

Die Verwendung aller in der Dokumentation aufgeführten Software-Produkte unterliegt den entsprechenden Lizenzvereinbarungen, und diese werden durch die Bedingungen dieses Urheberrechtsvermerks in keiner Weise verändert.

Diese Dokumentation wurde von CA hergestellt.

Diese Dokumentation wird mit „Restricted Rights“ (eingeschränkten Rechten) geliefert. Die Verwendung, Duplikierung oder Veröffentlichung durch die US-Regierung unterliegt den in FAR, Absätze 12.212, 52.227-14 und 52.227-19(c)(1) bis (2) und DFARS, Absatz 252.227-7014(b)(3) festgelegten Einschränkungen, soweit anwendbar, oder deren Folgebestimmungen.

Copyright © 2010 CA. Alle Rechte vorbehalten. Alle Marken, Produktnamen, Dienstleistungsmarken oder Logos, auf die hier verwiesen wird, sind Eigentum der entsprechenden Rechtsinhaber.

## CA-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA:

- BrightStor® Enterprise Backup
- CA Antivirus
- CA ARCserve® Assured Recovery™
- CA ARCserve® Backup Agent for Advantage™ Ingres®
- CA ARCserve® Backup Agent for Novell Open Enterprise Server for Linux
- CA ARCserve® Backup Agent for Open Files on NetWare
- CA ARCserve® Backup Agent for Open Files on Windows
- CA ARCserve® Backup Client Agent for FreeBSD
- CA ARCserve® Backup Client Agent for Linux
- CA ARCserve® Backup Client Agent for Mainframe Linux
- CA ARCserve® Backup Client Agent for NetWare
- CA ARCserve® Backup Client Agent for UNIX
- CA ARCserve® Backup Client Agent for Windows
- CA ARCserve® Backup Enterprise Option for AS/400
- CA ARCserve® Backup Enterprise Option for Open VMS
- CA ARCserve® Backup for Linux Enterprise Option for SAP R/3 for Oracle
- CA ARCserve® Backup for Microsoft Windows Essential Business Server
- CA ARCserve® Backup for UNIX Enterprise Option for SAP R/3 for Oracle
- CA ARCserve® Backup for Windows
- CA ARCserve® Backup for Windows Agent for IBM Informix
- CA ARCserve® Backup for Windows Agent for Lotus Domino
- CA ARCserve® Backup for Windows Agent for Microsoft Exchange Server
- CA ARCserve® Backup for Windows Agent for Microsoft SharePoint Server
- CA ARCserve® Backup for Windows Agent for Microsoft SQL Server
- CA ARCserve® Backup for Windows Agent for Oracle
- CA ARCserve® Backup for Windows Agent for Sybase
- CA ARCserve® Backup for Windows Agent for Virtual Machines
- CA ARCserve® Backup for Windows Disaster Recovery Option
- CA ARCserve® Backup for Windows Enterprise Module

- CA ARCserve® Backup for Windows Enterprise Option for IBM 3494
- CA ARCserve® Backup for Windows Enterprise Option for SAP R/3 for Oracle
- CA ARCserve® Backup for Windows Enterprise Option for StorageTek ACSLS
- CA ARCserve® Backup for Windows Image Option
- CA ARCserve® Backup for Windows Microsoft Volume Shadow Copy Service
- CA ARCserve® Backup for Windows NDMP NAS Option
- CA ARCserve® Backup for Windows Serverless Backup Option
- CA ARCserve® Backup for Windows Storage Area Network (SAN) Option
- CA ARCserve® Backup for Windows Tape Library Option
- CA ARCserve® Backup Patch Manager
- CA ARCserve® Backup UNIX and Linux Data Mover
- CA ARCserve® D2D
- CA ARCserve® High Availability
- CA ARCserve® Replication
- CA VM:Tape for z/VM
- CA 1® Tape Management
- Common Services™
- eTrust® Firewall
- Unicenter® Network and Systems Management
- Unicenter® Software Delivery
- Unicenter® VM:Operator®

## **Technischer Support – Kontaktinformationen**

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter <http://www.ca.com/worldwide>. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.



# Inhalt

---

<b>Kapitel 1: Einführung</b>	<b>9</b>
Einführung .....	9
Vorteile der Verwendung eines Client-Agenten .....	9
Unterstützte Client-Systeme.....	10
<b>Kapitel 2: Installieren der Client-Agenten</b>	<b>13</b>
Installationshinweise.....	13
Client Agent für Windows.....	13
Client Agent für NetWare .....	13
Enterprise Option für OpenVMS .....	14
Kommunikationsanforderungen für Client Agent-Installationen auf UNIX-, Linux- und Mainframe Linux-Plattformen .....	15
Installieren der Client-Agenten .....	15
Automatische Installation des Common Agent .....	16
Installationsverzeichnisse für den Common Agent und Client Agents .....	16
<b>Kapitel 3: Hinzufügen und Konfigurieren der Client-Agenten</b>	<b>19</b>
Hinzufügen von Client-Agenten .....	19
Hinzufügen, Importieren und Exportieren von Agenten und Knoten.....	19
Manuelles Hinzufügen von Client-Agenten .....	20
Konfiguration des Client Agent für Windows .....	22
Konfigurationshinweise für Windows .....	22
Optionen der Sicherheitskonfiguration .....	23
Die Optionen "Sicherungspriorität" und "Wiederherstellen/Vergleichen - Priorität" .....	23
Mehrere gleichzeitige Wiederherstellungs- oder Vergleichsvorgänge .....	24
Optionen für die Ausführung von Sicherungen und Wiederherstellungen .....	24
Verwenden der Backup Agent-Verwaltung zum Einstellen von Windows-Parametern .....	24
Konfigurieren der Kennwortsicherheit .....	28
Anzeigen der Konfigurationsauswahl .....	28
Aktivieren der Raw-Sicherung und Wiederherstellung .....	29
Konfigurieren der Windows-Netzwerkkommunikation .....	30
Festlegen von Workstation-Kennwörtern .....	32
Erstellen einer Windows-Zugriffssteuerungsliste.....	33
Virensuche aktivieren .....	34
Benutzerdefinierbare lokale Optionen .....	35
Ausschließen von Dateien aus Datenbankanwendungen von Sicherungen mit Client Agent für Windows .....	35

---

Konfiguration des NetWare Client Agent .....	36
Konfigurationshinweise für NetWare .....	36
Konfigurieren der NetWare-Netzwerkkommunikation .....	37
Sichern der Novell-Verzeichnisdienste (Novell Directory Services, NDS) .....	38
Client Agent-Konfiguration für UNIX, Linux und Mac OS X .....	38
Konfigurationshinweise für UNIX, Linux und Mac OS X .....	39
Kontrolldateien der Client-Agenten für UNIX, Linux und Mac OS X .....	39
Common Agent-Konfigurationsdatei für UNIX, Linux und Mac OS X .....	40
Snapshot- und DirectIO-Unterstützung für UNIX .....	49
Zugriffssteuerungslisten für UNIX, Linux und Mac OS X .....	55
Konfiguration der AS/400 Enterprise Option .....	58
Konfigurieren der Voreinstellungen zum Starten .....	58
Konfiguration der Leistung .....	59
Konfigurieren der Voreinstellungen zum Stoppen .....	60
Konfiguration der OpenVMS Enterprise Option .....	60
Konfigurieren der Port-Adresse .....	61
Optimierung des TCP/IP-Stack .....	61
Verfolgungsebenen für die OpenVMS Enterprise Option .....	61
<b>Kapitel 4: Verwenden der Client-Agenten</b>	<b>63</b>
Laufzeitstatistik .....	63
Anzeigen der Laufzeitstatistik für den Client Agent für Windows .....	64
Anzeigen der Laufzeitstatistik für NetWare Client Agent .....	64
Aktivitätsprotokolle .....	64
Anzeigen der Aktivitätsprotokolle auf einem Windows-Server .....	65
Anzeigen der Aktivitätsprotokolle auf einem NetWare Client Agent-Rechner .....	66
Anzeigen der Aktivitätsprotokolle auf einem UNIX-, Linux- oder Mac OS X Client-Agent-Rechner .....	66
Aktivitätsprotokolle auf Computern mit aktiver AS/400 Enterprise Option .....	66
Aktivitätsprotokolle auf Computern mit aktiver OpenVMS Enterprise Option .....	67
Löschen von Client Agent-Protokolldateien .....	67
Sichern von Daten auf einem Windows-Netzwerkserver .....	68
Starten und Stoppen des Client-Agenten .....	68
Voraussetzungen zum Starten und Stoppen von Windows .....	68
Voraussetzungen zum Starten und Stoppen von NetWare .....	69
Voraussetzungen zum Starten und Stoppen der Client-Agenten für UNIX, Linux und Mac OS X .....	70
Voraussetzungen zum Starten und Stoppen der AS/400 Enterprise Option .....	71
Voraussetzungen zum Starten und Stoppen der OpenVMS Enterprise Option .....	72
<b>Index</b>	<b>73</b>

# Kapitel 1: Einführung

---

Dieses Kapitel enthält folgende Themen:

[Einführung](#) (siehe Seite 9)

[Vorteile der Verwendung eines Client-Agenten](#) (siehe Seite 9)

[Unterstützte Client-Systeme](#) (siehe Seite 10)

## Einführung

CA ARCserve Backup ist eine umfassende Sicherungslösung für Anwendungen, Datenbanken, verteilte Server und Dateisysteme. Sie bietet Sicherungs- und Wiederherstellungsfunktionen für Datenbanken, unternehmenswichtige Anwendungen und Netzwerk-Clients. Zu den in CA ARCserve Backup enthaltenen kompatiblen Agenten gehören auch Client-Agenten für spezifische Betriebssysteme.

Client-Agenten sind eigene Software-Pakete, die auf den Computern im Netzwerk installiert werden und die Netzwerkschnittstelle zwischen diesen Computern und CA ARCserve Backup bilden. Die Client-Agenten ermöglichen nicht nur die Netzwerkverbindung, sondern übernehmen auch gemeinsam mit den Sicherungsservern im Netzwerk Aufgaben bei der Datenspeicherung. Je nach Anzahl und Konfiguration der Netzwerkrechner, für die regelmäßige Datensicherungs- und -wiederherstellungsfunktionen benötigt werden, sind mehrere Client-Agenten erforderlich.

Dieses Handbuch enthält Informationen zum Installieren, Konfigurieren und Hinzufügen von Client-Agenten für alle Workstations und Server in einer Netzwerkspeicherumgebung.

## Vorteile der Verwendung eines Client-Agenten

Die Client-Agenten von CA ARCserve Backup wurden für Unternehmen konzipiert, die ihre Netzwerkressourcen durch Auslagerung bestimmter Aufgaben auf zentrale Sicherungsserver und -datenträger entlasten müssen. Sie erfüllen u.a. folgende Aufgaben:

- Geringere Belastung des Kommunikationsnetzwerks
- Bessere Effizienz der CA ARCserve Backup-Server durch ausgelagerte Vorbereitung der Archivdaten auf den Client-Rechnern

- Bereitstellung detaillierter Datei- und Verzeichnisinformationen über den Remote-Client an den CA ARCserve Backup-Server
- Kommunikation mit dem Server zum Durchsuchen und Auswählen der Sicherungskomponenten
- Leichtere Überwachung des Sicherungsfortschritts
- Verwaltung und Überwachung von Sicherungsprotokollen mit dem Status aller Sicherungs- und Wiederherstellungsaktivitäten
- die Sicherung von Anwendungen oder Dateisystemen ermöglichen.

Client-Agenten können außerdem über einen einzelnen CA ARCserve Backup-Server im Netzwerk den Datenschutz für alle Client-Computer verbessern.

Wenn auf den Computern in Ihrem Netzwerk die erforderlichen Client-Agenten installiert sind, kann ein einzelner CA ARCserve Backup-Server Vorgänge zur Datensicherung und -wiederherstellung auf einer Vielzahl von Computern und Betriebssystemen durchführen.

## Unterstützte Client-Systeme

CA ARCserve Backup bietet Client Agents an, die folgende Plattformen unterstützen:

**Hinweis:** Eine detaillierte Beschreibung der unterstützten Betriebssysteme und Versionen finden Sie in der Datei *Client Agents Readme*. Diese befindet sich auf dem Installationsdatenträger von CA ARCserve Backup.

- CA ARCserve Backup Client Agent für Windows. Dieser Client-Agent unterstützt:
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows 7
  - Microsoft Vista™
  - Windows 2000
  - Windows XP
  - Windows Server 2003
  - Windows Small Business Server (Windows 2000 und Windows 2003)
- CA ARCserve Backup Client Agent für NetWare

- CA ARCserve Backup Client Agent für UNIX Dieser Client-Agent unterstützt:
  - AIX
  - HP-UX
  - Solaris
  - Tru64
  - FreeBSD
- CA ARCserve Backup Client Agent für Linux. Dieser Client-Agent unterstützt:
  - Red Hat
  - SuSE
  - Turbo
  - Debian
  - RedFlag
  - Miracle Linux
  - Asianux
- CA ARCserve Backup Client Agent für Mainframe Linux. Dieser Client-Agent unterstützt:
  - Red Hat Enterprise Server
  - SLES
- CA ARCserve Backup Enterprise Option für AS/400
- CA ARCserve Backup Client Agent für Mac OS X
- CA ARCserve Backup Enterprise Option für OpenVMS



# Kapitel 2: Installieren der Client-Agenten

---

Um einen Sicherungs- oder Wiederherstellungsjob durchführen zu können, müssen Sie die geeignete CA ARCserve Backup-Client-Agent-Software installieren und starten. Der Client-Agent ermöglicht die Kommunikation zwischen einer Workstation und dem CA ARCserve Backup-Server. Dieses Kapitel behandelt die Installation der Client-Agenten.

Dieses Kapitel enthält folgende Themen:

[Installationshinweise](#) (siehe Seite 13)

[Installieren der Client-Agenten](#) (siehe Seite 15)

[Automatische Installation des Common Agent](#) (siehe Seite 16)

[Installationsverzeichnisse für den Common Agent und Client Agents](#) (siehe Seite 16)

## Installationshinweise

Die folgenden Abschnitte enthalten Informationen, die Sie vor dem Installieren der Client-Agenten lesen müssen.

### Client Agent für Windows

Vor der Installation des Client Agent für Windows ist Folgendes zu beachten:

- Bevor Sie den Client Agent für Windows ausführen können, muss der Computer für die Kommunikation über eines oder mehrere der folgenden Netzwerkprotokolle konfiguriert werden:
  - Transmission Control Protocol/Internet Protocol (TCP/IP)
  - Windows-Socket (WinSock) Direct

### Client Agent für NetWare

Vor der Installation des Client Agent für NetWare ist Folgendes zu beachten:

- Der Client Agent für NetWare kann nur auf NetWare-Servern installiert werden. Außerdem muss für eine NetWare-Installation der lokale Rechner mit dem Novell-Client für Windows ausgestattet sein.
- Der NetWare-Server muss für die Kommunikation über TCP/IP konfiguriert werden.

- Sie benötigen Supervisor-Rechte für die eDirectory-Struktur des NetWare-Computers, auf dem Sie diesen Client-Agenten installieren. Weitere Informationen finden Sie in Ihrer Dokumentation zu Novell NetWare.
- Beste Leistung erzielen Sie mit den neuesten Prozessen für CLIB (NetWare C Library) und SMS (Systems Management Server).
- Die NLMs (NetWare Loadable Modules, über NetWare ladbare Programmmoduln) sind von Novell erhältlich.

## Enterprise Option für OpenVMS

Vor der Installation der Enterprise Option für OpenVMS ist Folgendes zu beachten:

- Computer, auf denen die unterstützten Alpha- und VAX-Betriebssysteme ausgeführt werden, können entweder TCP oder User Data Protocol (UDP) mit einem der folgenden Übertragungssoftwareprogramme verwenden:
  - Compaq UCX 4.2 eco 3 (auf Alpha)
  - Compaq UCX 3.3 eco 13 (auf VAX)
  - Compaq TCP/IP Version 5.0 bis 5.3
  - Process Software Multinet Version 4.1B (mit Patches) bis Version 4.4
  - Process Software TCPWARE Version 5.3 und 5.4

**Wichtig!** Falls nötig, können Sie auf demselben Computer zwei oder mehr dieser Übertragungssoftwarepakete installieren. Sie können allerdings immer nur jeweils ein Paket ausführen. Führen Sie nie zwei oder mehr dieser Übertragungssoftwarepakete gleichzeitig auf demselben Computer aus.

**Hinweis:** Wenn Sie zu einem beliebigen Zeitpunkt OpenVMS TCP/IP-Stacks ändern, müssen Sie die OpenVMS Enterprise Option neu installieren.

- Sie sollten Ihre OpenVMS-System-Festplatte sichern, bevor Sie die OpenVMS Enterprise Option installieren.
- Stellen Sie sicher, dass mindestens 10 Blöcke freier Speicherplatz für die Setup-Datei verfügbar sind.

## Kommunikationsanforderungen für Client Agent-Installationen auf UNIX-, Linux- und Mainframe Linux-Plattformen

Damit sichergestellt wird, dass Primärserver und Mitgliedsserver von CA ARCserve Backup mit den CA ARCserve Backup-Agenten kommunizieren können, die auf UNIX-, Linux-, und Mainframe Linux-Computern installiert sind, müssen Sie CA ARCserve Backup erlauben, gegebenenfalls mit dem Agenten über die Firewall zu kommunizieren, die auf den Agent-Computern konfiguriert ist. Sie können CA ARCserve Backup erlauben, mit den Agent-Computern zu kommunizieren, indem Sie CA ARCserve Backup zur Liste der Ausnahmen der Firewall auf den Agent-Computern hinzuzufügen.

Es wird empfohlen, CA ARCserve Backup zur Liste der Ausnahmen für die Firewall auf den Agent-Computern hinzuzufügen, bevor Sie die Agenten installieren.

Diese Anforderung wirkt sich auf die folgenden Komponenten von CA ARCserve Backup aus:

- Client Agent für UNIX
- Client Agent für Linux
- Client Agent für Mainframe Linux
- Oracle Agent auf Unix-Plattformen
- Oracle Agent auf Linux-Plattformen
- UNIX- und Linux-Data Mover

Informationen zur Konfiguration der Firewall auf den Agent-Computern finden Sie in der plattformspezifischen Dokumentation.

**Hinweis:** Standardmäßig wird die Kommunikation von CA ARCserve Backup über Port 6051 abgewickelt.

## Installieren der Client-Agenten

Windows-Client Agents oder plattformübergreifende Agents können Sie mit Hilfe der DVD "CA ARCserve Backup für Windows" installieren.

Weitere Informationen zur Installation von CA ARCserve Backup Client Agents finden Sie über die folgenden Verknüpfungen im Installationsbrowser von CA ARCserve Backup:

- Installationsanweisungen für CA ARCserve Backup Client Agents für Nicht-Windows-Plattformen.
- Installationsanweisungen für UNIX- und Linux-Data Mover für CA ARCserve Backup.

## Automatische Installation des Common Agent

Wenn Sie den Client-Agent für UNIX, Linux oder Mac OS X installieren, wird CA ARCserve Backup Common Agent automatisch installiert.

