CA ARCserve® Backup

Client Agent - Benutzerhandbuch

r12

Dieses Handbuch sowie alle zugehörigen Software-Hilfeprogramme (nachfolgend zusammen als “Dokumentation” bezeichnet) dienen ausschließlich zu Informationszwecken des Endbenutzers und können von CA jederzeit 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. Die Informationen in dieser Dokumentation sind geistiges Eigentum von CA und durch das Urheberrecht der Vereinigten Staaten sowie internationale Verträge geschützt.

Ungeachtet der oben genannten Bestimmungen ist der Benutzer, der über eine Lizenz verfügt, berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen innerbetrieblichen Gebrauch auszudrucken sowie eine Kopie der zugehörigen Software zu Sicherungs- und Wiederherstellungszwecken im Notfall (Disaster Recovery) anzufertigen, vorausgesetzt, dass jedes Exemplar diesen Urheberrechtsvermerk und sonstige Hinweise von CA enthält. Ausschließlich berechtigte Beschäftigte, Berater oder Vertreter des Benutzers, die an die Vertraulichkeitsbestimmungen der Produktlizenz gebunden sind, erhalten Zugriff auf diese Kopien.

Das Recht zum Drucken von Dokumentationskopien und Anfertigen einer Kopie der zugehörigen Software beschränkt sich auf den Zeitraum der vollen Wirksamkeit der Produktlizenz. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Lizenznehmer gegenüber CA schriftlich, dass alle Kopien oder Teilkopien der Dokumentation an CA zurückgegeben oder vernichtet worden sind.

CA STELLT DIESE DOKUMENTATION, SOWEIT ES DAS ANWENDBARE RECHT ZULÄSST UND SOFERN IN DER ANWENDBAREN LIZENZVEREINBARUNG NICHTS ANDERES ANGEBEBEN WIRD, SO WIE SIE VORLIEGT OHNE JEDE GEWÄHRLEISTUNG ZUR VERFÜGUNG; DAZU GEHÖREN, OHNE SICH JEDOCH DARAUF ZU BESCHRÄNKEN, STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG. IN KEINEM FALL HAFTET CA GEGENÜBER DEM ENDBENUTZER ODER DRITTEN FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER VERWENDUNG DIESER DOKUMENTATION ENTSTEHEN; DAZU GEHÖREN, OHNE SICH JEDOCH DARAUF ZU BESCHRÄNKEN, ENTGANGENE GEWINNE, BETRIEBSUNTERBRECHUNG, VERLUST IDEELLER UNTERNEHMENSWERTE ODER DATENVERLUST, SELBST WENN CA ÜBER DIESEN VERLUST ODER SCHADEN INFORMIERT WURDE.

Die Verwendung aller in der Dokumentation aufgeführten Produkte unterliegt der geltenden Lizenzvereinbarung des Endbenutzers.

Diese Dokumentation wurde von CA hergestellt.

Diese Dokumentation wird mit "Restricted Rights" (eingeschränkten Rechten) geliefert. Die Verwendung, Duplizierung 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.

Alle Marken, Produktnamen, Dienstleistungsmarken oder Logos, auf die hier verwiesen wird, sind Eigentum der entsprechenden Rechtsinhaber.

Copyright © 2008 CA. Alle Rechte vorbehalten.

CA-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA:

- Advantage™ Ingres®
- BrightStor® ARCserve® Backup for Laptops and Desktops
- BrightStor® CA-1® Tape Management
- BrightStor® CA-Dynam®/B Backup für VM
- BrightStor® CA-Dynam®/TLMS Tape Management
- BrightStor® CA-Vtape™ Virtual Tape System
- BrightStor® Enterprise Backup
- BrightStor® High Availability
- BrightStor® Storage Resource Manager
- BrightStor® VM:Tape®
- CA ARCserve® Backup Agent für Novell Open Enterprise Server für Linux
- CA ARCserve® Backup Agent for Open Files für NetWare
- CA ARCserve® Backup Agent for Open Files für Windows
- CA ARCserve® Backup Client Agent für FreeBSD
- CA ARCserve® Backup Client Agent für Linux
- CA ARCserve® Backup Client Agent für Mainframe Linux
- CA ARCserve® Backup Client Agent für NetWare
- CA ARCserve® Backup Client Agent für UNIX
- CA ARCserve® Backup Client Agent für Windows
- CA ARCserve® Backup Enterprise Option für AS/400
- CA ARCserve® Backup Enterprise Option für Open VMS
- CA ARCserve® Backup für Windows
- CA ARCserve® Backup Agent für IBM Informix für Windows
- CA ARCserve® Backup Agent für Lotus Domino für Windows
- CA ARCserve® Backup Agent für Microsoft Data Protection Manager für Windows
- CA ARCserve® Backup Agent für Microsoft Exchange für Windows
- CA ARCserve® Backup Agent für Microsoft SharePoint für Windows