## Installationsverzeichnisse für den Common Agent und Client Agents

Die folgende Tabelle beschreibt die Standardinstallationspfade für den CA ARCserve Backup Common Agent und die CA ARCserve Backup Client Agents für UNIX- und Linux-Plattformen.

<b>Plattform</b>	<b>Version</b>	<b>Common Agent-/Agent-Konfigurationsdatei</b>	<b>Client Agent (Dateisystem-Agent)</b>
AIX		/opt/CA/ABcmagt	/opt/CA/ABuagent
HP		/opt/CA/ABcmagt	/opt/CA/ABuagent
Solaris	SPARC 8, 10 x86	/opt/CA/BABcmagt	/opt/CA/BABuagent
Solaris	SPARC 9, 10	/opt/CA/ABcmagt	/opt/CA/ABuagent
Linux	SUSE	/opt/CA/ABcmagt	/opt/CA/ABuagent
	Redhat		
	Linux-OES		
	Asianux		
	Miracle		
	Red Flag		
	Turbo Linux		
Mainframe Linux	Red Hat SUSE	/opt/CA/BABcmagt	/opt/CA/BABuagent
FreeBSD		/opt/CA/BABcmagt	/opt/CA/BABuagent
Debian		/opt/CA/ABcmagt	/opt/CA/ABuagent
ESX		/opt/CA/ABcmagt	/opt/CA/ABuagent
Tru64		/opt/CA/BABcmagt	/opt/CA/BABuagent

**Hinweis:** Die obigen Verzeichnisse erscheinen auch in der Common Agent-Konfigurationsdatei (agent.cfg) mit anderen verwandten Konfigurationsdateien für die Dateisystem-Agents und den Agent für Oracle.

Eine komplette Liste der unterstützten Betriebssystemversionen finden Sie in der Client Agent-Readme-Datei auf dem Installationsdatenträger von CA ARCserve Backup.



# Kapitel 3: Hinzufügen und Konfigurieren der Client-Agenten

---

Nach der Installation von CA ARCserve Backup und der verschiedenen Client-Agenten müssen Sie jeden Client Agent-Rechner in Ihrem Netzwerk dem Sicherungsserver hinzufügen und konfigurieren. In diesem Kapitel werden die Verfahren zum Hinzufügen und Konfigurieren der Client-Agenten behandelt.

Dieses Kapitel enthält folgende Themen:

- [Hinzufügen von Client-Agenten](#) (siehe Seite 19)
- [Konfiguration des Client Agent für Windows](#) (siehe Seite 22)
- [Konfiguration des NetWare Client Agent](#) (siehe Seite 36)
- [Client Agent-Konfiguration für UNIX, Linux und Mac OS X](#) (siehe Seite 38)
- [Konfiguration der AS/400 Enterprise Option](#) (siehe Seite 58)
- [Konfiguration der OpenVMS Enterprise Option](#) (siehe Seite 60)

## Hinzufügen von Client-Agenten

Wenn Sie CA ARCserve Backup auf einem Windows-Server installiert haben, können Sie die Client-Agenten in Ihrem Netzwerk entweder mit Hilfe der Funktion zum Hinzufügen, Importieren und Exportieren von Knoten oder manuell hinzufügen. Die folgenden Abschnitte enthalten Informationen zu beiden Methoden.

### Hinzufügen, Importieren und Exportieren von Agenten und Knoten

Das Einrichten eines Jobs in einer Umgebung mit vielen Agenten und Knoten kann eine zeitaufwändige und mühsame Aufgabe sein. Wenn mehrere Agenten und Knoten gesichert werden sollen, ist es möglicherweise sehr zeitintensiv, diese Agenten und Knoten jeweils einzeln zum Sicherungs-Manager hinzuzufügen. Mit den Funktionen zum Hinzufügen, Importieren und Exportieren von Agenten bzw. Knoten können Sie mehrere Knoten und Agenten über die CA ARCserve Backup-Benutzeroberfläche hinzufügen, unabhängig davon, ob die Knoten und Agenten gesichert werden sollen.

**Hinweis:** Über die Central Agent-Verwaltung können Knoten auch hinzugefügt, importiert oder exportiert werden.

Sie haben die folgenden zwei Möglichkeiten, mit der Funktion zum Hinzufügen, Importieren und Exportieren von Knoten dem System mehrere Knoten und Agenten hinzuzufügen:

**Hinzufügen mehrerer Agenten und Knoten über die Benutzeroberfläche**

1. Wählen Sie im Sicherungs-Manager auf der Registerkarte "Quelle" bzw. im Wiederherstellungs-Manager auf der Registerkarte "Ziel" einen Knoten aus.
2. Geben Sie im Dialogfeld "Agenten hinzufügen/importieren/exportieren" die Namen aller Knoten und Agenten manuell ein, oder wählen Sie die Knoten in der links angezeigten Liste der Knoten und Agenten aus, die mit Auto-Discovery gefunden wurden.
3. Geben Sie einen Benutzernamen und ein Kennwort für die Knoten ein.
4. Speichern Sie die Informationen in der CA ARCserve Backup-Datenbank.
5. Zeigen Sie die Knoten und Agenten in der Sicherungs-Manager-Quellstruktur oder in der Central Agent-Verwaltung an.

**Hinzufügen mehrerer Knoten und Agenten mit Hilfe einer CSV- oder TXT-Datei**

1. Wählen Sie im Sicherungs-Manager auf der Registerkarte "Quelle" bzw. im Wiederherstellungs-Manager auf der Registerkarte "Ziel" einen Knoten aus.
2. Wählen Sie die CSV- oder TXT-Datei dann mit Hilfe der Importfunktion im Dialogfeld "Agenten hinzufügen/importieren/exportieren" über die Benutzeroberfläche aus.  
Die Namen der Knoten und Agenten werden aus der CSV- oder TXT-Datei importiert und zum System hinzugefügt.
3. Geben Sie einen Benutzernamen und ein Kennwort für die Knoten und Agenten ein.
4. Zeigen Sie die Knoten und Agenten in der Quellbaumstruktur des Sicherungs-Managers an.

## Manuelles Hinzufügen von Client-Agenten

Wenn Auto-Discovery aus einem Grund nicht alle Client-Agenten in Ihrem Netzwerk erkennt oder wenn Sie einen bestimmten Client-Agenten hinzufügen möchten, können Sie einen Client-Agenten manuell zu einem Windows- oder NetWare-Server hinzufügen, der den Windows-Manager verwendet. Zum manuellen Hinzufügen eines Client-Agenten müssen Sie jeden Client Agent-Rechner zum Sicherungs-Manager hinzufügen.

**So fügen Sie Client-Agenten manuell hinzu:**

1. Klicken Sie im Fenster "Sicherungs-Manager" auf die Registerkarte "Quelle".
2. Klicken Sie mit der rechten Maustaste auf das entsprechende Client-Agent-Objekt, z. B. "Windows-Systeme".
3. Wählen Sie "Rechner/Objekt hinzufügen".

Das Dialogfeld "Agent hinzufügen" wird angezeigt.



4. Geben Sie im Textfeld "Hostname" den Namen des Computers ein.
- Hinweis:** Wenn Sie einen Client Agent für NetWare hinzufügen, müssen Sie den Novell-Servernamen als Hostnamen verwenden.
5. Wählen Sie das Protokoll aus, das für die Verbindung mit dem Computer verwendet werden soll:
    - **TCP/IP:** Wählen Sie TCP/IP und, wenn Sie einen Client Agent für Windows hinzufügen, die Option "Computernamenauflösung verwenden". Mit der Computernamenauflösung kann der lokale Windows-Computer automatisch die IP-Adresse des Remote-Rechners beim Herstellen der Verbindung für Sicherungen und Wiederherstellungen erkennen. Dies ist die empfohlene Methode; sie funktioniert auch, wenn Sie die IP-Adresse des Computers nicht kennen.
- Hinweis:** Wenn der Windows-Zielcomputer über eine dynamische IP-Adresse verfügt, sollten Sie die Option für die Computernamenauflösung aktivieren.

Wenn Sie keinen Windows-Client-Agenten hinzufügen, die Computernamenauflösung auf Grund verschiedener DNS-Server- oder Netzwerkkonfigurationsprobleme fehlschlägt oder der Zielcomputer über mehrere IP-Adressen verfügt und Sie sicherstellen möchten, dass eine bestimmte Adresse verwendet wird, dann aktivieren Sie die Option für die Computernamenauflösung nicht und geben eine IP-Adresse ein.

6. Klicken Sie auf "Hinzufügen".

Der Client-Agent wird dem Server hinzugefügt.

## Konfiguration des Client Agent für Windows

In den folgenden Abschnitten werden die Konfigurationsoptionen für Client Agent für Windows erläutert.

### Konfigurationshinweise für Windows

Allgemeine Informationen zur Konfiguration von Client Agent für Windows:

- **Systemstatus wiederherstellen:** Der Systemstatus unterstützt die Option Am ursprünglichen Speicherort wiederherstellen.  
**Hinweis:** Der Systemstatus unterstützt auch die Wiederherstellung an einem alternativen Speicherort, es wird jedoch kein betriebsbereites System erneut erstellt, da sich die Dateien in Standardverzeichnissen befinden, die vom Client-Agenten während der Wiederherstellung erstellt wurden.
- **Freigabeunterstützung:** Wurde die Option Agent verwenden gewählt, sichert der Client Agent gewählte Freigaben über das Objekt Bevorzugte Freigaben/Rechner im Sicherungs-Manager, indem der Freigabename in den richtigen Pfad konvertiert wird.  
**Hinweis:** Auf Windows-Plattformen werden Freigaben als Ziel weder wiederhergestellt noch unterstützt, es sei denn, es handelt sich um Verwaltungsfreigaben.
- **Wiederherstellung der Systemstruktur:** Mit der Funktion KeysNotToRestore sollen wichtige Systemregistrierungsschlüssel während einer regulären Wiederherstellung der Client Agent-Systemstruktur geschützt werden. Diese Funktion ist jedoch nicht verfügbar, wenn Sie einzelne Systemschlüssel in einer Client Agent-Registrierungssitzung wiederherstellen möchten.

## Optionen der Sicherheitskonfiguration

Die Sicherheitsoptionen für den Client Agent für Windows werden im Dialogfeld "Konfiguration" definiert. Wählen Sie einen der beiden folgenden Sicherheitstypen aus:

### **Systemsicherheit**

Verwendet zur Durchführung von Sicherungs-, Wiederherstellungs- und Vergleichsvorgängen die Sicherheitseinstellungen von Windows. Der Client Agent ahmt dabei den aktiven Netzwerkbenutzer nach, verwendet für die Anmeldung also dessen Benutzernamen und Kennwort. Der Benutzername und das Kennwort sollten einem gültigen Benutzer in der lokalen Benutzerdatenbank bzw. (falls die Workstation Mitglied einer Domäne ist) in der Domänendatenbank zugeordnet sein.

### **Kennwortsicherheit**

Ermöglicht das Festlegen individueller Kennwörter für die Sicherheit. Mit dieser Einstellung kann der Client Agent unter Verwendung des lokalen Systemkontos ausgeführt werden. Standardmäßig ist die Kennwortsicherheit deaktiviert.

**Hinweis:** Wenn Kennwortsicherheit ausgewählt wird und DSA-basierte Datenbankagenten (zum Beispiel Sybase, Informix usw.) auf dem Rechner installiert sind, wird eine vollständige Knotensicherung nicht unterstützt. Wenn Sie nur Datenbanken sichern möchten, müssen Sie die Sicherheitsinformationen im Dialogfelds "Sicherheits- und Agent-Informationen" ändern, bevor Sie den Job übergeben.

## Die Optionen "Sicherungspriorität" und "Wiederherstellen/Vergleichen - Priorität"

Die Prozesspriorität für den Client Agent für Windows wird im Dialogfeld "Konfiguration" definiert. Wählen Sie eine der folgenden Einstellungen für die Sicherungspriorität und die Priorität für Wiederherstellen/Vergleichen:

### **Hoch**

Die Vordergrundverarbeitung führt Client-Agent-Funktionen vor anderen Prozessen aus.

### **Normal**

Die Standardverarbeitung führt Client-Agent-Funktionen ohne besonderen Status aus.

### **Niedrig**

Die Standardverarbeitung führt Client-Agent-Funktionen aus, wenn andere Prozesse ruhen.

## Mehrere gleichzeitige Wiederherstellungs- oder Vergleichsvorgänge

Simultane Wiederherstellungs- und Vergleichsvorgänge werden für den Client Agent für Windows im Dialogfeld "Konfiguration" aktiviert. Aktivieren Sie im Dialogfeld "Konfiguration" das Kontrollkästchen "Mehrere gleichzeitige Wiederherstellungs- oder Vergleichsvorgänge zulassen", damit der Client Agent für Windows mehrere gleichzeitige Wiederherstellungs- oder Vergleichsvorgänge akzeptiert.

## Optionen für die Ausführung von Sicherungen und Wiederherstellungen

Die Ausführungsoptionen für den Client Agent für Windows werden im Dialogfeld "Konfiguration" definiert. Wählen Sie die Programme vor und nach der Ausführung, und definieren Sie die Ausführungsverzögerung.

### Vor-Ausführung

Geben Sie den Namen der Stapelverarbeitungsprogramme (z. B. "C:\WINAGENT\PRE.CMD") ein, die vor dem Sicherungs- bzw. Wiederherstellungsvorgang automatisch ausgeführt werden sollen.

### Nach-Ausführung

Geben Sie den Namen der Stapelverarbeitungsprogramme (z. B. "C:\WINAGENT\POST.CMD") ein, die nach dem Sicherungs- bzw. Wiederherstellungsvorgang automatisch ausgeführt werden sollen.

### Ausführungsverzögerung

Geben Sie die Anzahl von Sekunden an, die der Client-Agent vor oder nach der Ausführung des Stapelverarbeitungsjobs warten soll.

## Verwenden der Backup Agent-Verwaltung zum Einstellen von Windows-Parametern

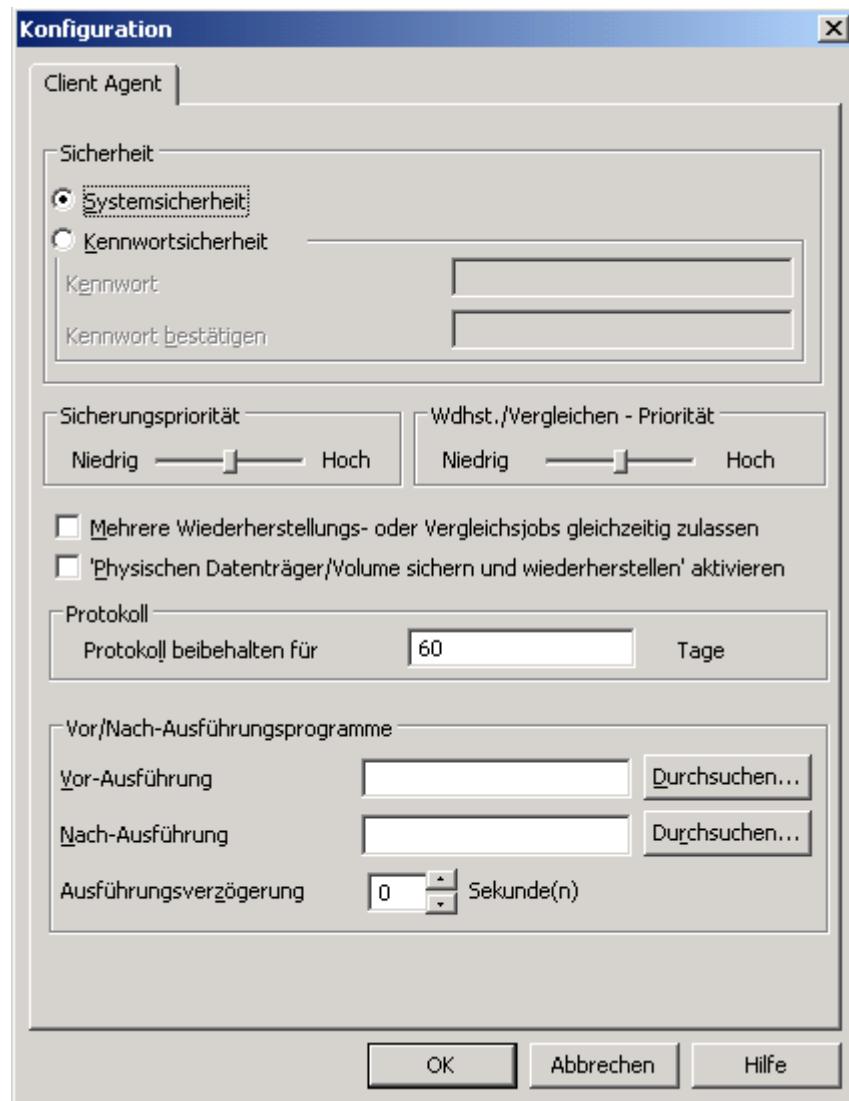
### So verwenden Sie Backup Agent-Verwaltung zum Einstellen von Windows-Parametern

1. Klicken Sie dazu auf "Start", "Programme" bzw. "Alle Programme", "CA", "ARCserve Backup-Agenten" und dann auf "Backup Agent - Verwaltung".

**Hinweis:** Der Inhalt des Fensters kann sich für die verschiedenen Client Agents je nach Betriebssystem leicht unterscheiden.

2. Wählen Sie in der Agent-Verwaltung die Registerkarte "Optionen".

Das Dialogfeld "Konfiguration" wird geöffnet.



Im Dialogfeld "Konfiguration" können Sie die folgenden Einstellungen definieren:

- **Sicherheitstyp:** Wählen Sie einen der beiden folgenden Sicherheitstypen aus:

**Systemsicherheit:** Wählen Sie diese Sicherheitsoption, wenn Sie die Windows-Sicherheit für die Durchführung von Sicherungs-, Vergleichs- und Wiederherstellungsvorgängen verwenden möchten. Der Client Agent ahmt dabei den aktiven Netzwerkbenutzer nach, verwendet für die Anmeldung also dessen Benutzernamen und Kennwort. Der Benutzername und das Kennwort sollten einem gültigen Benutzer in der lokalen Benutzerdatenbank bzw. (falls die Workstation Mitglied einer Domäne ist) in der Domänendatenbank zugeordnet sein.

**Hinweis:** Bei der Auswahl von "Systemsicherheit" werden Datenbankdateien von Exchange Server 2010 nicht gesichert (also übersprungen), wenn Sie den Client Agent verwenden, um Partitionen, Ordner oder Dateien zur Sicherung auswählen, wenn es sich beim Sicherungskonto des Client Agent um ein Domänenkonto mit mindestens der Rolle "Nur Organisations-Verwaltung anzeigen" handelt. Datenbankdateien von Exchange Server 2010 werden nicht übersprungen, wenn Sie Kennwortsicherheit auswählen oder eine andere Kontorolle verwenden, wie beispielsweise lokaler Administrator oder Domänenkonto ohne Berechtigung "Nur Organisations-Verwaltung anzeigen". Das System zeigt eine Warnung an, wenn diese Datenbankdateien verwendet werden.

**Kennwortsicherheit:** Wählen Sie diese Sicherheitsoption, um ein individuelles Sicherheitskennwort festzulegen. Mit dieser Einstellung kann der Client Agent unter Verwendung des lokalen Systemkontos ausgeführt werden. Standardmäßig ist die Kennwortsicherheit deaktiviert.

- **Prozesspriorität:** Mit diesen Einstellungen wird die Priorität der für Sicherungs-, Wiederherstellungs- und Vergleichsvorgänge benötigten Prozesse bestimmt. Wählen Sie eine der folgenden Einstellungen für die Sicherungspriorität und die Priorität für Wiederherstellen/Vergleichen:

**Hoch:** Die Vordergrundverarbeitung führt Client Agent-Funktionen vor anderen Operationen aus.

**Normal:** Die Standardverarbeitung führt Client Agent-Funktionen ohne besonderen Status aus.

**Niedrig:** Die Standardverarbeitung führt Client Agent-Funktionen aus, wenn andere Prozesse ruhen.

- **Mehrere gleichzeitige Wiederherstellungs- oder Vergleichjobs zulassen:** Aktivieren Sie diese Option, damit der Client Agent für Windows mehrere gleichzeitige Wiederherstellungs- oder Vergleichjobs akzeptiert.  
**Hinweis:** Standardmäßig ist diese Option deaktiviert, um sicherzustellen, dass neue Sicherungs- und Wiederherstellungsjobs des gleichen Datensatzes nicht während eines aktiven Wiederherstellungsjobs versehentlich gestartet werden. In diesem Fall verweigert der Agent die Anforderung des neuen Jobs und gibt die Meldung aus, dass der Client Agent für den CA ARCserve Backup-Server belegt ist.
- **'Physischen Datenträger/Volume sichern und wiederherstellen' aktivieren:** Ermöglicht die Durchführung von Raw-Sicherungen und -Wiederherstellungen auf physischen Datenträgern und Volumes.  
**Hinweis:** Weitere Informationen finden Sie im *Administrationshandbuch*.
- **Protokoll:** Die Protokolldatei wird unter dem folgenden Pfad gespeichert: <ARCserve\_HOME>\ARCserve Backup Client Agent for Windows\ntagent.log In dieser Protokolldatei werden die Protokolle aller ausgeführten Jobs gespeichert.  
**Protokoll speichern:** Gibt die Anzahl der Tage an (60 Tage sind Standard), die das Agentenprotokoll gespeichert werden soll. Nachdem die angegebene Anzahl an Tagen abgelaufen ist, wird das Protokoll gelöscht, sobald die nächste Agentensicherung, Wiederherstellung oder ein Vergleichsjob durchgeführt wird.
- **Programme vor und nach der Ausführung:** Wählen Sie eine der folgenden Ausführungsoptionen:
  - Vor-Ausführung:** Geben Sie die Namen der Batch-Programme (z. B. C:\WINAGENT\PRE.CMD) ein, die vor dem Sicherungs- bzw. Wiederherstellungsvorgang automatisch ausgeführt werden sollen.
  - Nach-Ausführung:** Geben Sie die Namen der Batch-Programme (z. B. C:\WINAGENT\POST.CMD) ein, die nach dem Sicherungs- bzw. Wiederherstellungsvorgang automatisch ausgeführt werden sollen.

3. Klicken Sie auf "OK", um die Änderungen zu speichern und das Dialogfeld zu schließen.

**Hinweis:** Wenn Sie die Konfiguration später ändern möchten, müssen Sie erneut das Dialogfeld "Konfiguration" aufrufen.

## Konfigurieren der Kennwortsicherheit

Der Client Agent-Dienst verwendet den Benutzernamen und das zugewiesene Kennwort des Knotens (Rechners), um sich im CA ARCserve Backup -Netzwerk anzumelden.

### **So richten Sie die Kennwortsicherheit für den Client Agent ein:**

1. Starten Sie den Sicherungs-Manager, und klicken Sie mit der rechten Maustaste auf den Rechnernamen. Ein Kontextmenü wird angezeigt.
2. Wählen Sie im Kontextmenü den Befehl "Sicherheit", um das Dialogfeld "Sicherheit" zu öffnen. Im Feld Benutzername sollte bereits der dem Client Agent zugewiesene Benutzername eingetragen sein.
3. Geben Sie das Kennwort für den Client Agent ein.

**Hinweis:** Der Benutzername und das Kennwort sollten einem gültigen Benutzer in der lokalen Datenbank des Rechners bzw. (falls die Workstation Mitglied einer Domäne ist) in der Domänendatenbank zugeordnet sein.

Wenn Sie das zu verwendende Benutzerkonto angeben, muss außerdem möglicherweise zwischen zwei Konten mit dem gleichen Namen (z.B. Administrator) unterschieden werden. Geben Sie hierzu an, wo Windows das jeweilige Konto finden kann. Sie können den Speicherort des Client-Objekts bei der Angabe des Benutzernamens in Form eines Strukturmamens eingeben. Für die Domäne NTDEV, die eine Workstation namens ENGINEER enthält, sind die entsprechenden Administratorkonten beispielsweise:

NTDEV\Administrator

ENGINEER\Administrator

## Anzeigen der Konfigurationsauswahl

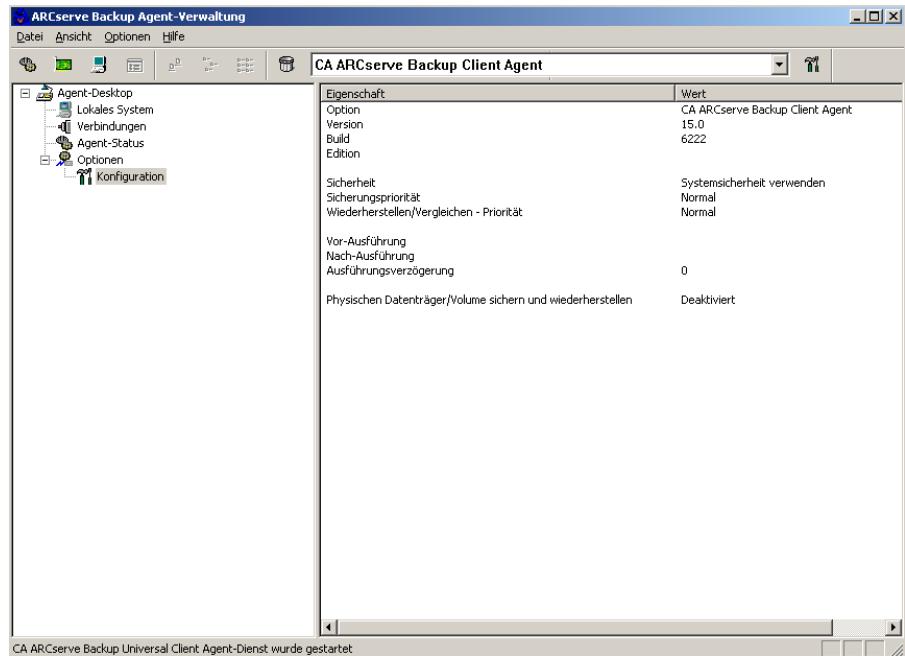
Bevor Sie Änderungen an Ihren Konfigurationseinstellungen vornehmen, sollten Sie Ihre aktuellen Einstellungen überprüfen.

### **So zeigen Sie Ihre Konfiguration an:**

1. Öffnen Sie die Backup Agent-Verwaltung.

2. Erweitern Sie "Optionen", und wählen Sie dann "Konfiguration" aus.

Die aktuellen Einstellungen werden angezeigt.



## Aktivieren der Raw-Sicherung und Wiederherstellung

Sie können CA ARCserve Backup verwenden, um Raw-Sicherungen und Wiederherstellungen von physischen Datenträgern und Volumen auszuführen.

Die Möglichkeit, eine Raw-Sicherung und Wiederherstellung von physischen Datenträgern und Volumes durchzuführen, ist standardmäßig deaktiviert. Sie müssen die Option für jeden Agenten aktivieren.

### **So aktivieren Sie die Raw-Sicherung und Wiederherstellung eines physischen Datenträgers oder Volumes:**

1. Klicken Sie im Windows-Startmenü auf "Start", zeigen Sie auf "Programme", "CA", "ARCserve Backup", und klicken Sie auf "Backup Agent-Verwaltung".  
Das Fenster "ARCserve Backup Agent-Verwaltung" wird geöffnet.
2. Klicken Sie auf "Optionen", "Konfiguration".  
Das Fenster "Konfiguration" wird geöffnet.

3. Klicken Sie auf "Physicalen Datenträger/Volume sichern und wiederherstellen" aktivieren".
4. Klicken Sie auf "OK".

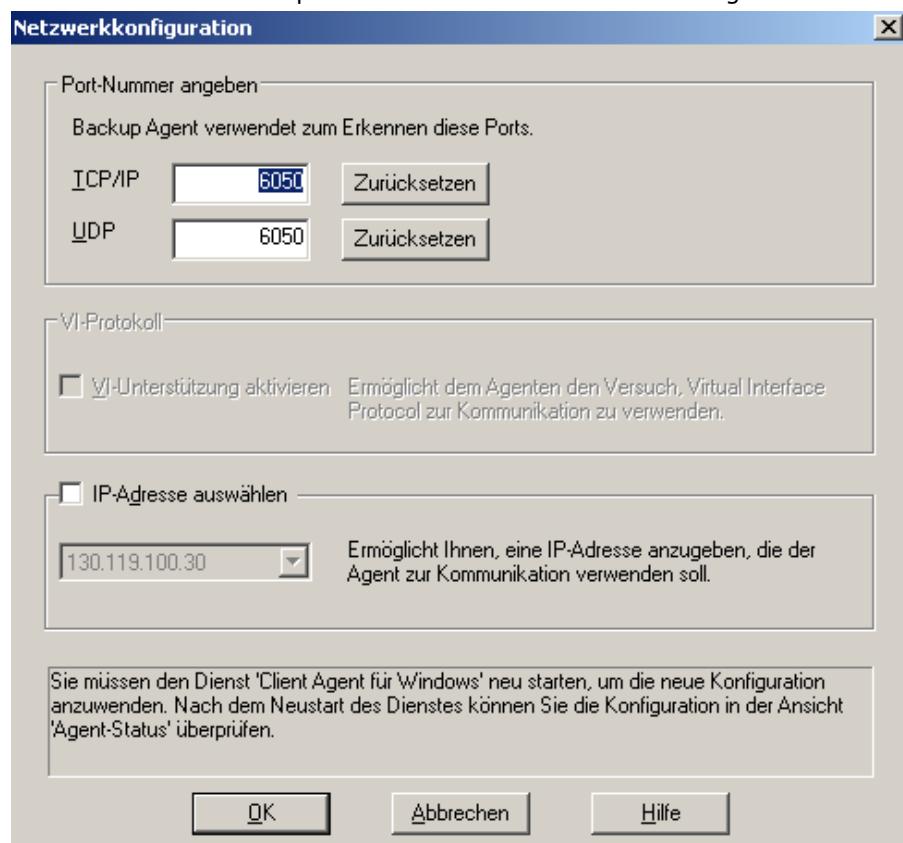
Die Funktion zur Raw-Sicherung und Wiederherstellung wird für den Agenten aktiviert. Weitere Informationen zur Durchführung von Raw-Sicherungen und -Wiederherstellungen finden Sie im *Administrationshandbuch*.

## Konfigurieren der Windows-Netzwerkkommunikation

CA ARCserve Backup Client Agent-Dienste werden von allen konfigurierten Client-Agenten gemeinsam genutzt. Standardmäßig verwenden Windows Client Agents den TCP/UDP-Port 6050. Sie können dieses Verhalten über die Backup Agent-Verwaltung im Menü "Netzwerkkonfiguration" ändern.

### So konfigurieren Sie die Windows-Netzwerkkommunikation:

1. Öffnen Sie die Backup Agent-Verwaltung.
2. Wählen Sie im Menü "Optionen" den Befehl "Netzwerkkonfiguration" aus:



3. In diesem Dialogfeld können Sie die folgenden Netzwerkparameter für den Client Agent festlegen:

#### **Port-Nummer angeben**

Übernehmen Sie die Standardwerte, oder geben Sie die Port-Werte ein, die CA ARCserve Backup verwenden soll. Wenn Sie den ursprünglichen Standardpfad verwenden möchten, klicken Sie auf "Zurücksetzen". Die aktualisierten Port-Informationen werden in der lokalen Datei "PortsConfig.cfg" unter "\Programme\CA\SharedComponents\ARCserve Backup" gespeichert.

**Hinweis:** Aktualisierte Port-Informationen müssen in der Server-Komponente von CA ARCserve Backup registriert werden. Hierzu müssen Sie die Remote-Server-Datei PORTSCONFIG.CFG ändern. Weitere Informationen zur Port-Konfiguration finden Sie im *Implementierungshandbuch*.

#### **IP-Adresse auswählen**

Der Client Agent für Windows unterstützt die Verwendung mehrerer Netzwerkschnittstellenkarten (NICs). Bei Computern mit mehreren Netzwerkkarten überprüft der Agent alle aktiven NICs im Rechner. Sie können diese Einstellung manuell außer Kraft setzen, indem Sie die IP-Adresse der Netzwerkkarte auswählen, die ausschließlich für Sicherungszwecke genutzt werden soll. Wenn Sie diese Konfiguration definieren, hört der Client Agent nur diese Netzwerkkarte ab. Alle anderen Netzwerkkarten werden ignoriert und Sie können über deren IP-Adressen keine Verbindung zum Client Agent herstellen.

Alle aktualisierten Informationen müssen auch in der Windows-Datei "PortsConfig.cfg" geändert und ins CA ARCserve Backup-Stammverzeichnis kopiert werden. Im Folgenden sehen Sie ein Beispiel für die Datei CAPORTCONFIG.CFG:

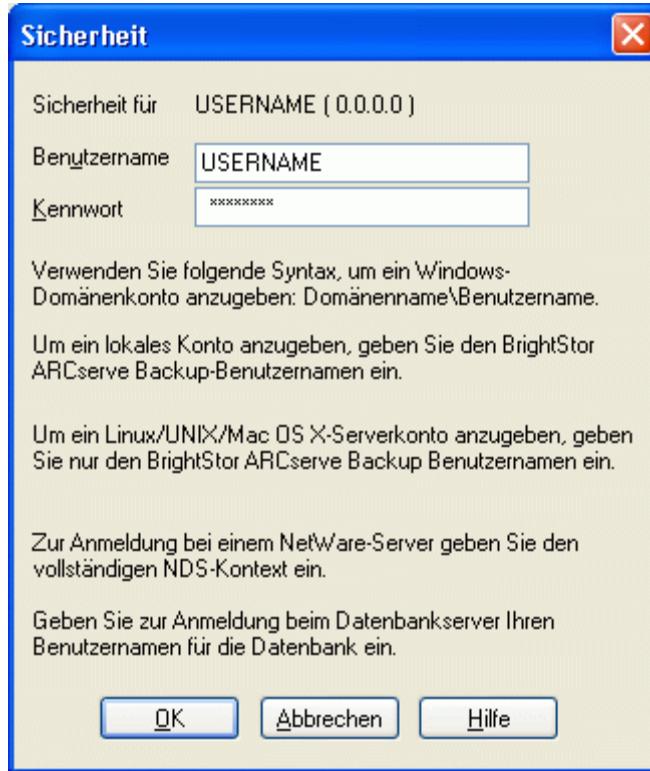
```
#Hostname IP-Adresse (optional) TCP-Port UDP-Port
#myhost   nnn.nnn.nnn.nnn      6050      6050
mymachine nnn.nnn.nnn.nn     7090      7085
```

## Festlegen von Workstation-Kennwörtern

Wenn Sie beim Konfigurieren des Client Agent für Windows über die Backup Agent-Verwaltung die Option "Kennwortsicherheit" ausgewählt haben, müssen Sie dasselbe Kennwort in CA ARCserve Backup angeben.

### So legen Sie das Kennwort für eine Workstation fest:

1. Klicken Sie im Sicherungs-Manager mit der rechten Maustaste auf den Namen des Client-Agenten.
2. Wählen Sie im Kontextmenü die Option "Sicherheit".



3. Geben Sie den Namen des lokalen Windows-Benutzerkontos oder des Windows-Domänenkontos (im Strukturformat) ein.
4. Geben Sie das Kennwort ein, und klicken Sie auf "OK".

**Hinweis:** Wenn Sie einen Client-Agenten verwenden, um Remote-Clients zu sichern und wiederherzustellen, werden durch das Kennwort für den Client-Agenten alle Freigabenklassenwörter für die Workstation außer Kraft gesetzt. Wenn Sie für Sicherungsjobs keine Client Agent-Software verwenden, müssen Sie im Sicherungs-Manager Kennwörter auf Freigabeebene angeben. Dabei müssen das Kennwort im Sicherungs-Manager und das Kennwort auf Freigabeebene übereinstimmen.

## Erstellen einer Windows-Zugriffssteuerungsliste

Sie können die Durchführung von Sicherungen eines Client Agent-Objekts für Windows auf bestimmte Server begrenzen, indem Sie eine Zugriffssteuerungsliste (ACL) erstellen. Diese Funktion wird durch den Sicherungs-Manager und die Backup Agent-Verwaltung definiert. Indem Sie eine Zugriffssteuerungsliste erstellen und deren Typ definieren, können Sie die Datensicherung und -wiederherstellung für den betroffenen Client Agent auf eine bestimmte Gruppe von CA ARCserve Backup-Servern beschränken. Folgende ACL-Typen sind verfügbar:

### **Keine Verwendung von ACLs**

Es wurde keine Liste angegeben (Standardeinstellung).

### **Liste der Server mit Zugriff**

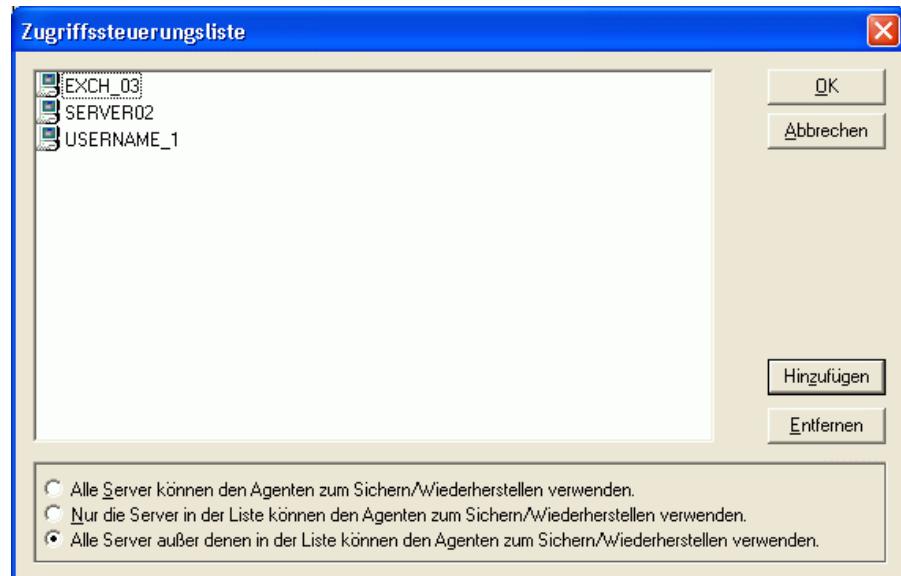
Eine Liste der Server, die zur Sicherung und Wiederherstellung auf den Client Agent-Rechner zugreifen dürfen.