- CA ARCserve® Backup Agent für Microsoft SQL Server für Windows
- CA ARCserve® Backup Agent für Oracle für Windows
- CA ARCserve® Backup Agent für Sybase für Windows
- CA ARCserve® Backup Agent für VMware für Windows
- CA ARCserve® Backup Disaster Recovery Option für Windows
- CA ARCserve® Backup Disk to Disk to Tape Option für Windows
- CA ARCserve® Backup für das Windows Enterprise-Modul
- CA ARCserve® Backup Enterprise Option für IBM 3494 für Windows
- CA ARCserve® Backup Enterprise Option für SAP R/3 für Oracle für Windows
- CA ARCserve® Backup Enterprise Option für StorageTek ACSLS für Windows
- CA ARCserve® Backup Image Option für Windows
- CA ARCserve® Backup Microsoft Volumeschattenkopie-Dienst für Windows
- CA ARCserve® Backup NDMP NAS Option für Windows
- CA ARCserve® Backup Serverless Backup Option für Windows
- CA ARCserve® Backup Storage Area Network (SAN) Option für Windows
- CA ARCserve® Backup Tape Library Option für Windows
- CA XOsoft™ Assured Recovery™
- CA XOsoft™
- Common Services™
- eTrust® Antivirus
- eTrust® Firewall
- Unicenter® Network and Systems Management
- Unicenter® Software Delivery
- Unicenter® VM:Operator®

Kontakt zum Kundendienst

Für technische Unterstützung online sowie eine vollständige Liste der Standorte, der Servicezeiten und der Telefonnummern wenden Sie sich an den Kundendienst unter http://www.ca.com/worldwide.

Inhalt

Kapitel 1: 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.

Dieses Kapitel enthält folgende Themen:

Funktionen des 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
- Sicherungsprotokolle mit dem Status der Sicherungs- und Wiederherstellungsvorgänge

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

Unterstützte Client-Systeme

CA ARCserve Backup verfügt über die folgenden Client-Agenten:

- CA ARCserve Backup Client Agent für Windows. Dieser Client-Agent unterstützt:
  - Windows Server 2008 (nur Kernbetriebssystem)
  - Microsoft Vista™
  - Windows 2000
  - Windows XP
  - Windows Server 2003
  - Windows Small Business Server (SBS) unter Windows 2000 Server oder Windows 2003 Server
- 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

- CA ARCserve Backup Client Agent für Mainframe Linux. Dieser Client-Agent unterstützt:
  - Red Hat Enterprise Server 3, 4 (31 Bit und 64 Bit) unter zSeries und S/390
  - SLES 8 und 9 (32-Bit und 64-Bit) unter zSeries und S/390
- CA ARCserve Backup Enterprise Option für AS/400
- CA ARCserve Backup Client Agent für Mac OS X
- CA ARCserve Backup Enterprise Option für OpenVMS

Weitere Informationen zu zusätzlichen Hardware- und Software-Voraussetzungen bei der Installation und Ausführung von Client-Agenten finden Sie in der Readme auf der Installations-CD. Wenn Sie Hilfe benötigen, wenden Sie sich an den Technischen Support unter http://ca.com/worldwide.

Die Funktionsweise von Client-Agenten

CA ARCserve Backup und die Client-Agenten sind für Datenspeicheraktivitäten in Unternehmen und Organisationen mit vernetzten Computern ausgelegt. Mit den Client-Agenten können Sie wichtige Unternehmensdaten im Netzwerk sichern und wiederherstellen. Die Client-Agenten unterstützen Sie, indem sie:

- die Sicherung von Anwendungen oder Dateisystemen ermöglichen.
- die Überwachung des Sicherungsfortschritts erleichtern.
- die Überwachung von Aktivitäten im Sicherungsprotokoll vereinfachen.

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.

Funktionen des Agenten

In diesem Abschnitt werden die Funktionen der verschiedenen Client Agenten von CA ARCserve Backup erläutert.

Push-Technologie

Alle Client-Agenten nutzen zur Automatisierung des Sicherungs- und Wiederherstellungsprozesses die Push-Technologie. Der Client-Agent enthält eigene interne Client-Prozesse, die dazu beitragen, die ressourcenbelastenden Sicherungsprozesse auf dem CA ARCserve Backup-Server zu optimieren. Mit dieser Funktion filtert und packt der Client-Agent seine Archivdaten, bevor er sie an den Server übergibt. Diese Methode der Datenvorbereitung und -übertragung ermöglicht das Durchsuchen von Verzeichnissen in Echtzeit. Außerdem werden die Systemressourcen des Sicherungsservers entlastet, die Datenübertragung durch den Einsatz der Pakettechnologie verbessert, Netzwerksicherheit geboten und Sicherungs- und Wiederherstellungsjobs überwacht.

Nach der Installation und Konfiguration der Client-Agenten können Sie mit CA ARCserve Backup Daten von allen Workstations in Ihrem Datennetzwerk abrufen. Der Client-Agent durchsucht die ihm zugewiesenen Verzeichnisse, bereitet die Daten vor und überträgt sie über das Paketnetzwerk. Anschließend bereitet der Sicherungsserver die Daten für die Speicherung auf den vorgesehenen Sicherungsgeräten vor. Durch diese aufeinander abgestimmten Prozesse zwischen Client-Workstation und Sicherungsserver entsteht eine wirkungsvolle automatisierte Sicherungsumgebung.

Windows-Computernamenauflösung

Mit der Computernamenauflösung kann der lokale Windows-Computer automatisch die IP-Adresse des Remote-Rechners beim Herstellen der Verbindung für Sicherungen und Wiederherstellungen erkennen.

Sowohl der Sicherungsserver als auch die Netzwerk-Clients können diese Funktion verwenden. Ein lokaler CA ARCserve Backup-Server kann die Computernamenauflösung zum Herstellen der Verbindung und zum Sichern von Daten auf Remote-Rechnern verwenden.