### **Liste der Server ohne Zugriff**

Eine Liste der Server, die zur Sicherung und Wiederherstellung nicht auf den Client Agent-Rechner zugreifen dürfen. Alle anderen Server im Netzwerk können auf das Client-Objekt zugreifen.

### **So erstellen Sie eine Windows-Zugriffssteuerungsliste:**

1. Öffnen Sie die Backup Agent-Verwaltung.
2. Wählen Sie im Menü "Optionen" die Option "Zugriffssteuerungsliste" aus.



3. Wenn die Zugriffssteuerungsliste angezeigt wird, wird ACL standardmäßig **nicht** verwendet, und die Einstellung **Alle Server können den Agenten zum Sichern/Wiederherstellen verwenden.** ist ausgewählt. Wählen Sie **eine** der folgenden Optionen, um eine ACL zu erstellen:
  - Nur die Server in der Liste können den Agenten zum Sichern/Wiederherstellen verwenden.
  - Alle Server außer denen in der Liste können den Agenten zum Sichern/Wiederherstellen verwenden.
4. Klicken Sie auf "Hinzufügen", um der Zugriffssteuerungsliste Namen von Client Agents hinzuzufügen. Die Zahl der Namen ist nicht beschränkt. Wenn Sie Client Agents aus der Liste entfernen möchten, klicken Sie für jeden einzelnen Client Agent auf "Entfernen".
5. Klicken Sie auf "OK", wenn Sie keine weiteren Client Agent-Namen hinzufügen bzw. entfernen möchten.

## Virensuche aktivieren

CA Anti-Virus bietet zusätzlichen Schutz für wichtige Daten und schützt sie sogar während der Sicherung oder Wiederherstellung vor Viren.

Mit dieser Option können Sie Client Agent für Windows so konfigurieren, dass Viren während eines Sicherungs-, Kopier-, Zähl- oder Wiederherstellungsvorgangs automatisch erkannt und die betroffenen Dateien repariert werden.

### So aktivieren Sie die Virensuche:

1. Öffnen Sie den Backup- oder Wiederherstellungs-Manager.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche "Optionen", um das Dialogfeld "Globale Optionen" zu öffnen.
3. Klicken Sie auf die Registerkarte "Virus".
4. Wählen Sie "Virensuche aktivieren" aus.
5. Aktivieren Sie die Optionen für die Virensuche, die Sie für den Client-Agenten verwenden möchten. Folgende Möglichkeiten stehen u.a. zur Auswahl:

#### Auslassen

Infizierte Dateien werden nicht gesichert bzw. wiederhergestellt.

#### Umbenennen

Infizierte Dateien werden in Dateien mit der Erweiterung "x.AVB" umbenannt (z. B. "0.AVB", "1.AVB", "2.AVB"). Ist bereits eine Datei mit demselben Namen und der Erweiterung AVB vorhanden, wird die Erweiterung mit einer Zahl verändert, z.B. AV0, AV1, AV2.

### Löschen

Infizierte Dateien löschen.

### Bereinigen

CA Anti-Virus bereinigt die infizierten Dateien. Mit der Option "Bereinigen" werden infizierte Dateien während einer Sicherung automatisch und ohne Benutzereingriff repariert.

6. Wenn Sie möchten, dass die Komponentendateien jedes Archivs einzeln geprüft werden, aktivieren Sie Komprimierte Dateien durchsuchen.

**Hinweis:** Diese Option kann die Sicherungs- oder Wiederherstellungsleistung beeinträchtigen.

## Benutzerdefinierbare lokale Optionen

Wenn Sie ein übergeordnetes Objekt (in einer Datenbankkonfiguration mit übergeordneten und untergeordneten Objekten) explizit auswählen, können Sie mit der rechten Maustaste auf ein Client Agent-Objekt klicken, um die lokalen Sicherungsoptionen anzupassen. Weitere Informationen zum expliziten Packen von Jobs finden Sie im *Implementierungshandbuch*. Weitere Informationen zum Auswählen von Quellen beim Anpassen lokaler Optionen finden Sie im *Administrationshandbuch*.

## Ausschließen von Dateien aus Datenbankanwendungen von Sicherungen mit Client Agent für Windows

Der Client Agent für Windows kann Datenbank- und Protokolldateien von Sicherungen und aus Datenbankanwendungen wie Microsoft Exchange und Microsoft SQL Server bei der Durchführung von Sicherungen ausschließen.

Während der Sicherung kommuniziert der Client Agent für Windows mit dem Datenbankagenten, um eine Liste mit Dateien zu erhalten, die beim Sicherungsjob von der Sicherung des Dateisystems ausgeschlossen werden sollen. Der Client Agent für Windows schließt anschließend Dateien von der Sicherung des Dateisystems entsprechend der Antwort aus, die er vom Datenbankagenten erhalten hat. Wenn der Datenbankagent offline ist, gilt für den Client Agent die Annahme, dass alle Dateien gesichert werden sollen, und der Sicherungsjob für das Dateisystem wird entsprechend fortgeführt.

**Beispiel:**

Wenn Sie ein Microsoft Exchange-Serververzeichnis als Sicherungsquelle auswählen und die Sicherung des Dateisystems mit dem Client Agent für Windows durchführen, wird wie folgt ausgeschlossen:

- Wenn der Exchange-Informationsspeicher online ist, stellt der Agent für Microsoft Exchange Server eine Liste der Exchange-Datenbanken und Protokolldateien zur Verfügung, die vom Sicherungsjob ausgeschlossen werden sollen.  
Dadurch überspringt CA ARCserve Backup die ausgeschlossenen Dateien und schließt die Sicherung des Dateisystems ab.
- Wenn der Exchange-Informationsspeicher offline ist, stellt der Agent für Microsoft Exchange eine leere Liste ohne Exchange-Datenbanken oder Protokolldateien zur Verfügung, die vom Sicherungsjob ausgeschlossen werden sollen.  
Dadurch überspringt CA ARCserve Backup die Exchange-Server-Dateien nicht, und während der Sicherung des Dateisystems werden alle Dateien miteinbezogen.

## Konfiguration des NetWare Client Agent

In den folgenden Abschnitten wird die Konfiguration des CA ARCserve Backup NetWare Client Agent erläutert.

**Hinweis:** Auf dem Windows-Rechner muss der Novell-Client für Windows konfiguriert sein, damit Sie NetWare-Server im Netzwerk installieren und ausführen können.

### Konfigurationshinweise für NetWare

Beachten Sie bei der Konfiguration des Client Agents für NetWare Folgendes:

- Der Client Agent bietet keine Unterstützung mehrerer Jobs. Es kann immer nur ein Job auf einmal bedient werden. Wenn von mehreren CA ARCserve Backup-Servern aus Jobs in die Warteschlange des Client Agent gestellt werden, kann der aktuelle Job fehlschlagen.
- CA ARCserve Backup überspringt geöffnete NetWare-Dateien während einer Sicherung. Bei der Sicherung von NetWare-Dateien mit dem Client Agent für NetWare werden manchmal mehrere Dateien während der Sicherung als geöffnet erkannt und übersprungen. Wählen Sie in diesem Fall im Dialogfeld "Sicherungsoptionen" die Registerkarte "Wiederholen", und aktivieren Sie anschließend im Abschnitt "Gemeinsamer Dateizugriff" die Option "Sperrmodus verwenden, wenn 'Schreiben verweigern' nicht möglich". Übergeben Sie den Job dann noch einmal.

- Für NetWare gilt eine maximale Pfadlänge von 255 Zeichen, z.B. DIR1\DIR2\...DIRx. Diese Einschränkung gilt nur für NetWare, nicht für die anderen Client Agents, beispielsweise für Windows-, UNIX- oder Linux-Systeme.

**Hinweis:** Ist ein NetWare-Pfadname länger als 255 Zeichen, werden Sicherungs- und Wiederherstellungsvorgänge zwar ordnungsgemäß ausgeführt, die Pfadeinträge werden während des Durchsuchens jedoch abgeschnitten angezeigt. Auch die Optionen zur Wiederherstellung am ursprünglichen Speicherort oder an einem alternativen Speicherort sind nach wie vor bei der Wiederherstellung mit demselben Client Agent-Typ verfügbar.

## Konfigurieren der NetWare-Netzwerkkommunikation

Geben Sie in der Datei ASCONFIG.INI die IP-Adresse ein, die dem Client Agent vom Systemadministrator zugewiesen wurde, um den Client Agent für NetWare für die Kommunikation zu konfigurieren. Die Angabe einer IP-Adresse ist gerade bei einem Server mit mehreren IP-Adressen sinnvoll: Anstatt nur die erste gebundene Adresse zu verwenden, sucht der Client Agent in der Datei ASCONFIG.INI nach der zu verwendenden IP-Adresse.

### So bearbeiten Sie die Datei "ASCONFIG.INI":

1. Öffnen Sie die Datei ASCONFIG.INI im Stammverzeichnis des Client Agent mit einem Texteditor.
2. Fügen Sie die folgende Zeile dem Abschnitt [NetWare Agent] hinzu, und geben Sie dabei die IP-Adresse an, die der Client Agent verwenden soll:

IPAddress = nnn.nnn.nnn.nnn

Wenn der Abschnitt [NetWare Agent] nicht existiert, erstellen Sie ihn, indem Sie am Ende der Datei ASCONFIG.INI die folgende Zeile hinzufügen:

[NetWare Agent]

3. Speichern Sie die Datei, und beenden Sie den Editor.
4. Entladen Sie den Client Agent, und starten Sie ihn neu. Das Entladen ist notwendig, damit die Änderungen an der Datei ASCONFIG.INI wirksam werden. Verwenden Sie zum Entladen des Client Agent die Menüoption zum Entladen und Beenden von NetWare Client Agent. Als Alternative können Sie auch an der Serverkonsole folgenden Befehl eingeben:

unload nwagent

5. Starten bzw. laden Sie den Client Agent nach dem Entladen neu, indem Sie an der Server-Eingabeaufforderung den folgenden Befehl eingeben:

`nwagent`

An der Eingabeaufforderung des Servers wird eine Meldung eingeblendet, in der die Verwendung der in der Datei ASCONFIG.INI festgelegten IP-Adresse bestätigt wird:

IP-Adresse nnn.nnn.nnn.nnn in Datei ASCONFIG.INI wird verwendet.

Eine entsprechende Meldung wird im Laufzeitmeldungsbildschirm des Client Agent angezeigt:

IP-Adresse nnn.nnn.nnn.nnn ist an die Verwendung von NetWare Push-Agent gebunden.

Der Client Agent ist nun bereit, Sicherungs- und Wiederherstellungsjobs unter Verwendung der in der Datei ASCONFIG.INI festgelegten IP-Adresse auszuführen.

## Sichern der Novell-Verzeichnisdienste (Novell Directory Services, NDS)

Für eine ordnungsgemäße Sicherung der Novell-Verzeichnisdienste müssen Sie in das Feld "NDS-Anmeldename" den vollständigen NDS-Namen eingeben. Beispiel:

`.cn=admin.o=organization_name`

Beim Wiederherstellen von NetWare-Sitzungen müssen Sie bei der Eingabe der Sicherheitsinformationen den vollen NDS-Namen eingeben.

# Client Agent-Konfiguration für UNIX, Linux und Mac OS X

Die Konfigurationsdatei uag.cfg der Client-Agenten für UNIX, Linux und Mac OS X befindet sich auf der Remote-Client-Workstation im Stamverzeichnis des Client-Agenten. Diese Datei wird immer auf Einträge durchsucht, wenn ein Job an die Workstation übergeben wird, und kann zum Einstellen mehrerer Optionen für den Client-Agenten verwendet werden.

**Wichtig!** Ändern Sie die Variablen in der Agenten-Konfiguration niemals eigenständig, sondern ausschließlich unter Anleitung eines Mitarbeiters des Technischen Supports von CA.

## Konfigurationshinweise für UNIX, Linux und Mac OS X

Im Folgenden werden Probleme beschrieben, die Sie bei der Konfiguration des Client-Agenten auf der UNIX-, Linux- und Mac OS X-Plattform berücksichtigen sollten.

- **Sitzungskennwörter:** Für UNIX-, Linux- und Mac OS X-Sitzungen dürfen Sitzungskennwörter maximal 22 Byte lang sein.
- **Verzeichnisnamen mit einem Zeichen:** In Wiederherstellungsansichten kann es Anzeigeprobleme geben, wenn Verzeichnisnamen mit nur einem Zeichen wiederhergestellt werden. Die Daten werden in der Datenbankansicht korrekt angezeigt.
- **Symbolische Verknüpfungen und NFS verfolgen:** Die Optionen Symbolische Verknüpfung verfolgen und NFS verfolgen werden bei Wiederherstellungsvorgängen nicht unterstützt.

**Hinweis:** Falls in den CA ARCserve Backup-Optionsdefinitionen dieser Client Agents Konflikte bestehen, haben die Optionen, die über den Sicherungs-Manager festgelegt wurden, immer Vorrang gegenüber Optionen, die manuell in die Konfigurationsdatei "uag.cfg" eingetragen wurden.

## Kontrolldateien der Client-Agenten für UNIX, Linux und Mac OS X

In den Kontrolldateien der Client-Agenten für UNIX, Linux und Mac OS wird festgelegt, welche Verzeichnisse, Dateisysteme oder Dateisystemtypen von Sicherungsvorgängen auf einer bestimmten Workstation ausgeschlossen werden sollen. Insbesondere müssen für die Client-Agenten für UNIX, Linux und Mac OS X die folgenden Pakete installiert sein:

- Der Common Agent
- Der Universal Agent (uagent)

**Hinweis:** Vor der Installation des "uagent" muss der Common Agent installiert werden.

Für die beiden Pakete werden u.a. folgende Kontrolldateien installiert:

- Datei zur Verzeichnissteuerung

In der Datei zur Verzeichnissteuerung, uagcntl, können Sie alle Verzeichnisse bzw. Dateisysteme aufführen, die von Sicherungsvorgängen auf einer Workstation ausgeschlossen werden sollen. Geben Sie Verzeichnisse und Dateisysteme in dieser Datei mit einem Schrägstrich (/), gefolgt vom vollständigen Pfadnamen in einer Zeile an. Beispiel:

/opt/account1

**Hinweis:** Die Datei zur Verzeichnissteuerung wird auf der Client Agent-Workstation im uagent-Stammverzeichnis gespeichert.

- Datei zur Dateisystemsteuerung

In der Datei zur Dateisystemsteuerung, fscntl, werden die Dateisystemtypen auf einer bestimmten Workstation aufgeführt, die von Sicherungsvorgängen ausgeschlossen werden sollen. Tragen Sie jeden auszuschließenden Dateisystemtyp in der Datei fscntl in einer eigenen Zeile ein.

**Hinweis:** Die Dateisystemdatei wird auf der Client Agent-Workstation im uagent-Stammverzeichnis gespeichert.

- Browser-Konfigurationsdatei

Die Browser-Konfigurationsdatei, cabr.cfg, ermöglicht die Anzeige von Partitionsgeräten in einem Browser. Der absolute Name des Partitionsgeräts muss in einer eigenen Zeile der Datei cabr.cfg angegeben werden.

- Common Agent-Konfigurationsdatei

In der Common Agent-Konfigurationsdatei, agent.cfg, werden alle auf dem System installierten UNIX-, Linux- und Mac OS X-Client-Agenten überwacht. Das Skript wird automatisch ausgeführt, nachdem uagent installiert wurde.

**Hinweis:** Die Dateien zur Verzeichnis- und Dateisystemsteuerung können nur durch einen Systemadministrator bearbeitet werden. Je nach den Zugriffsrechten, die der Systemadministrator einer Datei zugewiesen hat, können gegebenenfalls jedoch auch andere Benutzer die Dateien anhängen.

## Common Agent-Konfigurationsdatei für UNIX, Linux und Mac OS X

Common Agent (Binärdatei "caagentd") ist eine Standardkomponente aller Client-Agenten für UNIX, Linux und Mac OS X. Die Installation erfolgt automatisch während der Erstinstallation eines Client-Agenten für UNIX, Linux oder Mac OS X.

Common Agent befindet sich im Verzeichnis /opt/CA/ABcmagt. Er verwendet zur Verwaltung der auf dem System installierten Client-Agenten eine Konfigurationsdatei namens "agent.cfg", die sich ebenfalls im Verzeichnis "/opt/CA/ABcmagt" befindet.

**Hinweis:** CA ARCserve Backup installiert verwandte Konfigurationsdateien für den Common Agent, die Dateisystem-Agents und den Agent für Oracle in unterschiedlichen Verzeichnissen auf den verschiedenen UNIX- und Linux-Plattformen. Weitere Informationen finden Sie unter [Installationsverzeichnisse für den Common Agent und Client Agent für UNIX und Linux](#) (siehe Seite 16).

Während der Installation eines neuen Client-Agenten wird die Datei agent.cfg mit den Informationen des neuen Client-Agenten aktualisiert. Eine Bearbeitung dieser Konfigurationsdatei ist nur in seltenen Fällen erforderlich. Manuelle Änderungen an dieser Datei müssen nur vorgenommen werden, um einige Meldungen bei der Fehlersuche zu aktivieren oder den standardmäßigen TCP/IP-Port für die Ausführung von Common Agent zu ändern.

Im Folgenden sehen Sie ein Beispiel für die Datei "agent.cfg" bei installiertem Client Agent:

```
[0]
#[ABagntux]
NAME      ABagntux
VERSION   nn.nn.nn
HOME      /opt/CA/ABuagent
ENV       CA_ENV_DEBUG_LEVEL=4:$CA_ENV_DEBUG_LEVEL
ENV       LD_LIBRARY_PATH=/opt/CA/CAlib:/opt/CA/ABcmagt:$LD_LIBRARY_PATH
ENV       SHLIB_PATH=/opt/CA/CAlib:/opt/CA/ABcmagt:$SHLIB_PATH
ENV       LIBPATH=/opt/CA/CAlib:/opt/CA/ABcmagt:$LIBPATH
BROWSER   cabr
AGENT     uagentd
MERGE    umrgd
VERIFY   umrgd

[36] DISABLED
#[ABcmagt]
#NAME ABcmagt
#HOME /opt/CA/ABcmagt
#TCP_PORT 6051
#UDP_PORT 6051
```

### Struktur der Common Agent-Konfigurationsdatei

Jeder Abschnitt der Datei agent.cfg enthält Feldgruppen, die einem auf einem UNIX-, Linux- oder Mac OS X-Gerät im Sicherungsnetzwerk installierten Client-Agenten direkt entsprechen. Mit Ausnahme des Speicherorts des Stammverzeichnisses für den Agenten sind alle Felder in der Datei vorgegeben.

Der Inhalt des Feldes der Umgebungsvariablen (ENV) wird ebenfalls während der Installation und Konfiguration des Client-Agenten festgelegt. Sie können jedoch gegebenenfalls manuell Werte für diese Variable in die Datei eingeben. Sie sollten agent.cfg nur in bestimmten Fällen verändern, z.B. wenn Sie ein zusätzliches Umgebungsfeld mit einer bestimmten Datenbank verknüpfen möchten.

**Hinweis:** Die an der Datei "agent.cfg" vorgenommenen Änderungen werden erst dann wirksam, wenn der Client Agent-Rechner gestartet (oder heruntergefahren und erneut gestartet) wird.

In der folgenden Tabelle sehen Sie ein Beispiel für die Datei agent.cfg und eine Beschreibung der einzelnen Agent-Felder.

Dateiinhalt	Feldbeschreibung
[0]	Objekttyp, die vordefinierte Nummer eines bestimmten Client-Agenten im Netzwerk für UNIX oder Linux
[4]	Objekttyp, die vordefinierte Nummer eines bestimmten Client-Agenten im Netzwerk für Mac OS X
NAME ABagntux	Name des Client-Agenten
VERSION nn.n	Release- und Versionsnummer des Client-Agenten
HOME /opt/CA/ABuagent	Standardmäßiges Stammverzeichnis des Client-Agenten
#ENV CA_ENV_DEBUG_LEVEL=4	Umgebungsvariable, die an den Client-Agenten übergeben wird
#ENV CAAGPERF_ENABLE=1	Aktiviert die Snapshot- und DirectIO-Funktionen auf Solaris und HP. Weitere Informationen finden Sie unter "Konfigurieren von Snapshot und DirectIO".
ENV LD_LIBRARY_PATH	Suchpfad der gemeinsam genutzten Bibliothek für Sun, Linux, Tru64 und Mac OS X
ENV SHLIB_PATH	Suchpfad der gemeinsam genutzten Bibliothek für HP
ENV LIBPATH	Suchpfad der gemeinsam genutzten Bibliothek für AIX
BROWSER cabr	Browser-Modul für den Client-Agenten
AGENT uagentd	Sicherungs-Modul für den Client Agent-Daemon
MERGE umrgd	Einfüge-Daemon
VERIFY umrgd	Such-Daemon

## Client Agent-Stammverzeichnis

Das standardmäßige Stammverzeichnis des Client Agent, ABuagent, wird während der Installation und des Setup automatisch definiert. Sie können jedoch gegebenenfalls ein anderes Stammverzeichnis bestimmen.

Den Namen des Stammverzeichnisses finden Sie in der Datei agent.cfg im Abschnitt ABagntux. Der Name des Stammverzeichnisses des Client-Agenten wird durch die Variable HOME definiert.

## Common Agent-Komponenten

Common Agent wird ständig als Daemon ausgeführt und wartet für alle auf dem System installierten Client-Agenten für UNIX, Linux und Mac OS X auf Anforderungen. Während der Installation der einzelnen Agenten werden die Komponenten BROWSER, AGENT, MERGE und VERIFY jeweils in einem eigenen Abschnitt in Common Agent registriert.

Nicht alle genannten Komponenten sind in jedem Client-Agenten enthalten. In der folgenden Beispielkonfigurationsdatei sehen Sie im Abschnitt für Client Agent für UNIX, Linux oder Mac OS X die BROWSER-Komponente "cabr", die AGENT-Komponente "uagentd" und die MERGE- und VERIFY-Komponente "umrgd". Andere Client-Agenten verwenden hingegen andere BROWSER- und AGENT-Komponenten.

```
[0]
#[ABagntux]
NAME      ABagntux
VERSION   nn.nn.nn
HOME      /opt/CA/ABuagent
ENV       CA_ENV_DEBUG_LEVEL=4:$CA_ENV_DEBUG_LEVEL
ENV       LD_LIBRARY_PATH=/opt/CA/CALib:/opt/CA/ABCmagt:$LD_LIBRARY_PATH
ENV       SHLIB_PATH=/opt/CA/CALib:/opt/CA/ABCmagt:$SHLIB_PATH
ENV       LIBPATH=/opt/CA/CALib:/opt/CA/ABCmagt:$LIBPATH
BROWSER   cabr
AGENT     uagentd
MERGE    umrgd
VERIFY   umrgd
```

## Konfiguration der Port-Adresse

Der Standard-Port für TCP und UDP ist 6051. Der TCP-Port wird für die Kommunikation und Datenübertragung zwischen dem Sicherungsserver ("cprocess") und dem Client-Agenten verwendet. Die Benutzeroberfläche des Sicherungs-Managers verwendet den UDP-Port zum Durchsuchen von Hosts.

Wenn Sie den TCP-Port und/oder den UDP-Port konfigurieren möchten, müssen Sie die Konfigurationsdateien sowohl auf dem CA ARCserve Backup-Server als auch für den Client-Agenten ändern, damit deren Werte übereinstimmen.

Die Namen der Konfigurationsdateien lauten folgendermaßen:

- **"CAPortConfig.cfg"**: für CA ARCserve Backup-Windows-Server
- **agent.cfg**: für Client-Agenten

**Hinweis:** Wichtige Informationen zu den UNIX-, Linux- und Mac OS X-Konfigurationsdateien finden Sie unter "Kontrolldateien der Client-Agenten für UNIX, Linux und Mac OS X".

Das folgende Beispiel zeigt die Windows-Server-Konfigurationsdatei ("CAPortConfig.cfg"):

```
#Hostname IP-Adresse (optional) TCP-Port UDP-Port
#myhost xxx.xxx.xxx.xxx 6051 6051
```

Das folgende Beispiel zeigt die Syntax für die Client Agent-Konfigurationsdatei (agent.cfg):

```
[36]
NAME ABcmagt
HOME /opt/CA/ABcmagt
TCP_PORT 7090
UDP_PORT 7085
```

## Port-Nummern für Common Agent

Standardmäßig verwendet Common Agent den Port 6051 sowohl für TCP als auch für UDP. Wenn Sie den Standard-Port ändern möchten, müssen Sie im Abschnitt [ABcmagt] der Datei agent.cfg die neuen Port-Nummern eintragen und Common Agent anschließend mit dem Befehl caagent stop, gefolgt von dem Befehl caagent start, neu starten. Verwenden Sie den Befehl "caagent update" *nicht* nach dem Ändern von Port-Nummern.

**Hinweis:** Im Normalfall sollte diese Methode **nicht** zum Starten oder Stoppen von Common Agent **verwendet werden**. Führen Sie stattdessen die Skripte zum Starten und Stoppen der einzelnen Client-Agenten für UNIX, Linux und Mac OS X aus, die auf dem System installiert sind.

Im Folgenden sehen Sie ein Beispiel für eine Konfigurationsdatei, bevor und nachdem die Skriptänderungen vorgenommen wurden.

Vor der Änderung:

```
[36]
#[ABcmagt]
#NAME      ABcmagt
#HOME      /opt/CA/ABcmagt
#TCP_PORT  6051
#UDP_PORT  6051
```

Nach der Änderung:

```
[36]
#[ABcmagt]
NAME      ABcmagt
HOME      /opt/CA/ABcmagt
TCP_PORT  9051
UDP_PORT  9051
```

Die Port-Änderungen werden nach dem Neustart von Common Agent wirksam. Wenn Sie Common Agent für die Ausführung über einen vom Standard abweichenden Port konfigurieren, müssen Sie auch den CA ARCserve Backup-Server so konfigurieren, dass er auf Common Agent zugreifen kann. Erstellen Sie hierzu in der Datei port.cfg einen Eintrag für den Client-Agenten. Diese Datei befindet sich im config-Unterverzeichnis des Stammverzeichnisses – \$BAB\_HOME/config/port.cfg – auf dem Sicherungsserver.

Standardmäßig verwendet Common Agent einen weiteren UDP-Port, 0xA234 (41524), um Anforderungen von CA ARCserve Backup zur automatischen Erkennung (Auto Discovery) der Client-Agenten für UNIX, Linux und Mac OS X zu empfangen. Dieser Port ist nicht konfigurierbar.

## Benutzerinformationen für Host-Äquivalenz

Bei der Überprüfung der Benutzerinformationen durch Common Agent erhalten Host-Äquivalenzeinstellungen des Systems eine stärkere Gewichtung. Ein UNIX-, Linux- oder Mac OS X-System kann so eingerichtet werden, dass bestimmte Benutzer ohne Angabe von Benutzerinformationen auf bestimmte Hosts zugreifen können. Hierzu fügen Sie die IDs der gewünschten Benutzer zur Datei /etc/hosts.equiv bzw. .rhosts hinzu. Common Agent folgt standardmäßig diesen Regeln und prüft dann das Kennwort des Benutzers, um dessen Berechtigung festzustellen. Definieren Sie die Umgebungsvariable NO\_HOSTS\_EQUIV=1 in der Datei agent.cfg, wie im folgenden Beispiel gezeigt, um die Überprüfung auf ein Host-Äquivalent zu deaktivieren.

```
[36]
#[ABcmagt]
NAME    ABcmagt
HOME    /opt/CA/ABcmagt
ENV     NO_HOSTS_EQUIV=1
```

Bei Bedarf können Sie Common Agent mit einer Reihe von Zugriffssteuerungslisten in den 'Kein-Kennwort-Modus' oder Einzelbenutzermodus versetzen. Weitere Informationen zu ACLs finden Sie unter [UNIX-, Linux- und Mac OS X-Zugriffssteuerungslisten](#) (siehe Seite 55).

### Funktionsweise der Common Agent-Verbindungsanforderungen

Um eine Client Agent-Sitzung zu starten, fordert der CA ARCserve Backup-Server eine Verbindung für einen Client Agent für UNIX, Linux oder Mac OS X an, die eine spezifische Sicherungskomponente verwenden soll (beispielsweise BROWSER, BACKUP oder RESTORE). Wenn die Anforderung eingeht, nimmt Common Agent die Verbindung an und überprüft die Anmeldeinformationen des Benutzers für das System.

Nach Überprüfung des Benutzers sucht Common Agent in der Datei agent.cfg nach einem Eintrag, der dem jeweiligen Client-Agenten und der angegebenen Komponente entspricht. Erst wenn sowohl der Client-Agent als auch die angeforderte Komponente geprüft wurden, aktiviert Common Agent den Client-Agenten und die Komponente. Anschließend kehrt Common Agent wieder in den Ruhezustand zurück und wartet auf weitere Anforderungen.

### Konfigurierbare Optionen

Mit Optionen wird die Funktionsweise des Client-Agenten optimiert und angepasst. Keine der Optionen ist jedoch für den Betrieb des Client-Agenten erforderlich. Eine vollständige Liste der Optionen, die beim Starten der Client-Agenten für UNIX, Linux oder Mac OS X zur Verfügung stehen, finden Sie in der folgenden Tabelle.

**Hinweis:** Die Festlegung von Optionen sollte durch erfahrene Administratoren mit UNIX-, Linux- oder Mac OS X-Kenntnissen erfolgen. Wenn Sie nicht sicher sind, was eine Option oder ein Parameter bedeutet, sollten Sie die Funktion nur unter Anleitung eines Mitarbeiters des Technischen Supports von CA aktivieren.

Option	Beschreibung
-ALLOW <Netzwerkadresse> <Hostadresse>	Verwenden Sie diese Option im Einzelbenutzermodus mit der Option -S oder -NOPASSWORD, um die IP-Adressen der Computer zu definieren, die auf die Client-Agenten ohne Überprüfung zugreifen dürfen.

---

-ALLOW N:172.16.0.0(255.255.255.0) H:172.31.255.255

In diesem Beispiel bezeichnet N eine Netzwerkadresse und H die IP-Adresse eines Hosts. Sie können optional auch eine Teilnetzmaske angeben.

---

<b>Option</b>	<b>Beschreibung</b>
-b bufsize	Die E/A-Puffergröße der Festplatte in Byte. Die möglichen Optionen liegen zwischen 16384 und 65536Byte; Standardwert: 65536Byte.
-c n	Die Zeit bis zum Eintritt des Ruhemodus während des Wartevorgangs in Millisekunden (ms). Die möglichen Optionen liegen zwischen null (0) und 1000ms; Standardwert: 50ms.
-CAUSER USER	Definiert den Einzelbenutzermodus. Wird zusammen mit den Optionen -S oder -NOPASSWORD verwendet, um die Liste zum Zulassen oder Verweigern einzelner Benutzer festzulegen.

Beispiel:

-CAUSER A: USER1 N: USER2

In diesem Beispiel steht A für -ALLOW (Zulassen) und N für -DENY (Verweigern).

---

<b>Option</b>	<b>Beschreibung</b>
-DENY <Netzwerkadresse> <Hostadresse>	Verwenden Sie im Einzelbenutzermodus diese Option mit der Option -S oder -NOPASSWORD, um die IP-Adressen zu definieren, die keinen Zugriff auf die Client-Agenten haben dürfen.

Beispiel:

-DENY N:172.16.0.0(255.255.255.0) H:172.31.255.255

In diesem Beispiel bezeichnet N eine Netzwerkadresse und H die IP-Adresse eines Hosts. Sie können optional auch eine Teilnetzmaske angeben.

---

<b>Option</b>	<b>Beschreibung</b>
-l	Veranlasst den Client-Agenten, auf Advisory Locks zu prüfen. Standardwert: Nur Mandatory Locks.
-m maxbuf	Gibt die Anzahl der Puffer an, die für E/A zugewiesen sind. Möglich sind 2 bis 1024 Puffer, der Standardwert ist 128.

Option	Beschreibung
-NOPASSWORD	Geben Sie diese Option an, wenn Sie die Optionen -ALLOW, -DENY oder -CAUSER verwenden müssen. Diese Option entspricht der Option -S im Einzelbenutzermodus, wenn kein Kennwort erforderlich ist.
-P <i>n</i>	Legt das Standard-Zeitlimit fest, gefolgt von einer variablen Zahl. Diese variable Zahl ( <i>n</i> ) ist benutzerdefiniert und bezeichnet Minuten (0 bis 10). Der Standardwert ist 5 Minuten.

Die Option -P 10 weist beispielsweise dem vor der Sicherung oder Wiederherstellung auszuführenden Skript eine Wartezeit von 10 Minuten zu.

**Hinweis:** Wenn Sie die Option "-P" ohne Angabe der Zahl *n* verwenden, tritt ein Fehler auf.

Option	Beschreibung
-Prebackup <i>Dateiname</i>	Führt vor oder nach dem Sicherungs- oder Wiederherstellungsjob die Standardskripte aus, mit denen sie verknüpft sind. Der Dateiname ist optional. Wenn kein Dateiname angeführt ist, wird uag_pre_backup als Dateiname verwendet.
-Postbackup <i>Dateiname</i>	
-Prerestore <i>Dateiname</i>	
-Postrestore <i>Dateiname</i>	
-S	Aktiviert die Option für den Einzelbenutzermodus. Im Einzelbenutzermodus werden Benutzerinformationen nicht mit den gültigen Benutzer-IDs und Kennwörtern verglichen. Stattdessen wird der Zugriff anhand der Optionen -ALLOW, -DENY oder -CAUSER erteilt. Weitere Informationen finden Sie unter der jeweiligen Option.
-s <i>async nonblocking</i>	Stellt die Socket-E/A auf asynchronen Nichtsperrmodus ein.
-s <i>bufsize</i>	Gibt die Größe des Socket-Puffers an. Möglich sind 4096 bis 65536. Der Standardwert ist systemabhängig.
-s <i>SocketMode</i>	Gibt an, dass der Socket-Modus für Sicherungsvorgänge verwendet werden soll.
-sparse	Unterscheidet zwischen Operationen an Dateien mit geringer Datendichte und normalen Dateien. Mit dieser Option wird die Effizienz der Sicherung oder Wiederherstellung von Dateien mit geringer Datendichte verbessert.  <b>Hinweis:</b> Kontingentdateien werden bei Sicherungs- und Wiederherstellungsvorgängen unabhängig von der Angabe der Option "-sparse" immer als Dateien mit geringer Datendichte behandelt.
-verbose oder -v	Versetzt das System in den ausführlichen Modus, um die Eingabe von

<b>Option</b>	<b>Beschreibung</b>
detaillierten Fehlersuchmeldungen an der Konsole zu ermöglichen.	

## Snapshot- und DirectIO-Unterstützung für UNIX

Die Client-Agenten für UNIX unterstützen die Snapshot- und DirectIO-Funktionen. Damit Sie diese Funktionen nutzen können, muss eine der folgenden Umgebungen auf dem Rechner vorhanden sein, auf dem der Client Agent für UNIX ausgeführt wird:

<b>Funktion</b>	<b>Plattform</b>	<b>Software-Voraussetzungen</b>
Snapshot	Solaris	UFS-Dateisystem mit installiertem fssnap-Paket (Solaris 8 und 9) oder die erweiterte Version des VxFS-Dateisystems
Snapshot	HP-UX 11.0	Erweiterte Version des VxFS-Dateisystems oder des Online Journaling File System (Online JFS)
DirectIO	Solaris	UFS- oder VxFS-Dateisystem
DirectIO	HP-UX 11.0	Erweiterte Version des VxFS-Dateisystems oder Online JFS

### Beschreibung von Snapshot und DirectIO

Mit der DirectIO-Funktion erstellt der Client Agent einen 'Schnappschuss' (Snapshot) von erweiterten Versionen von VxFS oder Online JFS (HP-UX) bzw. UFS mit installiertem fssnap (Solaris). Anschließend lädt der Client-Agent den Snapshot in ein temporäres Verzeichnis des Stamm-Volumes und erzeugt dann die Sicherung des Snapshots. Nach Abschluss der Snapshot-Sicherung entlädt der Client-Agent den Snapshot aus dem temporären Verzeichnis und löscht ihn.

Damit Sie eine Snapshot-Sicherung durchführen können, müssen Sie einen Snapshot-Puffer angeben. Dies ist der Speicherplatz auf der Festplatte, in dem die ursprünglichen Daten gespeichert werden, bevor sie auf dem Volume, von dem der Snapshot erstellt wurde, überschrieben werden. Bei der Verwendung des Snapshot-Puffers ist Folgendes zu beachten:

- Der Snapshot-Puffer muss groß genug sein, um alle Daten zu speichern, die während der gesamten Dauer der Sicherung auf dem Volume, von dem der Snapshot erstellt wurde, geändert werden. Wenn im Snapshot-Puffer nicht genügend Speicherplatz vorhanden ist, wird der Snapshot ungültig und die Sicherung schlägt fehl.
- Das Volume, von dem der Snapshot erstellt wurde, und der Snapshot-Puffer sollten sich nicht im selben Dateisystem befinden.
- Die beste Leistung ist zu erzielen, wenn sich das Volume, von dem der Snapshot erstellt wurde, und der Snapshot-Puffer auf physisch getrennten Festplatten befinden.
- Auf der Solaris-Plattform mit UFS und fssnap kann der Snapshot-Puffer ein Dateiname, ein Verzeichnisname oder eine unformatierte Partition sein.

Bei einer Sicherung oder Wiederherstellung mit DirectIO müssen Sie die Client-Umgebung überprüfen und die Konfigurationsdatei caagperf.cfg bearbeiten. Sie können Snapshot und DirectIO für die Dateisysteme in der Datei caagperf.cfg anzeigen, indem Sie nach Übermittlung des Sicherungs- oder Wiederherstellungsjobs den Befehl mount in der Befehlszeile ausführen.