Sicherheitsfunktionen

Die Client-Agenten für CA ARCserve Backup verfügen über verschiedene Sicherheitsfunktionen, beispielsweise Kennwortschutz für den Client-Agenten, Systemanmeldung, intelligente Datenverschlüsselung zwischen Client und Server und integrierte Virensuche mit Reparatur von befallenen Dateien. Die folgenden Abschnitte enthalten weitere Informationen zu den Datenverschlüsselungs- und Virensuchfunktionen von CA ARCserve Backup.

Intelligente Datenverschlüsselung zwischen Client und Server

Mit der Funktion zur intelligenten Verschlüsselung von Daten zwischen Client und Server können Sie die Netzwerksicherheit weiter verbessern, indem Sie die während eines Sicherungsjobs übertragenen Datenpakete mit einem Sitzungskennwort verschlüsseln. Diese Funktion nutzt die AES 256-Verschlüsselung und gewährleistet, dass die übertragenen oder archivierten Daten sicher und kennwortgeschützt sind. Außerdem wird sowohl die Vertraulichkeit der über das Netzwerk übertragenen Daten als auch die Sicherheit Ihrer Sicherungsdatenträger gewahrt. Benutzer, die den Verschlüsselungscode nicht kennen, können Sicherungsbänder nicht missbrauchen oder wiederherstellen.

Wenn Sie diese Funktion wählen, werden die Sicherungsdaten verschlüsselt. Dies gilt für zwischen Client und Server übertragene Datenpakete, Daten auf dem lokalen Server und Daten, die auf Sicherungsdatenträger verschoben wurden.

Integrierte Virensuche und Reparatur

CA ARCserve Backup führt mit den entsprechenden eTrust Antivirus-Komponenten eine Virenprüfung und -beseitigung zum Schutz Ihrer Daten durch.

Wichtig! *CA ARCserve Backup beinhaltet nur die Komponenten zur Prüfung und Bereinigung. eTrust Antivirus wird nicht vollständig installiert. Für den Windows-Client-Agenten muss eTrust Antivirus zum Empfangen automatischer Aktualisierungen von Virensignaturen vollständig installiert werden.*

Wenn die Virensuchfunktion aktiviert ist, sucht CA ARCserve Backup während Sicherungs- und Kopiervorgängen in den Daten nach Viren. Somit sind wertvolle Daten vor Beschädigung durch Viren geschützt. Wird die Bereinigungskomponente während der Konfiguration gewählt, werden infizierte Dateien ohne jeglichen Benutzereingriff repariert. Somit sind wertvolle Daten vor Beschädigung durch Viren geschützt.

Weitere Informationen zur eTrust Antivirus-Integration finden Sie im *Administrator-Handbuch*.

Auto Discovery von Client-Agenten

Auf CA ARCserve Backup-Systemen, die auf einem Windows-Server installiert sind, können Sie die Funktion zur automatischen Erkennung (Auto Discovery) für alle Computer im Netzwerk aktivieren, auf denen Client-Agenten für Windows oder UNIX, Linux oder Mac OS X ausgeführt werden. Mit Hilfe von Auto-Discovery kann CA ARCserve Backup alle Windows-, UNIX-, Linux- und Mac OS X-Computer erkennen, auf denen die entsprechenden Client-Agenten ausgeführt werden, und automatisch die benötigte Liste der Computer erzeugen, für die regelmäßige Sicherungen geplant werden.

Mehrere Netzwerkkarten

Client Agent für Windows unterstützt die Verwendung mehrerer Netzwerkkarten (Network Interface Cards, NICs). Bei Computern mit mehreren Netzwerkkarten überprüft der Client-Agent alle aktiven NICs, um zu ermitteln, welche Karten aktiviert sind und für die Übertragung verwendet werden.

Optimierte Netzwerkverbindungen

Rechner, auf denen der Windows Client Agent ausgeführt wird, können mit Hilfe von Algorithmen zur Verbindungswiederherstellung nach vorübergehenden Netzwerkausfällen den Betrieb wieder aufnehmen (bei schweren Netzwerkfehlern kann der Windows Client Agent den Betrieb nicht wieder aufnehmen). Die Struktur von CA ARCserve Backup bietet darüber hinaus die Möglichkeit zur Analyse von Netzwerkverbindungen.

Durchsuchen von Verzeichnissen auf Remote-Rechnern in Echtzeit

Mit dieser Funktion können Systemadministratoren Datei- und Verzeichnisinformationen zum Remote-Zielrechner in Echtzeit anzeigen.

Cyclic Redundancy Check (zyklische Redundanzprüfung)

Die Client-Agenten erzeugen für alle an den CA ARCserve Backup-Server gesendeten Dateien CRC-Codes (Cyclic Redundancy Check). Diese dienen dazu, die Integrität der zu sichernden Dateien zu überprüfen.

Globale Optionen für Sicherungsprüfung

Client-Agenten unterstützen die globalen Optionen für Sicherungsprüfung "Sicherungsdatenträger durchsuchen" und "Sicherungsdatenträger mit Original vergleichen", mit denen Sie überprüfen können, ob Ihre Daten ordnungsgemäß gesichert wurden.

Wenn Sie die Option "Sicherungsdatenträger durchsuchen" auswählen, überprüft CA ARCserve Backup den Header jeder Datei auf dem Sicherungsdatenträger. Kann der Header gelesen werden, wird angenommen, dass die Daten fehlerfrei sind. Andernfalls wird das Aktivitätsprotokoll mit diesen Informationen aktualisiert.