Bei der Snapshot-Funktion wird nach dem Ausführen des Befehls mount als Ausgabe ein neues schreibgeschütztes Dateisystem angezeigt, dessen Bereitstellungspunkt mit dem Präfix SNAP\_HOME\_ beginnt. Ein Benutzer von DirectIO kann die Änderungen an den Bereitstellungsoptionen in diesem spezifischen Dateisystem beobachten. Sofern Sie in der Datei caagperf.cfg das Protokollierungs-Flag aktiviert haben, werden detaillierte Meldungen auch in der Datei caagperf.cfg aufgezeichnet.

In den folgenden Abschnitten wird die Konfiguration eines Client-Agenten für UNIX zur Verwendung dieser Funktionen beschrieben.

## Konfigurieren von Snapshot und DirectIO

Gehen Sie folgendermaßen vor, um die Snapshot- und DirectIO-Funktionen zu konfigurieren:

1. Aktivieren Sie die Umgebungsvariable CAAGPERF\_ENABLE, indem Sie in der Datei agent.cfg die folgende Zeile hinzufügen:

```
ENV CAAGPERF_ENABLE=1
```

**Hinweis:** Die Datei "agent.cfg" befindet sich im Verzeichnis "/opt/CA/ABcmagt".

Nachdem Sie die Umgebungsvariable aktiviert haben, sieht der Abschnitt des Client-Agenten in der Datei agent.cfg folgendermaßen aus:

```
[0]
NAME      ABagentux
VERSION   nn.nn.nn
HOME      /opt/CA/uagent
ENV       LD_LIBRARY_PATH=/usr/local/Calib:/opt/CA/ABcmagt
ENV       CAAGPERF_ENABLE=1
```

2. Bereiten Sie die Konfigurationsdatei caagperf.cfg im Verzeichnis /opt/CA/ABcmagt vor. Sie müssen in der Datei caagperf.cfg angeben, welche Vorgangstypen für die angegebenen Dateisysteme durchgeführt werden sollen. Weitere Informationen finden Sie im folgenden Abschnitt.

## Parameter und Werte der Konfigurationstabelle

Das Format der Konfigurationsdatei ist mit einer INF-Datei unter Windows vergleichbar. Sie besteht aus Abschnitten und Schlüssel-Wert-Paaren. Abschnittsnamen befinden sich in eckigen Klammern, die Schlüssel-Wert-Paare liegen im Format SCHLÜSSEL=WERT vor, wobei jede Zeile jeweils ein Paar enthält. Bei allen Einträgen in der Konfigurationsdatei ist die Groß-/Kleinschreibung zu beachten.

Die Schlüssel-Wert-Paare befinden sich unterhalb der Volumes, zu denen sie gehören. Die Abschnittsnamen entsprechen den Namen der Volumes. Beispiele für die Syntax für Abschnittsnamen in der Datei caagperf.cfg sind [/] oder [/export/home]. Wenn für ein Volume mehrere Einträge vorhanden sind, ist das Verhalten des Client-Agenten nicht definiert.

Mit Hilfe der Schlüssel-Wert-Paare werden Parameter für das Volume festgelegt, zu dem sie gehören. Standardmäßig sind alle Optionen deaktiviert. Wenn ein Volume keine besondere Verarbeitung erfordert, sollte es nicht in der Datei caagperf.cfg aufgeführt werden.

Die Schlüssel und ihre Werte werden in der folgenden Tabelle beschrieben:

Schlüssel	Wert
DOSNAP	Aktiviert die Snapshot-Funktion auf einem Volume. Der Wert sollte BACKUP lauten, da der Snapshot während eines Sicherungsvorgangs erstellt werden sollte.
SNAPSHOTBUFFER	Gibt den Puffer an, der zum Speichern der ursprünglichen Daten verwendet wird, bevor diese auf dem Volume, von dem der Snapshot erstellt wurde, überschrieben werden. Der Wert sollte ein Dateiname oder eine Partition sein. Die Datei kann eine Datei oder ein Verzeichnis auf einem anderen Volume sein.
	Der Wert dieses Feldes ist abhängig vom Typ des Dateisystems. Bei der erweiterten Version von VxFS oder Online JFS stimmt der Wert mit dem Namen einer leeren Partition überein. Bei UFS entspricht der Wert einem Datei-, Verzeichnis- oder Partitionsnamen.
DOUBIO	Aktiviert die DirectIO-Funktion auf einem Volume. Mögliche Werte sind BACKUP, RESTORE und BACKUP_RESTORE. Der Wert dieses Feldes ist abhängig von Ihren Anforderungen an Sicherung oder Wiederherstellung.

Möglicherweise sind die folgenden Beispiel-Konfigurationsdateien für Sie hilfreich.

## Konfigurationsdateien für UNIX-Systeme

Die folgenden Beispiele zeigen unterschiedliche Konfigurationsdateien für UNIX-Systeme.

### **Beispiel: Betriebssystem Solaris 8 oder Solaris 9 mit dem Dateisystem UFS und installiertem fssnap**

Die erste Zeile der Datei ist ein Flag für die Fehlersuche. Die auf den Fehlersucheintrag folgenden drei Abschnitte entsprechen den Volumes /opt, /export/home und / auf der Festplatte.

Für die Abschnitte [/opt] und [/export/home] ist die Snapshot-Funktion während der Sicherung aktiviert, für den Abschnitt [/] ist DirectIO für Sicherung und Wiederherstellung aktiviert.

```
##DEBUG
[/opt]
DOSNAP=BACKUP
SNAPSHOTBUFFER=/garbage/snapbufferfile_1

[/export/home]
DOSNAP=BACKUP
SNAPSHOTBUFFER=/garbage/snapbufferfile_2

[/>
DOUBIO=BACKUP_RESTORE
```

### **Beispiel: Betriebssystem Solaris 8, auf dem die erweiterte Version des VxFS-Dateisystems installiert ist**

Die Datei enthält drei Abschnitte. Die erste Zeile der Datei ist ein Flag für die Fehlersuche. Die drei Abschnitte der Datei beziehen sich auf die Volumes /opt, /export/home und /. Für die Abschnitte [/opt] und [/export/home] ist die Snapshot-Funktion während der Sicherung aktiviert, für das Volume / ist DirectIO für Sicherung und Wiederherstellung aktiviert.

```
T##DEBUG
[/opt]
DOSNAP=BACKUP
SNAPSHOTBUFFER=/dev/dsk/c0t0d0s4

[/export/home]
DOSNAP=BACKUP
SNAPSHOTBUFFER=/dev/dsk/c0t0d0s4

[/>
DOUBIO=BACKUP_RESTORE
```

**Beispiel: Betriebssystem HP-UX, auf dem entweder die erweiterte Version des VxFS-Dateisystems oder das Online JFS-Dateisystem installiert sein kann**

Die Datei enthält vier Abschnitte. Die erste Zeile der Datei ist ein Flag für die Fehlersuche. Die Abschnitte der Datei beziehen sich auf die Volumes/, /var, /usr und /export. In dieser Datei ist für das Volume / während Sicherung und Wiederherstellung DirectIO aktiviert, für die anderen Volumes ist die Snapshot-Funktion während der Sicherung aktiviert.

```
##DEBUG
[/]
DOUBIO=BACKUP_RESTORE

[/var]
DOSNAP=BACKUP
SNAPSHOTBUFFER=/dev/vg00/lvol7

[/usr]
DOSNAP=BACKUP
SNAPSHOTBUFFER=/dev/vg00/lvol7

[/export]
DOSNAP=BACKUP
SNAPSHOTBUFFER=/dev/vg00/lvol7
```

**Verfolgungsebenen für die AS/400 Enterprise Option**

In bestimmten Fällen müssen Sie möglicherweise gemäß den Anweisungen vom Technischen Support von CA die für die AS/400 Enterprise Option protokollierte Aktivitätsebene ändern. Da Verfolgungsebenen die Leistung der Sicherung beeinträchtigen können, ändern Sie die Werte nur dann, wenn Sie spezifische Anweisungen vom Technischen Support von CA erhalten.

In der folgenden Tabelle sind alle Verfolgungsebenen für die AS/400 Enterprise Option aufgeführt:

Ebene	Beschreibung
ASO\$TRACE	Steuert die Verfolgungstiefe des Client-Agenten. Gültige Werte sind -1 und 0 bis 0xFFFFFFFF. Wenn ASO\$TRACE auf den Wert -1 eingestellt ist, sind die Protokolle am detailliertesten.
ASO\$TRACE_AST	Dies ist ein Umschalter. Wenn diese Funktion definiert ist, werden Asynchronous System Traps (ASTs) verfolgt.
ASO\$TRACE_IDENT	Dies ist ein Formatierungsparameter. Der empfohlene Wert liegt zwischen 0 und 5. Der Standardwert ist 3.

ASO\$TRACE\_DATA

Steuert die Anzahl der Byte in jedem protokollierten Paket. Der Bereich ist unbegrenzt und beginnt bei 0. Der Standardwert ist 300.

---

## Zugriffssteuerungslisten für UNIX, Linux und Mac OS X

Client-Agenten für UNIX, Linux und Mac OS X unterstützen ACLs nur im Einzelbenutzermodus. Dieser wird auch als 'Kein-Kennwort-Modus' bezeichnet. Ein Client-Agent für UNIX, Linux und Mac OS X (oder ein Datenbank-Agent) kann in den Einzelbenutzermodus versetzt werden, indem Sie den Eintrag NOPASSWORD im entsprechenden Abschnitt der Konfigurationsdatei für Common Agent, agent.cfg, im Verzeichnis /opt/CA/ABcmagt hinzufügen. Ein Client-Agent für UNIX, Linux und Mac OS X kann auch im Einzelbenutzermodus gestartet werden, wenn in der Datei uag.cfg die Option -S oder -NOPASSWORD angegeben wird. Sie können die folgenden beiden ACL-Typen mit dem Client Agent für UNIX, Linux oder Mac OS X verwenden:

### **Beispiel: Benutzer Zugriff erteilen oder verweigern**

Eine Zugriffssteuerungsliste kann es bestimmten Benutzern ermöglichen oder verbieten, Sicherungen oder Wiederherstellungen vorzunehmen. Im folgenden Beispiel sehen Sie einen Ausschnitt aus der Datei agent.cfg. Sie müssen an den Abschnitten für andere Client-Agenten ähnliche Änderungen vornehmen, wenn auch für diese Client-Agenten ACLs gelten sollen.

```
[0]
NAME ABagentux
VERSION nn.n.n
HOME /opt/CA/ABuagent
NOPASSWORD
CAUSER A:CAUSER1 N:CAUSER2
```

Mit NOPASSWORD wird der Einzelbenutzermodus aktiviert, und mit CAUSER werden die Benutzer angegeben, denen die Berechtigung erteilt oder verweigert wird. (A steht für ALLOW und N steht für DENY.) A:CAUSER1 aktiviert CAUSER1, um Jobs auszuführen, und N:CAUSER2 verweigert den Zugriff auf CAUSER2.

**Hinweis:** Für Client-Agenten für UNIX und Linux ist der Objekttyp [0]. Für Mac OS X Client-Agenten ist der Objekttyp [4].

### Beispiel: Zugriff auf das System mit IP-Adressen

Eine Zugriffssteuerungsliste kann festlegen, ob bestimmte IP-Adressen auf das System zugreifen können. Im folgenden Beispiel sehen Sie einen Ausschnitt aus der Datei agent.cfg. Sie müssen in der Datei an den Abschnitten für andere Client-Agenten ähnliche Änderungen vornehmen, wenn auch für diese Client-Agenten ACLs gelten sollen.

```
[0]
NAME ABagentux
VERSION nn.n.n
HOME /opt/CA/ABuagent
NOPASSWORD
ALLOW N:172.16.0.0(255.255.255.0) H:172.31.255.255
DENY N:192.168.0.0(255.255.255.0) H:192.168.255.255
```

Hierbei aktiviert NOPASSWORD den Einzelbenutzermodus, und ALLOW und DENY legen fest, ob eine bestimmte Netzwerk- oder IP-Adresse Zugriff auf das System hat. N bezeichnet hierbei eine Netzwerkadresse, H die IP-Adresse eines Hosts.

**Hinweis:** Auf eine Netzwerkadresse kann eine optionale Teilnetzmaske folgen. Diese wird in Klammern angezeigt.

Für Client-Agenten für UNIX, Linux und Mac OS X kann der spezifische ACL-Typ in der Datei uag.cfg angegeben werden. Ebenso kann er mit den Optionen -S, -NOPASSWORD, CAUSER, -ALLOW und -DENY angegeben werden. Weitere Informationen zu diesen Optionen finden Sie unter "Konfigurierbare Optionen".

Beide ACL-Typen können nebeneinander verwendet werden. In jedem Fall erhält DENY Vorrang gegenüber ALLOW. Im Einzelbenutzermodus werden alle Vorgänge am Client-Agenten mit Superuser-Rechten vorgenommen. Die Protokolldatei caagentd.log enthält Informationen zu den Benutzern, IP- und Netzwerkadressen, denen im Einzelbenutzermodus der Zugriff verweigert wurde.

### Unterstützung von Zugriffssteuerungslisten für Sicherung und Wiederherstellung für UNIX und Linux

Mit dem CA ARCserve Backup Client Agent für UNIX, dem CA ARCserve Backup Client Agent für Linux und dem CA ARCserve Backup Client Agent für Mainframe Linux kann die Zugriffssteuerungsliste (ACL) für Dateien und Verzeichnisse auf einem Linux-System, das über den Linux-Client Agent gesichert wurde, gesichert und wiederhergestellt werden. Die erweiterten Attribute für Linux werden ebenfalls gesichert. Mit Hilfe von ACLs können Administratoren den Zugriff auf Dateien und Verzeichnisse genauer steuern. Der Linux-Client-Agent ist in der Lage, die ACL für jede Datei und jedes Verzeichnis zu lesen und festzulegen.

## Prüfen der ACL-Bibliotheken

Führen Sie folgenden Befehl aus, um zu prüfen, ob die erforderlichen ACL-Bibliotheken installiert sind:

```
>rpm -qa |grep libacl
```

Sind die Pakete "libacl-devel-\*" oder "libacl-\*" nicht aufgeführt, müssen Sie sie installieren.

## Installieren von ACL-Bibliothekspaketen

### So installieren Sie ACL-Bibliothekspakete:

1. Kopieren Sie die ACL-Bibliothekspakete vom CD-Image, oder laden Sie sie aus dem Internet auf Ihr Linux-System herunter.  
-libacl-Paket (z.B. libacl-2.2.3-1.rpm)  
-libacl-devel-Paket (z.B. libacl-devel-2.3.3-1.rpm)
2. Führen Sie zur Installation der Pakete die folgenden Befehle aus:

```
rpm -ivh <libacl-Paketname>
rpm -ivh <libacl-devel-Paketname>
```

Wie in folgendem Beispiel:

```
>rpm -ivh libacl-2.3.3-1.rpm
>rpm -ivh libacl-devel-2.3.3-1.rpm
```

Hierdurch wird die Bibliothek libacl.so auf Ihrem Linux-System installiert.

Wenn der Linux Client Agent auf einem 32-Bit-Linux-System ausgeführt wird, ist die ACL-Unterstützung jetzt aktiviert. Wenn der Linux Client Agent auf einem 64-Bit-Linux-System ausgeführt wird, müssen Sie sicherstellen, dass es sich bei der Bibliothek libacl.so um die 32-Bit-Version handelt. Sie können die Version überprüfen und gegebenenfalls eine Verknüpfung zu einer 32-Bit-Bibliothek erstellen.

## Prüfen der Linux-Version der ACL-Bibliothek

Wechseln Sie zum Überprüfen der Version in das Verzeichnis, in dem "libacl.so" installiert ist.

### Prüfen der Linux-Version der ACL-Bibliothek

1. Führen Sie ls -l ./libacl.so aus, um die verknüpfte Zielbibliotheksdatei für libacl.so anzuzeigen.
2. Führen Sie file libacl.so <verknüpfte Zielbibliothek> aus, und verwenden Sie dabei den Namen der Bibliotheksdatei.

Das Ergebnis gibt an, ob libacl.so auf eine 32-Bit- oder eine 64-Bit-Version verweist.

### Erstellen einer Verknüpfung zur 32-Bit-Linux-ACL-Bibliothek

Wenn "libacl.so" auf eine 64-Bit-Bibliothek verweist, müssen Sie eine Verknüpfung zwischen der 32-Bit-Bibliothek und "libacl.so" erstellen. Im folgenden Beispiel wird dargestellt, wie Sie die Verknüpfung auf eine 64-Bit Mainframe Linux-Plattform erstellen:

```
> cd /lib  
> ln -sf libacl.so.1 libacl.so
```

Verwenden Sie den entsprechenden Verknüpfungsbefehl für Ihr 64-Bit-Linux-System.

## Konfiguration der AS/400 Enterprise Option

Die Voreinstellungen zum Starten und Stoppen für die AS/400 Enterprise Option werden mit den Befehlen straso und endaso konfiguriert.

### Konfigurieren der Voreinstellungen zum Starten

Die Einstellungen für Sicherungen auf Bibliotheksebene können so konfiguriert werden, dass sie die AS/400 Enterprise Option erweitern.

#### **So konfigurieren Sie Voreinstellungen zum Starten:**

1. Geben Sie in der Befehlszeile Folgendes ein:

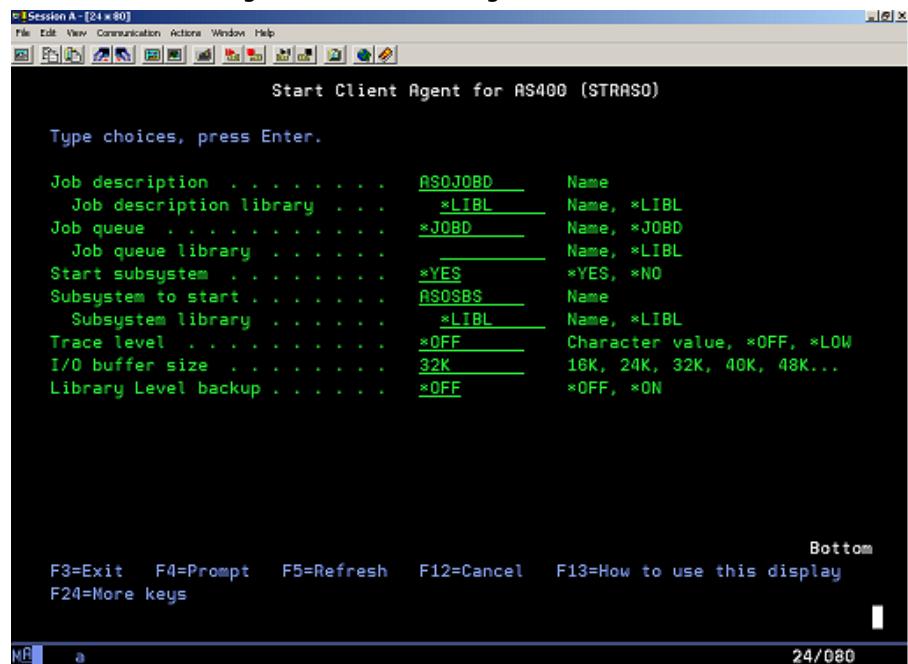
```
straso
```

2. Drücken Sie <font size= -1>F4</font>.

Die verfügbaren Optionen werden angezeigt.

3. Geben Sie Ihre Einstellungen ein, und drücken Sie die Eingabetaste.

**Hinweis:** Sie können die Voreinstellungen für die Sicherung auf Bibliotheksebene und die Verwendung von QaneSava konfigurieren. Diese Voreinstellungen steigern die Leistung. Weitere Informationen finden Sie im Abschnitt "Konfiguration der Leistung".



```

Session A - [24 x 80]
File Edit View Communication Actions Windows Help
Start Client Agent for AS400 (STRASO)

Type choices, press Enter.

Job description . . . . . ASOJOB
  Job description library . . . *LIBL
  Job queue . . . . . *JOBD
  Job queue library . . . .
  Start subsystem . . . . *YES
  Subsystem to start . . . ASOSBS
  Subsystem library . . . *LIBL
  Trace level . . . . . *OFF
  I/O buffer size . . . . 32K
  Library Level backup . . . *OFF

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
MR a 24/080

```

## Konfiguration der Leistung

Standardmäßig sind sowohl die Sicherung auf Bibliotheksebene als auch die Verwendung von QaneSava aktiviert. Diese Einstellungen steigern die Leistung des Agenten bei Sicherungen auf Bibliotheksebene.

Verwenden Sie das Flag für die Verwendung von QaneSava, um zwischen "\*EIN" und "\*AUS" zu wechseln. Ist das Flag für die Verwendung von QaneSava auf "\*EIN" gesetzt, wird bei den Sicherungen keine temporäre "SAVF"-Datei erstellt. Ist das Flag auf "\*AUS" gesetzt, wird bei den Sicherungen eine temporäre "SAVF"-Datei erstellt.

Über das Flag für die Sicherung auf Bibliotheksebene können Sie die Sicherung von Bibliotheken steuern. Ist das Flag auf "\*EIN" gesetzt, wird der Befehl "SAVLIB" auf die Bibliotheksobjekte angewendet. Der Befehl "SAVLIB" steigert die Leistung, da sowohl die Bibliotheksinformationen als auch alle Dateien innerhalb einer Bibliothek in einer einzigen Sicherung gespeichert werden. Die Sicherungsfunktion auf Bibliotheksebene ist besonders nützlich, wenn mehrere Bibliothekssicherungen durchgeführt werden.

Ist das Flag auf "\*AUS" gesetzt, wird über den Befehl "SAVOBJ" jede Datei in einer separaten Bibliothek gesichert. Gehen Sie so vor, wenn Sie keine Sicherungen auf Bibliotheksebene planen.

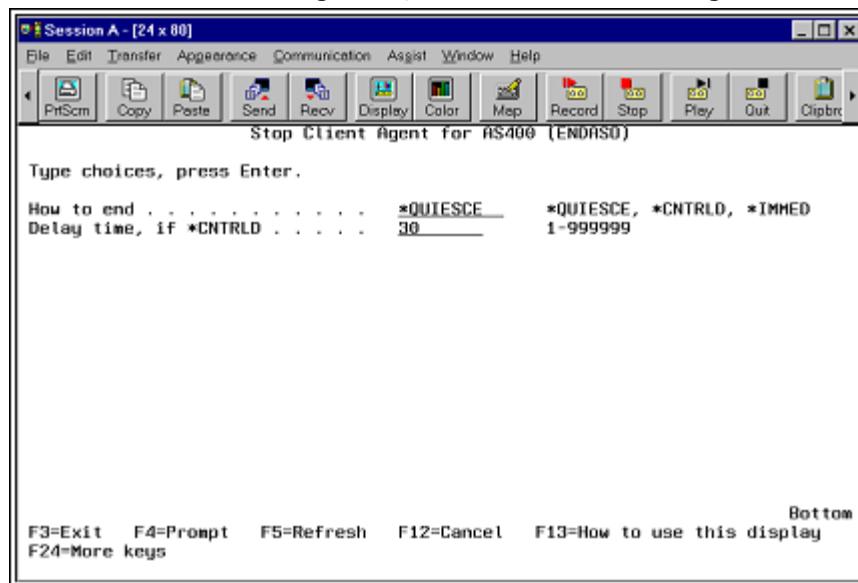
**Hinweis:** Die Sicherungsfunktion auf Bibliotheksebene unterstützt keine Zuwachs- oder Änderungssicherungen.

## Konfigurieren der Voreinstellungen zum Stoppen

Gegebenenfalls können Sie Voreinstellungen zum Stoppen der AS/400 Enterprise-Option festlegen.

### So konfigurieren Sie Voreinstellungen zum Stoppen:

1. Geben Sie in der Befehlszeile Folgendes ein:  
endaso
2. Drücken Sie <font size= -1>F4</font>.  
Die Optionen werden auf dem Konfigurationsbildschirm angezeigt.
3. Geben Sie Ihre Einstellungen ein, und drücken Sie die Eingabetaste.



## Konfiguration der OpenVMS Enterprise Option

Außer der Port-Adresse erfordert die OpenVMS Enterprise Option keine zusätzliche Konfiguration nach der Installation.

## Konfigurieren der Port-Adresse

Die Standardadresse für TCP- und UDP-Ports lautet "6050". Der TCP-Port wird für die Kommunikation und Datenübertragung zwischen "cprocess" und Client Agent verwendet. CA ARCserve Backup verwendet den UDP-Port zum Durchsuchen von Hosts.

Wenn Sie den TCP- oder UDP-Port konfigurieren möchten, tragen Sie den folgenden Befehl in die Datei bab\$startup.com ein:

```
DEFINE /SYSTEM ASO$PORT_NUMBER nnnn
```

In diesem Beispiel steht nnnn für die Port-Nummer des Sicherungs-Managers.

**Wichtig!** Voraussetzung für OpenVMS ist, dass sowohl dem UDP-Port als auch dem TCP-Port dieselbe Port-Nummer zugewiesen ist.

## Optimierung des TCP/IP-Stack

Die Konfiguration des TCP/IP-Stack kann die Leistung des Client-Agenten beeinflussen. In der Regel sind die TCP-Kontingente für Senden und Empfangen auf 4096 eingestellt. Setzen Sie diese Werte auf den höchsten, für diesen Stack auf dem OpenVMS-System zulässigen Wert.

## Verfolgungsebenen für die OpenVMS Enterprise Option

Möglicherweise müssen Sie, den Anweisungen vom Technischen Support von Computer Associates folgend, die für die OpenVMS Enterprise Option protokolierte Aktivitätsebene ändern. Da Verfolgungsebenen die Leistung der Sicherung beeinträchtigen können, ändern Sie die Werte nur dann, wenn Sie spezifische Anweisungen vom Technischen Support von CA erhalten.

Ebene	Beschreibung
ASO\$TRACE	Steuert die Verfolgungstiefe des Client-Agenten. Gültige Werte sind -1 und 0 bis 0xFFFFFFFF. Wenn ASO\$TRACE auf den Wert -1 eingestellt ist, sind die Protokolle am detailliertesten.
ASO\$TRACE_AST	Dies ist ein Umschalter. Wenn diese Funktion definiert ist, werden Asynchronous System Traps (ASTs) verfolgt.
ASO\$TRACE_IDENT	Dies ist ein Formatierungsparameter. Der empfohlene Wert liegt zwischen 0 und 5. Der Standardwert ist 3.
ASO\$TRACE_DATA	Steuert die Anzahl der Byte von jedem protokollierten Paket. Der Bereich ist unbegrenzt und beginnt bei 0. Der Standardwert ist 300.



# Kapitel 4: Verwenden der Client-Agenten

---

Dieses Kapitel beschreibt unter Anderem das Starten und Beenden von Client Agents und das planen oder initiieren von Sicherungen von Client Agents in Standardumgebungen.

Dieses Kapitel enthält folgende Themen:

- [Laufzeitstatistik](#) (siehe Seite 63)
- [Aktivitätsprotokolle](#) (siehe Seite 64)
- [Sichern von Daten auf einem Windows-Netzwerkserver](#) (siehe Seite 68)
- [Starten und Stoppen des Client-Agenten](#) (siehe Seite 68)

## Laufzeitstatistik

Die Laufzeitkomponenten der Client-Agenten für Windows und NetWare stellen statistische Daten in Echtzeit zur Verfügung und zeigen den Fortschritt von Sicherungs- und Wiederherstellungsjobs während der Durchführung an.

**Hinweis:** Laufzeitstatistiken sind nur unter Windows und NetWare verfügbar.

## Anzeigen der Laufzeitstatistik für den Client Agent für Windows

Mit CA ARCserve Backup können Sie die Durchlaufzeitstatistik für Computer mit Client Agent für Windows anzeigen.

### **So zeigen Sie die Laufzeitstatistik für den Client Agent für Windows an:**

1. Klicken Sie im Windows-Startmenü auf "Programme", wählen Sie unter "CA" die Option "ARCserve Backup", und klicken Sie auf "Backup Agent - Verwaltung".

Das Dialogfeld "Backup Agent – Verwaltung" wird geöffnet.

2. Wählen Sie "Verbindungen".

CA ARCserve Backup zeigt die letzten 32 bearbeiteten Jobs an.

Wenn der Job noch aktiv ist, können Sie darauf klicken, um die aktuelle Laufzeitstatistik anzuzeigen. Ist der Job bereits abgeschlossen, wird die vollständige Statistik angezeigt.

**Hinweis:** Die Statistik wird in Speicher abgelegt. Wenn Sie Backup Agent-Verwaltung und den Universal Agent-Dienst beenden, geht daher die Verbindungsstatistik verloren. Sie können die Ergebnisse des Jobs jedoch weiterhin im Aktivitätsprotokoll nachlesen.

## Anzeigen der Laufzeitstatistik für NetWare Client Agent

Wenn bei Verwendung von NetWare Client Agent das Laufzeitfenster nicht verfügbar ist, müssen Sie erst zu diesem Fenster wechseln. Wenn Sie zum Anzeigen der Serverkonsole die Remote-Konsole (RCONSOLE.EXE) verwenden, halten Sie gleichzeitig die Tasten Alt und F3 gedrückt, bis das Laufzeitfenster geöffnet wird. An der Serverkonsole drücken Sie gleichzeitig die Alt- und Esc-Taste, um in das Fenster zu wechseln.

**Hinweis:** Durch gleichzeitiges Drücken von Strg und Esc wird eine Liste der aktuellen Fenster angezeigt, aus der Sie dann das Laufzeitfenster auswählen können.

## Aktivitätsprotokolle

Das serverbasierte CA ARCserve Backup-System erzeugt ein Aktivitätsprotokoll, in dem Informationen über alle vom Client-Agenten verarbeiteten Jobs angezeigt werden. In den folgenden Abschnitten wird erläutert, wie Sie das Aktivitätsprotokoll für jeden Client-Agenten von der Server-Seite und von der Client-Agent-Seite anzeigen können.

## Anzeigen der Aktivitätsprotokolle auf einem Windows-Server

### So zeigen Sie das Aktivitätsprotokoll auf einem CA ARCserve Backup-Server unter Windows an:

- Wählen Sie auf der CA ARCserve Backup Manager-Konsole im Menü "Schnellstart" den Befehl "Jobstatus" aus.

Der Jobstatus-Manager wird geöffnet.

Klicken Sie auf die Registerkarte "Aktivitätsprotokoll", um eine Liste mit Protokollen anzuzeigen (siehe folgendes Beispiel):

Typ	Server	Datum	Job	Sitzung	Meldung
Diese Woche [ 04.04.2010 - 10.04.2010 ]					
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Bandprocess wurde gestartet.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			RAID-Option wurde gestartet
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenträger aus Laufwerk [1] wird in freien Slot [14] von Wechsler [Gerät:5][CA SIMLIBRARY ] verschoben.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenträger aus Laufwerk [3] wird in freien Slot [12] von Wechsler [Gerät:5][CA SIMLIBRARY ] verschoben.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenträger aus Laufwerk [1] wird in freien Slot [12] von Wechsler [Gerät:5][CA SIMLIBRARY ] verschoben.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Wechsler [Gerät:5][CA SIMLIBRARY ] wird initialisiert.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenbankprozess wurde wiederzugewonnen.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenbankprozess wurde unterbrochen.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenbankprozess wurde gestartet. (MSQL)
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Autorisierungsdienst gestartet
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Jobprocess wird gestartet
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Nachrichtenprozess wurde gestartet.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Benutzer [carolo] Geladen Dienst [Dashboard Sync Service] [wik3ee-x32de] verwendet <ARCserveBgr.exe>
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenträger aus Laufwerk [2] wird in freien Slot [10] von Wechsler [Gerät:5][CA SIMLIBRARY ] verschoben.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenträger aus Laufwerk [2] wird in freien Slot [10] von Wechsler [Gerät:5][CA SIMLIBRARY ] verschoben.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenträger aus Laufwerk [1] wird in freien Slot [9] von Wechsler [Gerät:5][CA SIMLIBRARY ] verschoben.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Wechsler [Gerät:5][CA SIMLIBRARY ] wird initialisiert.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Benutzer [carolo] Geladen Dienst [Tape Engine] [wik3ee-x32de] verwendet <ARCserveBgr.exe>
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			[JOBANTRITTSLAUFZEIT]: Bereitige [Jobnr.: 61] [Beschreibung: LINUX - HSI]
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			[JOBANTRITSCHLANGE]: Bereinigt [Jobnr.: 33] [Beschreibung: My Linux Backup]
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Bandprocess wurde gestoppt.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Bandprocess wurde gestartet.

- Wählen Sie aus dem Jobstatus-Menü die Option "Aktivitätsprotokoll" aus und klicken Sie auf "Druckvorschau".

Die Druckvorschauausgabe einer Aktivitätsprotokolldatei des Client Agent ist auf folgendem Bildschirm zu sehen:

CA ARCserve Backup-Aktivitätsprotokoll					
Typ	Server	Datum	Job	Sitzung	Meldung
Diese Woche [ 04.04.2010 - 10.04.2010 ]					
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Bandprocess wurde gestartet.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			RAID-Option wurde gestartet
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenträger aus Laufwerk [1] wird in freien Slot [14] von Wechsler [Gerät:5][CA SIMLIBRARY ] verschoben.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenträger aus Laufwerk [3] wird in freien Slot [12] von Wechsler [Gerät:5][CA SIMLIBRARY ] verschoben.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenträger aus Laufwerk [1] wird in freien Slot [12] von Wechsler [Gerät:5][CA SIMLIBRARY ] verschoben.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Wechsler [Gerät:5][CA SIMLIBRARY ] wird initialisiert.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenbankprozess wurde wiederzugewonnen.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenbankprozess wurde unterbrochen.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenbankprozess wurde gestartet. (MSQL)
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Autorisierungsdienst gestartet
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Jobprocess wird gestartet
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Nachrichtenprozess wurde gestartet.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Benutzer [carolo] Geladen Dienst [Dashboard Sync Service] [wik3ee-x32de] verwendet <ARCserveBgr.exe>
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenträger aus Laufwerk [2] wird in freien Slot [10] von Wechsler [Gerät:5][CA SIMLIBRARY ] verschoben.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenträger aus Laufwerk [2] wird in freien Slot [10] von Wechsler [Gerät:5][CA SIMLIBRARY ] verschoben.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Datenträger aus Laufwerk [1] wird in freien Slot [9] von Wechsler [Gerät:5][CA SIMLIBRARY ] verschoben.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Wechsler [Gerät:5][CA SIMLIBRARY ] wird initialisiert.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Benutzer [carolo] Geladen Dienst [Tape Engine] [wik3ee-x32de] verwendet <ARCserveBgr.exe>
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			[JOBANTRITTSLAUFZEIT]: Bereitige [Jobnr.: 61] [Beschreibung: LINUX - HSI]
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			[JOBANTRITSCHLANGE]: Bereinigt [Jobnr.: 33] [Beschreibung: My Linux Backup]
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Bandprocess wurde gestoppt.
Informationen	WIK3EE-X32DE	08.04.2010 04:41:44			Bandprocess wurde gestartet.

## Anzeigen der Aktivitätsprotokolle auf einem NetWare Client Agent-Rechner

NetWare Client Agent schreibt in die Datei NWAGENT.LOG, die im Stammverzeichnis des Client-Agenten erstellt wird. Sie können diese Protokolldatei anzeigen, indem Sie sie im Windows-Explorer aus dem Stammverzeichnis des Client-Agenten heraus öffnen. Sie können den Inhalt der Protokolldatei auch anzeigen, indem Sie an der Konsole NWAGENT.LOG zur Anzeige auswählen.

## Anzeigen der Aktivitätsprotokolle auf einem UNIX-, Linux- oder Mac OS X Client Agent-Rechner

Sobald die Ausführung des Client-Agenten für UNIX, Linux oder Mac OS X beginnt, wird im Verzeichnis für Protokolldateien die Aktivitätsprotokolldatei uag.log erstellt und gespeichert. Das Verzeichnis für Protokolldateien befindet sich unter dem Stammverzeichnis des Client-Agenten.

In der Datei uag.log werden alle Aktivitäten und Fehler aufgezeichnet, die während Sicherungs- und Wiederherstellungsjobs des Rechners auftreten. Die Jobs werden der Reihe nach nummeriert und sind in der Protokollansicht außerdem anhand von Datum und Uhrzeit zu unterscheiden.

Auf dem Client Agent-Rechner können Sie den Inhalt der Protokolldateien mit dem Befehl *print Dateiname* anzeigen.

**Hinweis:** Alle Protokollmeldungen, die sich auf Common Agent beziehen, befinden sich in der Datei /opt/CA/ABcmagt/logs/caagentd.log.

## Aktivitätsprotokolle auf Computern mit aktiver AS/400 Enterprise Option

Die AS/400 Enterprise Option erstellt in der CA ARCserve Backup-Bibliothek eine Protokolldatei. Die beiden Dateiteile sind:

- AGENT.MBR: Protokolliert die mit Agentenoperationen verbundenen Aktivitäten und Fehler.
- ASBR.MBR: Protokolliert Informationen zu CA ARCserve Backup-Suchvorgängen.

## Aktivitätsprotokolle auf Computern mit aktiver OpenVMS Enterprise Option

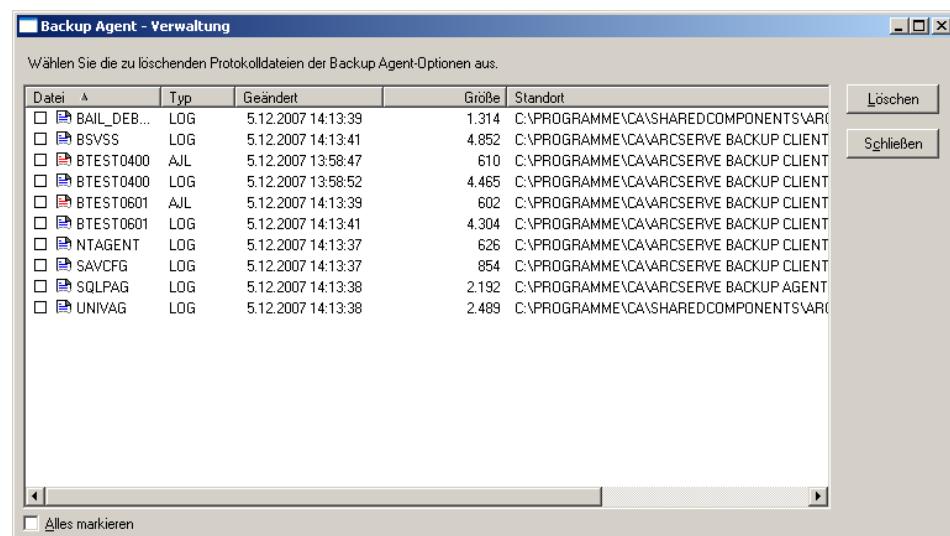
Sobald der Agent auf dem Server ausgeführt wird, erzeugt CA ARCserve Backup eine Aktivitätsprotokolldatei mit den Namen "aso\$agent\_<Knotenname>.log" und speichert diese im Protokollverzeichnis. Für jeden Job und jeden folgenden Start des Agenten wird eine neue Protokolldatei angelegt (zu erkennen an der fortlaufenden Jobnummer, Datum und Uhrzeit). Der Inhalt der einzelnen Protokolldateien wird durch die Verfolgungsebene bestimmt, die im Agenten aktiviert ist.