Hinweis: Wenn Sie die globale Sicherungsprüfungs-Option für "Sicherungsdatenträger durchsuchen" auswählen und die Option "CRC-Wert berechnen und auf Sicherungsdatenträger speichern" zusätzlich zur Überprüfung des Headers jeder Datei auf dem Sicherungsträger aktivieren, führt CA ARCserve Backup eine CRC-Prüfung durch, indem der CRC-Wert neu berechnet und mit dem auf dem Datenträger gespeicherten Wert verglichen wird.

Wenn Sie die Option "Sicherungsdatenträger mit Original vergleichen" auswählen, liest CA ARCserve Backup Datenblöcke vom Datenträger und vergleicht die Daten byteweise mit den Quelldateien auf dem Quellrechner und gewährleistet damit, dass die Daten auf dem Datenträger genau mit den Daten auf der Festplatte übereinstimmen. Bei der Feststellung einer Abweichung wird das Aktivitätsprotokoll mit diesen Informationen aktualisiert.

Weitere Informationen zu den Optionen für die Sicherungsprüfung finden Sie in der Online-Hilfe.

Zugriffssteuerungslisten (ACLs)

Mit Zugriffssteuerungslisten (Access Control Lists, ACLs) für Client-Agenten für Windows, UNIX, Linux und Mac OS X können Sie steuern, welcher CA ARCserve Backup-Server über den Client-Agenten auf die Workstation zugreift. Die Originalkonfiguration dieser Client-Agenten ermöglicht allen Sicherungsservern das Sichern und Wiederherstellen von Daten über einen Client-Agenten für Windows, UNIX, Linux oder Mac OS X. Indem Sie eine Zugriffssteuerungsliste erstellen, können Sie Datensicherungs- und -wiederherstellungsvorgänge für den jeweiligen Client-Agenten auf eine bestimmte Gruppe von Servern beschränken.

Hinweis: Der Agent für FreeBSD Version 5.3 und 5.4 sichert ACLs (Zugriffssteuerungslisten) und stellt sie wieder her. Es werden sowohl Standard- als auch Zugriffs-ACLs unterstützt. Diese Funktion wird in FreeBSD 4.11 nicht unterstützt.

Erweiterte Attribute für den Client Agent für Linux und FreeBSD

Der Client Agent für Linux und FreeBSD Version 5.3 und 5.4 sichert erweiterte Attribute und stellt sie wieder her. FreeBSD 4.11 unterstützt diese Funktion nicht.

Dateisystemspezifische Flags für den Client Agent für Linux- und FreeBSD

Der Client Agent für Linux und die FreeBSD-Agenten unterstützen die Sicherung und Wiederherstellung von dateisystemspezifischen Attributen (in FreeBSD als Flags bezeichnet). FreeBSD 4.11, 5.3 und 5.4 unterstützen diese Funktion.

Datenkomprimierung

Die Client-Agenten für Windows, UNIX, Linux und Mac OS X unterstützen die Komprimierung von Daten bei der Übertragung im Transmission Control Protocol/Internet Protocol-Netzwerk (TCP/IP). Unter Komprimierung versteht man die Verringerung der Datengröße, um Speicherplatz zu sparen und die Übertragungsdauer zu verbessern. Wenn diese Option aktiviert ist, komprimiert der Client-Agent alle Datenpakete, bevor er mit der Übertragung an den Sicherungsserver beginnt.

Multistreaming

Wenn Sie mehrere Laufwerke und mehrere Volumes sichern müssen, können Sie den Client-Agenten dieses Systems so konfigurieren, dass Multistreaming verwendet wird. Mit Multistreaming können Sie alle verfügbaren Bandgeräte im System nutzen. Bei Multistreaming wird ein Sicherungsjob in mehrere Jobs aufgeteilt, die alle Bandgeräte verwenden. Somit wird im Vergleich zur sequentiellen Single-Stream-Verarbeitung der Durchsatz der Sicherung erhöht.

Auf einem Windows-Server wird Multistreaming auf Volume-Ebene für reguläre Dateisysteme verwendet (zwei Volumes können gleichzeitig auf zwei verschiedenen Geräten ausgeführt werden). Für bevorzugte Freigaben, Remote-Datenbankserver und Windows NT/2000/XP-Agenten wird Multistreaming auf Knotenebene durchgeführt. Auf UNIX- oder Linux-Servern können Sie die Multistreaming-Ebene konfigurieren.

Die Anzahl von Jobs, die Sie gleichzeitig ausführen können, ist auf die Anzahl der lokalen Geräte und Remote-Geräte oder -Gruppen im System beschränkt. Bei Multistreaming wird ein Master-Job erstellt, der Slave-Jobs für die erforderliche Anzahl Volumes auslöst. Sobald ein Job auf einem Gerät abgeschlossen ist, wird ein anderer Job ausgeführt, bis keine Jobs mehr ausgeführt werden müssen. Weitere Informationen zu Multistreaming finden Sie im *Administrator-Handbuch*.

Multiplexing

Beim Multiplexing werden Daten aus verschiedenen Quellen gleichzeitig auf denselben Datenträger geschrieben. Wenn die Multiplexing-Option aktiviert ist, werden Jobs mit mehreren Quellen in untergeordnete Jobs aufgeteilt. Jeder Quelle entspricht dabei ein untergeordneter Job. Diese untergeordneten Jobs schreiben Ihre Daten gleichzeitig auf denselben Datenträger. Weitere Informationen zu Multiplexing finden Sie im *Administrator-Handbuch*.

Snapshot und DirectIO für Solaris und HP-UX

Die Leistung von Volumes mit einem bestimmten UNIX- oder Veritas-Dateisystem (UFS bzw. VxFS) kann mit den Funktionen Snapshot und DirectIO (Direct Input/Output) optimiert werden.

Hinweis: Diese Funktionen sind nur auf Volume-Ebene und nur für Solaris und HP-UX-Systeme verfügbar.

Mit der Snapshot-Funktion ermöglicht der Client-Agent Ihnen eine schnellere und effizientere Datensicherung. Der CA ARCserve Backup-Client-Agent erstellt einen Snapshot eines UNIX-Volumes, lädt den Snapshot in ein temporäres Verzeichnis, das auf dem Stamm-Volume erstellt wird, und erzeugt dann die Sicherung. Nach Abschluss der Snapshot-Sicherung entlädt der Dateisystem-Agent den Snapshot aus dem temporären Verzeichnis und löscht ihn. Manche Rechner im Netzwerk können einen Snapshot ihrer Sicherungsdaten erstellen und an einem alternativen Bereitstellungspunkt laden. Sicherungsanwendungen können dann an dem alternativen Bereitstellungspunkt auf die Daten zugreifen und diese sichern.

Mit der DirectIO-Funktion lädt der UNIX Client Agent erneut das Volume, indem er die Option zum Laden von DirectIO verwendet. Mit dieser Funktion kann die Leistung bei Eingabe-/Ausgabevorgängen verbessert werden, und doppelte Pufferanforderungen können vermieden werden.

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:

Systemvoraussetzungen

Weitere Informationen zu Hardware- und Software-Voraussetzungen bei der Installation und Ausführung von Client-Agenten finden Sie in der Readme auf der Installations-CD. Wenn Sie Hilfe benötigen, wenden Sie sich an den Technischen Support unter http://ca.com/worldwide.

Installationshinweise

Der folgende Abschnitt enthält 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

- Wenn Sie während der Installation des Client Agent für Windows ein Remote-Setup durchführen, gelten einige Einschränkungen. Es gelten die folgenden Einschränkungen:
  - **Windows XP**: Es ist keine Remote-Installation auf einem Rechner unter Windows XP möglich, wenn auf dem Computer die Funktion zum Erzwingen von Netzwerk-Anmeldungen über lokale Konten zur Authentifizierung als Gast konfiguriert ist.
  - **Windows XP (64-Bit Edition)**: Die Remote-Installation wird nicht unterstützt.
  - **Windows 2003 (64-Bit Edition)**: Die Remote-Installation wird nicht unterstützt.

  In diesen Fällen können Sie den Client Agent für Windows direkt von der CA ARCserve Backup-Installations-CD installieren.

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 eines der folgenden Netzwerkprotokolle konfiguriert werden:
  - TCP/IP
- 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 Programmmodule) 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.

Installieren der Client-Agenten

Es gibt zwei CA ARCserve Backup-Installation CDs. Verwenden Sie zur Installation eines Windows-Client-Agenten die CD CA ARCserve Backup r12 für Windows. Verwenden Sie zur Installation eines plattformübergreifenden Agenten die CD CA ARCserve Backup r12 Agent.

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. Die folgenden Abschnitte enthalten Informationen zum Common Agent.

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

Common Agent (Binärdatei caagentd) ist eine Standardkomponente für alle Client-Agenten für UNIX, Linux und Mac OS X, die automatisch während der Erstinstallation jedes Client-Agenten für UNIX, Linux und Mac OS X installiert wird.

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

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

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

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.

Möglicherweise sind nicht alle genannten Komponenten 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]
#[BABagntux]
NAME            BABagntux
VERSION         nn.nn.nn
HOME            /opt/CA/BABuagent
ENV             CA_ENV_DEBUG_LEVEL=4:$CA_ENV_DEBUG_LEVEL
ENV             LD_LIBRARY_PATH=/opt/CA/CAlib:/opt/CA/BABcmagt:$LD_LIBRARY_PATH
ENV             SHLIB_PATH=/opt/CA/CAlib:/opt/CA/BABcmagt:$SHLIB_PATH
ENV             LIBPATH=/opt/CA/CAlib:/opt/CA/BABcmagt:$LIBPATH
BROWSER         cabr
AGENT           uagentd
MERGE           umrgd
VERIFY          umrgd
```

Port-Nummern für Common Agent

Standardmäßig verwendet Common Agent den Port 6051 sowohl für TCP als auch für User Datagram Protocol (UDP). Wenn Sie den Standard-Port ändern möchten, müssen Sie im Abschnitt [BABcmagt] 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]
#[BABcmagt]
#NAME            BABcmagt
#HOME            /opt/CA/BABcmagt
#TCP_PORT        6051
#UDP_PORT        6051
```