## Löschen von Client Agent-Protokolldateien

Bei UNIX-, Linux- und Mac OS X-Client-Agenten können Sie Protokolldateien auf die gleiche Weise löschen wie andere Dateien auf diesem Rechner. Führen Sie z.B. Folgendes aus:

```
$>rm uag.log
```

Bei Client Agent für Windows können Sie mit Hilfe der Backup Agent-Verwaltung Protokolldaten löschen: Wählen Sie im Menü "Optionen" die Option "Client Agent-Protokolldateien löschen". Wählen Sie die Protokolldateien aus, die Sie löschen möchten, und klicken Sie wie in der folgenden Abbildung gezeigt auf "Löschen":



## Sichern von Daten auf einem Windows-Netzwerkserv

Wenn Sie einen Client-Agenten auf einem Windows-Server installiert haben, können Sie die Serverdaten folgendermaßen über den Client-Agenten sichern.

### So sichern Sie Daten auf einem Windows-Netzwerkserv:

1. Öffnen Sie den Sicherungs-Manager.
2. Klicken Sie auf die Registerkarte "Quelle".
3. Erweitern Sie die Netzwerkstruktur und anschließend die Struktur "Windows-Systeme", bis Sie den Client-Rechner gefunden haben.
4. Klicken Sie mit der rechten Maustaste auf den Client-Rechner. Wählen Sie aus dem Kontextmenü den Befehl "Agent verwenden".
5. Aktivieren Sie das Kontrollkästchen "Agent verwenden".
6. Wählen Sie ein Protokoll aus. Wählen Sie entweder "TCP/IP", und geben Sie die Adresse des Client-Computers ein, oder wählen Sie "Computernamenauflösung verwenden", damit der Client Agent mit Hilfe von DHCP (Dynamic Host Configuration Protocol) eine IP-Netzwerkadresse ermittelt.
7. Klicken Sie auf "OK".  
Der Client-Agent ist jetzt ausgewählt.
8. Wenn Sie eine Sicherheitsabfrage erhalten, geben Sie die entsprechenden Sicherheitsdaten für Ihre Umgebung ein.

## Starten und Stoppen des Client-Agenten

In den folgenden Abschnitten wird die Vorgehensweise zum Starten und Stoppen der verschiedenen Client-Agenten erläutert.

**Hinweis:** Wird der Client Agent zu einem beliebigen Zeitpunkt während eines Sicherungs- oder Wiederherstellungsjobs gestoppt, schlägt der Job fehl und muss neu gestartet werden.

### Voraussetzungen zum Starten und Stoppen von Windows

Der Windows Client Agent verwendet die allgemeine Komponente Universal Agent. Diese Komponente wird während der Installation installiert oder aktualisiert. Der Universal Agent ist als ein Dienst registriert, der automatisch gestartet und standardmäßig unter Verwendung des lokalen Systemkontos ausgeführt wird. Der Windows Client Agent wird geladen, sobald der Dienst gestartet wird. Der Windows Client Agent ist auch dann verfügbar, wenn keine Benutzer beim System angemeldet sind.

Verwenden Sie die Backup Agent-Verwaltung zum Starten oder Stoppen des Windows Client Agent. Die Backup Agent-Verwaltung überwacht die Aktivität des Client-Agenten und schützt vor versehentlichen Jobfehlern, wenn der Universal Agent-Dienst gestoppt wird.

### Starten oder Stoppen von Windows Client Agent

#### **So starten oder stoppen Sie einen Windows Client-Agenten:**

1. Öffnen Sie die Backup Agent-Verwaltung.
  2. Wählen Sie aus dem Menü "Optionen" die Option "Dienste" aus.
  3. (Optional) Wenn Sie nicht möchten, dass der Client Agent automatisch beim Start Ihres Computers gestartet wird, deaktivieren Sie das Kontrollkästchen "Backup Agent-Dienst beim Systemstart starten".
  4. Klicken Sie auf den Pfeil, um den Dienst zu starten, oder auf den roten Punkt, um den Dienst zu stoppen.
- Hinweis:** Das Stoppen des Dienstes beeinträchtigt andere Komponenten, die den Universal Agent verwenden.
5. Schließen Sie den Backup Agent-Dienst-Manager.

### Voraussetzungen zum Starten und Stoppen von NetWare

Bei der Installation von NetWare Client Agent wird die Netzwerk-Client-Funktionsdatei "NWAGENT.NCF" erstellt. Stellen Sie sicher, dass die Datei im Verzeichnis "SYSTEM" auf dem SYS-Volume des NetWare-Servers erstellt und gespeichert wurde, bevor Sie den Client-Agenten starten.

### Starten von NetWare Client Agent

Geben Sie an der Konsoleaufforderung des Remote-Servers den folgenden Befehl ein, um NetWare Client Agent zu starten:

nwagent

NetWare Client Agent enthält das Modul CSLOADER.NLM, das Überwachungsfunktionen durchführt. Beim Starten von NetWare Client Agent wird gleichzeitig auch CSLOADER.NLM gestartet. CSLOADER.NLM zeigt die Ergebnisse dieses Vorgangs an und zeichnet sie zu Informationszwecken als Meldungen in den Protokolldateien auf. Die Meldungen können bei der Suche nach einer Fehlerquelle hilfreich sein.

CSLOADER.NLM funktioniert auch zusammen mit dem Pre-Flight Check (PFC.NLM), der die Umgebung auswertet, in der der Client Agent ausgeführt wird. Erfüllt die Umgebung die Voraussetzungen nicht, wird CSLOADER.NLM vom Prüfmechanismus angewiesen, die Ladesequenz abzubrechen.

## Stoppen von NetWare Client Agent

Geben Sie an der Konsolenaufforderung des NetWare-Servers den folgenden Befehl ein, um NetWare Client Agent zu stoppen:

```
unload nwagent
```

## Voraussetzungen zum Starten und Stoppen der Client-Agenten für UNIX, Linux und Mac OS X

Stellen Sie vor dem Starten sicher, dass der Client Agent konfiguriert wurde. Sollte dies noch nicht der Fall sein, führen Sie das folgende Skript aus:

```
#abuagent/uagentsetup
```

In diesem Beispiel ist *abuagent* der vollständige Pfadname für das Stammverzeichnis des Agenten. Der standardmäßige Pfad ist /opt/CA/ABuagent.

## Starten des Client-Agenten für UNIX, Linux oder Mac OS X

Nach dem Installieren eines Client-Agenten für UNIX, Linux oder Mac OS X wird dieser automatisch gestartet.

Um den Status des Agenten zu prüfen, geben Sie folgenden Befehl in der Befehlszeile ein:

```
# uagent status
```

Um den Agenten zu starten, geben Sie folgenden Befehl in der Befehlszeile ein:

```
# uagent start
```

Wenn der Agent nicht aktiviert ist, führen Sie das Konfigurationsskript (*uagentsetup*) aus.

## Stoppen des Client-Agenten für UNIX, Linux oder Mac OS X

Um den Client-Agenten für UNIX, Linux oder Mac OS X zu stoppen, melden Sie sich als "root" an, und geben Sie in der Befehlszeile folgenden Befehl ein:

```
# uagent stop
```

## Status beim Starten und Stoppen des Common Agent

Bei jedem Starten oder Stoppen eines Client-Agenten verändern die UNIX-, Linux- oder Mac OS X-Systemskripte die Datei agent.cfg und markieren den Eintrag für den Client-Agenten als aktiviert oder deaktiviert. Außerdem benachrichtigen sie Common Agent von dieser Änderung. Daraufhin ermittelt Common Agent anhand der Zahl der noch aktivierte Einträge in der Konfigurationsdatei, ob er weiter ausgeführt werden soll.

Beispielsweise wird mit dem Befehl uagent stop für einen UNIX-Client der Abschnitt für [ABagntux] als deaktiviert markiert. Ist "ABagntux" der einzige Abschnitt der Datei (wenn nur ein CA ARCserve Backup-Client Agent installiert ist), wird der Common Agent beendet. In diesem Fall müssen Sie den Befehl uagent start eingeben, um den Abschnitt [ABagntux] der Datei agent.cfg wieder zu aktivieren.

Nach Eingabe des Befehls uagent start ändert sich der Status von Common Agent von deaktiviert zu aktiviert. Wenn also ein bestimmter Client Agent gestartet oder gestoppt wird, nehmen die Skripte die entsprechenden Änderungen an der Datei agent.cfg vor und benachrichtigen Common Agent. Daraufhin entscheidet Common Agent anhand der Zahl der noch aktivierte Abschnitte in der Konfigurationsdatei, ob er weiter ausgeführt werden soll.

## Prüfen des Status der Client-Agenten für UNIX, Linux und Mac OS X

Melden Sie sich als "root" an, und geben Sie an der Befehlszeile folgenden Befehl ein, um den Status der Client-Agenten für UNIX, Linux oder Mac OS X zu überprüfen:

```
# uagent status
```

Schlägt dieser Befehl fehl, muss der Client Agent möglicherweise konfiguriert werden. Führen Sie folgendes Skript aus, um den Client-Agenten zu konfigurieren:

```
#abuagent/uagentsetup
```

In diesem Beispiel ist *abuagent* der vollständige Pfadname für das Stammverzeichnis des Agenten. Der standardmäßige Pfad ist /opt/CA/ABuagent.

## Voraussetzungen zum Starten und Stoppen der AS/400 Enterprise Option

Sie müssen über die Berechtigung \*JOBCTL (Jobkontrolle) verfügen, um den Client-Agenten starten oder stoppen zu können.

### **Starten des Client Agent für Enterprise Option für AS/400**

Um den Agenten zu starten, melden Sie sich bei AS/400 an und geben folgenden Befehl in der Befehlszeile ein:

straso

### **Stoppen des Client Agent für Enterprise Option für AS/400**

Um den Agenten zu stoppen, melden Sie sich bei AS/400 an und geben folgenden Befehl in der Befehlszeile ein:

endaso

## **Voraussetzungen zum Starten und Stoppen der OpenVMS Enterprise Option**

Stellen Sie sicher, dass Sie über die erforderlichen Netzwerkrechte verfügen, um den OpenVMS-Rechner zu betreiben, auf dem sich der Client Agent befindet.

### **Starten des Client Agent für Enterprise Option für OpenVMS**

Um den Agenten zu starten, melden Sie sich als system an und geben folgenden Befehl in der Befehlszeile ein:

@sys\$startup:bab\$startup.com

### **Stoppen des Client Agent für Enterprise Option für OpenVMS**

Um den Agenten zu stoppen, melden Sie sich als "system" an und geben folgenden Befehl in der Befehlszeile ein:

@sys\$startup:bab\$shutdown.com

### **Prüfen des Status für den Client Agent für Enterprise Option für OpenVMS**

Um den Status des Client-Agenten zu prüfen, melden Sie sich an und geben folgenden Befehl in der Befehlszeile ein:

show sys /proc=aso\$\*

# Index

---

## A

ABuagent/uagentsetup, Befehl - 70  
ACL-Bibliothek  
    32-Bit-Linux - 57  
    Linux libacl.so - 57  
    Pakete - 57  
    Voraussetzungen - 57  
agent.cfg  
    Client Agent-Konfigurationsdatei - 44  
Aktivitätsprotokoll  
    Anzeigen - 65  
    AS/400-Verfolgungsebenen - 54  
    Beispiel - 65  
    Infos - 64  
AS/400  
    endaso, Befehl - 60  
    Jobkontrolle - 71  
    Konfiguration - 58  
    Sicherung auf Bibliotheksebene, Funktion - 59  
    straso, Befehl - 72  
ASCONFIG.INI - 37

## B

bab\$shutdown.com OpenVMS, Befehl - 72  
bab\$startup.com OpenVMS, Befehl - 72  
Backup Agent-Verwaltung - 24  
Befehle  
    \$>rm uag.log - 67  
    ABuagent/uagentsetup - 70  
    bab\$shutdown.com OpenVMS - 72  
    bab\$startup.com OpenVMS - 72  
    caagent - 44  
    endaso AS/400 - 72  
    mount - 49  
    nwagent - 69  
    print <Dateiname>, Befehl zur Anzeige von  
        Protokollen - 66  
    straso AS/400 - 72  
    uagent status - 70  
Benutzerzugriff, Common Agent - 45  
Besondere Aspekte bei der Installation  
    NetWare - 13  
    OpenVMS - 14

Windows - 13  
Browser-Konfigurationsdatei - 39

## C

caagent  
    start, Befehl - 44  
    stop, Befehl - 44  
    update, Befehl - 44  
caagentd  
    Binärdatei für Common Agent - 40  
    Protokolldatei für Common Agent - 66  
caagperf.cfg, Konfigurationsdatei - 49, 51  
caagperf.log, Datei - 49  
cabr.cfg, Browser-Konfigurationsdatei - 39  
CAPortConfig.cfg  
    Beispiel - 30  
    Konfigurationsdatei - 44  
Common Agent  
    agent.cfg - 40  
    Automatische Installation - 16  
    caagentd, Binärdatei - 40  
    Host-Äquivalenz, Benutzerzugriff - 45  
    Konfigurationsdatei - 40  
    Port-Nummern - 44  
    Verbinden - 46  
    Verwenden von Skripten zum Starten und  
        Stoppen - 44  
    Verzeichnis - 40  
Computernamenauflösung  
    Auswahl des Protokolls - 68  
cprocess - 44

## D

Datei zur Dateisystemsteuerung - 39  
Datei zur Verzeichnissteuerung - 39  
DirectIO  
    Infos - 49  
    UNIX-Unterstützung - 49

## E

Einzelbenutzermodus - 55  
endaso AS/400, Befehl - 72  
Erstellen einer Verknüpfung zwischen 32-Bit-  
Bibliothek und libacl.so - 58

---

## F

fscntl, Datei zur Dateisystemsteuerung - 39  
fssnap - 49

## H

Hinzufügen oder automatisches Erkennen von Client-Agenten - 19  
Hinzufügen von Client-Agenten manuell zu einem Windows- oder NetWare-Server - 20  
Host-Äquivalenz, Benutzerzugriff - 45

## I

Installieren  
  ACL-Bibliotheken - 57  
  Client Agent für Windows - 15  
IP-Adresse  
  ACLs für UNIX, Linux und Mac OS X - 55

## J

Jobkontrolle für AS/400 - 71

## K

Kennwort, Windows - 32  
Konfigurationsdateien  
  agent.cfg - 44  
  caagperf.cfg - 49, 52  
  CAPortConfig.cfg - 30, 44  
  port.cfg - 44  
  PortsConfig.cfg - 30  
  Solaris, Beispiel - 53  
Konfigurieren  
  AS/400 - 58  
  NetWare Client Agent - 36  
  OpenVMS - 60  
  Snapshot und DirectIO - 51  
  UNIX, Linux und Mac OS X Client Agent - 38  
  Windows Client Agent - 22  
  Windows-Netzwerkkommunikation - 30  
  Windows-Sicherheitsoptionen - 28  
Kontrolldateien - 39

## L

Laufzeitstatistik - 63  
libacl.so, ACL-Bibliothek - 57  
Linux  
  32-Bit-ACL-Bibliothek - 57  
Prüfen der ACL-Bibliotheksversion - 57

Verknüpfung zur 32-Bit-ACL-Bibliothek - 58

## M

Manager-Benutzeroberfläche für Windows - 20

## N

NetWare  
  ASCONFIG.INI - 37  
  CSLOADER.NLM - 69  
  Geöffnete Dateien - 36  
  Konfigurieren des Client-Agenten - 36  
  NDS - 38  
  Netzwerk-Client-Funktion - 69  
  nwagent, Befehl - 69  
  Pfadname - 36  
  unload nwagent, Befehl - 70  
  Netzwerkkarten (NIC)  
    IP-Adresse - 30  
  Novell-Verzeichnisdienste (NDS) - 38  
  nwagent, Befehl - 69  
  nwagent.log, NetWare-Protokolldatei - 66

## O

OpenVMS  
  bab\$shutdown.com, Befehl - 72  
  bab\$startup.com, Befehl - 72  
  Konfiguration - 60  
  Optimierung des TCP/IP-Stack - 61  
  show sys /proc=aso\$\*, Befehl - 72

## P

Packen von Jobs - 35  
port.cfg  
  Common Agent - 44  
  UNIX- und Linux-Konfigurationsdatei - 44  
Port-Adresse konfigurieren - 44  
Port-Nummern, Common Agent - 44  
PortsConfig.cfg, Konfigurationsdatei - 30  
print <Dateiname>, Befehl - 66  
Protokoll - 20  
Protokolldateien  
  Aktivität - 65  
  caagperf.log - 49  
  Löschen - 67  
  nwagent.log - 66  
Prüfen des Agent-Status  
  OpenVMS - 72  
  UNIX, Linux und Mac OS X - 70

---

## S

für UNIX, Linux und Mac OS X - 55

show sys /proc=aso\$\* OpenVMS, Befehl - 72  
Sicherung auf Bibliotheksebene, Funktion - 59  
Skripte  
    uagentsetup - 70  
    Verwenden zum Ändern der Datei agent.cfg  
        - 71  
Snapshot  
    Ausgabe - 49  
    Funktionen - 49  
    Infos - 49  
    Puffer - 49  
    UNIX-Unterstützung - 49  
Stammverzeichnis - 43  
Starten von Client-Agenten - 68  
Stoppen von Client-Agenten - 68  
straso AS/400, Befehl - 72

## U

uag.cfg - 38  
uagcntl, Datei zur Verzeichnissteuerung - 39  
uag.log, Aktivitätsprotokolldatei - 66  
uagent, Befehl - 70  
uagentsetup, Skript - 70  
UDP-Port, Common Agent - 44  
Umgebungsvariable (ENV) - 41  
unload nwagent, Befehl - 70

## V

Verfolgungsebenen  
    AS/400 - 54  
    OpenVMS - 61  
Virensuche - 34

## W

Windows  
    Backup Agent-Verwaltung - 24  
    Freigabenunterstützung - 22  
    IP-Adresse - 30  
    Kennwortsicherheit - 24  
    Port-Nummer - 30  
    Prozesspriorität - 24  
    Systembereich wiederherstellen - 22  
    Systemstatus wiederherstellen - 22  
    Virensuche aktivieren - 34

## Z

Zugriffssteuerungslisten (ACL)