Nach der Änderung:

```
[36]
#[BABcmagt]
NAME             BABcmagt
HOME             /opt/CA/BABcmagt
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]
#[BABcmagt]
NAME    BABcmagt
HOME    /opt/CA/BABcmagt
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 im Kapitel “Hinzufügen und Konfigurieren der Client-Agenten” unter “Zugriffssteuerungslisten für UNIX, Linux und Mac OS X”.

Unterstützung von Zugriffssteuerungslisten 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

Zur Aktivierung dieser Funktion sind bestimmte ACL-Bibliotheken erforderlich. 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, installieren Sie sie mit Hilfe der folgenden Vorgehensweise.

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. Gehen Sie folgendermaßen vor:

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, on 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. Das folgende Beispiel erläutert die Erstellung einer Verknüpfung auf einer Mainframe-Linux-Plattfom mit 64-Bit.

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

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

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:

Automatische Erkennung oder manuelles Hinzufügen von Client-Agenten

Wenn Sie CA ARCserve Backup auf einem Windows-Server installiert haben, können Sie die Client-Agenten in Ihrem Netzwerk mit Hilfe von Auto Discovery automatisch erkennen lassen oder Client-Agenten manuell hinzufügen. Die folgenden Abschnitte enthalten Informationen zu beiden Methoden.

Automatisches Erkennen von Client-Agenten

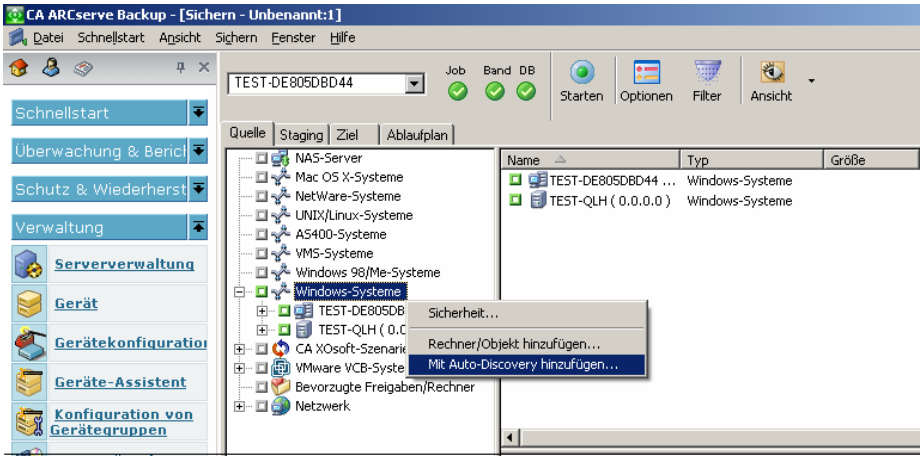
Wenn Sie CA ARCserve Backup auf einem Windows- Server installiert haben, der den Windows-Manager verwendet, können Sie mit Hilfe von Auto Discovery die Client-Agenten für Windows, UNIX, Linux und Mac OS X, die in Ihrem Netzwerk installiert sind und ausgeführt werden, automatisch erkennen lassen. Damit Sie die Auto-Discovery-Funktion zur Erstellung der Sicherungs- und Wiederherstellungsliste verwenden können, muss der Sicherungsprozess ausgeführt werden. Standardmäßig wird der Sicherungsprozess beim ersten Start von CA ARCserve Backup automatisch gestartet. Während bestimmter Vorgänge kann es jedoch notwendig sein, den Prozess zu beenden.

So führen Sie das automatische Erkennen von Client-Agenten durch:

1. Klicken Sie im Fenster "Sicherungs-Manager" auf die Registerkarte "Quelle".

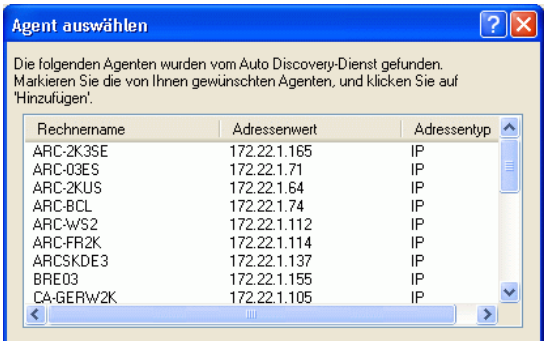
   Hinweis: Wenn der Sicherungsprozess nicht ausgeführt wird, werden Sie bei diesem Vorgang aufgefordert, ihn zu starten.

2. Wählen Sie auf der Registerkarte "Quelle" das entsprechende Client-Agent-Objekt, z. B. "Windows-Systeme".



3. Klicken Sie mit der rechten Maustaste, und wählen Sie im Kontextmenü "Mit Auto-Discovery hinzufügen".

   CA ARCserve Backup zeigt im Dialogfeld "Agent auswählen" eine Liste aller Rechner an, die durch Auto Discovery gefunden werden:



4. Wählen Sie in dieser Liste die Client-Agenten aus, die Sie zur Sicherungsliste hinzufügen möchten.

   Hinweis: Halten Sie die Strg-Taste gedrückt, um mehrere Agenten auszuwählen.

5. Klicken Sie auf "Hinzufügen".
6. Klicken Sie auf "Schließen".

Jeder ausgewählte Agent wird nun im Sicherungs-Manager als Mitglied des jeweiligen Betriebssystems angezeigt.

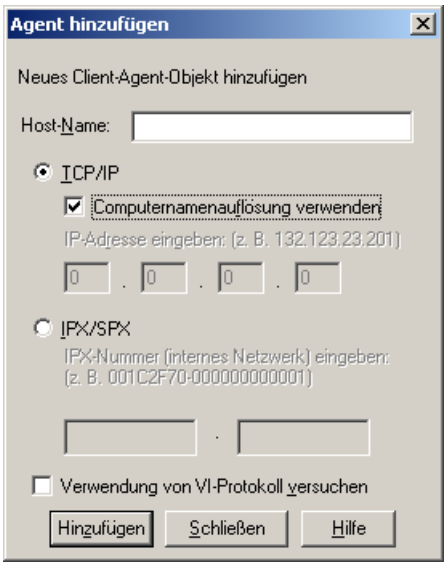
Manuelles Hinzufügen von Client-Agenten

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, und 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 Dialogfeld "Sicherheits- und Agenteninformationen" 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

Simulate 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 Vergleichjobs zulassen**, damit der Client Agent für Windows mehrere gleichzeitige Wiederherstellungs- oder Vergleichjobs akzeptiert.

Konfigurationsoptionen für die Ausführung von Sicherungen und Wiederherstellungen

Die Optionen für die Programmausführung des 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

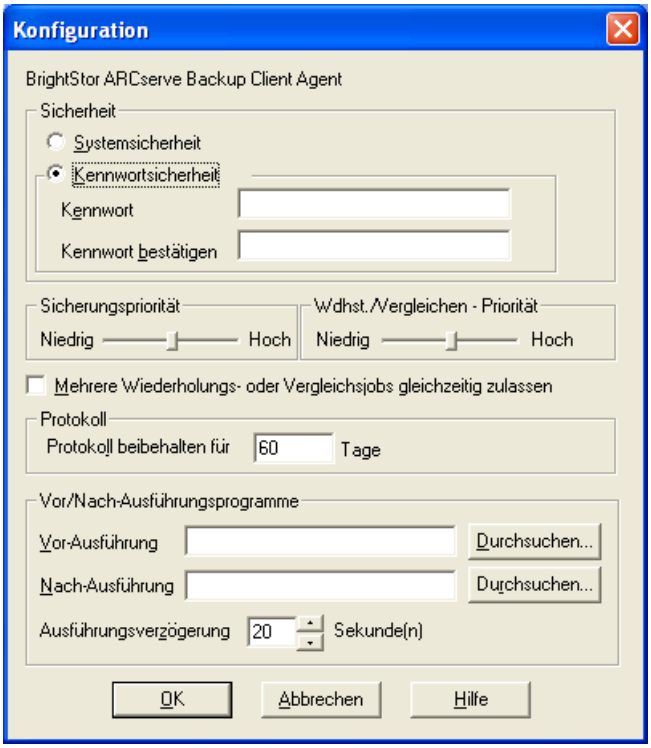
So konfigurieren Sie den CA ARCserve Backup Client Agent:

1. Öffnen Sie die Agent-Verwaltung. 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 für die verschiedenen Client-Agenten je nach Betriebssystem unterschiedlich sein.

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.

  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.

- **Protokoll**: Der Protokollordner ist im folgenden Verzeichnis gespeichert: c: :\Programme\CA\ARCserve Backup Client Agent for Windows. In diesem Ordner sind die Protokoll- und Indexdateien für jeden Job, der ausgeführt wird, 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 Stapelverarbeitungsprogramme (z. B. C:\WINAGENT\PRE.CMD) ein, die vor dem Sicherungs- bzw. Wiederherstellungsvorgang automatisch ausgeführt werden sollen.

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

  Ausführungsverzögerung: Geben Sie an, wie viele Sekunden der Client Agent vor oder nach der Ausführung des Stapelverarbeitungsjobs warten soll.

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 von Optionen zur Kennwortsicherheit

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

So richten Sie die Kennwortsicherheit für den Client-Agenten 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-Agenten zugewiesene Benutzername eingetragen sein.
3. Geben Sie das Kennwort für den Client-Agenten 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.

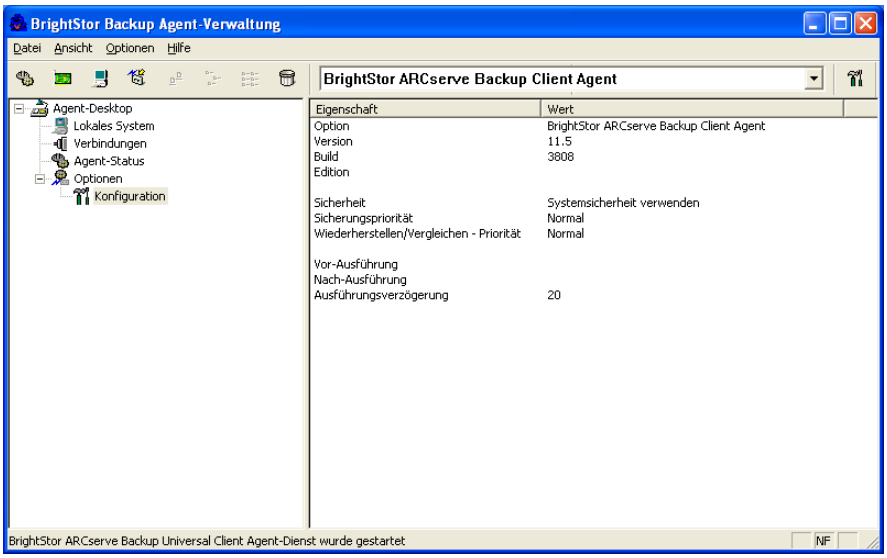
   Wenn Sie das zu verwendende Benutzerkonto angeben, muss außerdem möglicherweise zwischen zwei Konten mit dem gleichen Namen (z. B. Administrator) unterschieden werden. Geben Sie hierzu an, wo Windows das jeweilige Konto finden kann. Sie können den Speicherort des Client-Objekts bei der Angabe des Benutzernamens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

   ```
   NTDEV\Administrator

   ENGINEER\Administrator
   ```

Anzeigen der Konfigurationsauswahl

Sie können in der Backup Agent-Verwaltung die gewählten Konfigurationseinstellungen anzeigen, indem Sie den Knoten "Optionen" einblenden und anschließend "Konfiguration" auswählen, wie im folgenden Beispiel dargestellt:

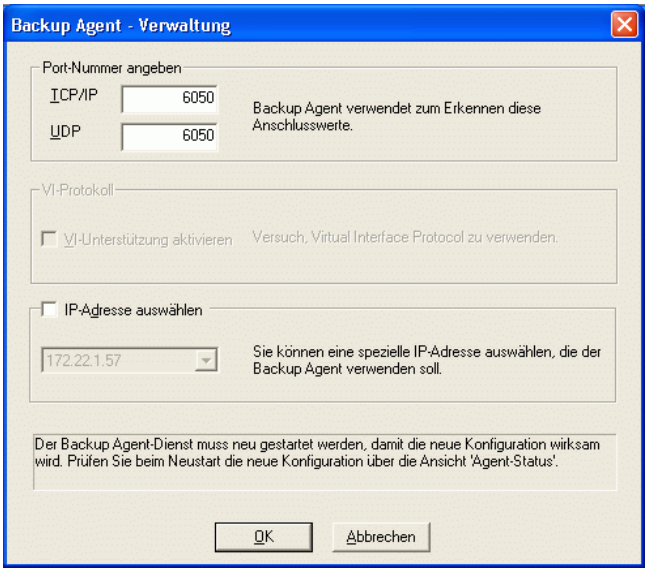


Konfigurieren der Windows-Netzwerkkommunikation

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

So konfigurieren Sie die 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-Agenten 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 mit 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 *Administrator-Handbuch*.

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:

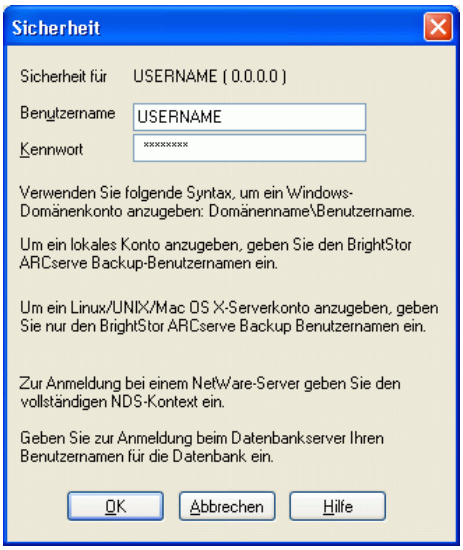
```
#Hostname IP-Adresse (optional) TCP-Port UDP-Port
#myhost   nnn.nnn.nnn.nnn       6050     6050
mymachine nnn.nnn.nnn.nn        7090     7085
```

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 geben Sie das Client Agent-Kennwort in CA ARCserve Backup ein:

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 Freigabenkennwörter 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 von Zugriffssteuerungslisten

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-Agenten 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

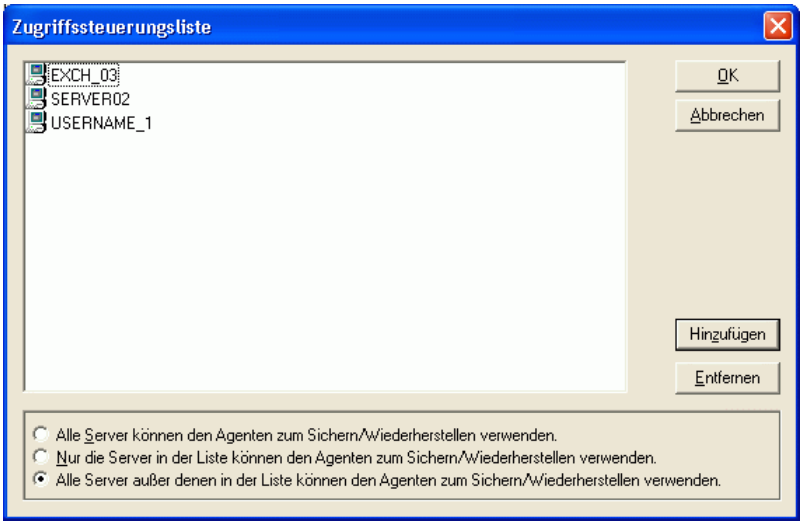
Eine Liste der Server, die zur Sicherung und Wiederherstellung auf den Client Agent-Rechner zugreifen dürfen.

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 ACL (Zugriffssteuerungsliste) und definieren die zugehörigen Typen:

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-Agenten hinzuzufügen. Die Zahl der Namen ist nicht beschränkt. Wenn Sie Client-Agenten aus der Liste entfernen möchten, klicken Sie für jeden einzelnen Client-Agenten auf "Entfernen".
5. Klicken Sie auf "OK", wenn Sie keine weiteren Client Agent-Namen hinzufügen bzw. entfernen möchten.

Virensuche aktivieren

eTrust Antivirus bietet zusätzlichen Schutz für wichtige Daten und schützt sie sogar während Sicherungs- oder Wiederherstellungsvorgängen 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 für Client Agenten für Windows:

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

   eTrust Antivirus 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 *Administrator-Handbuch*.

Konfiguration des NetWare Client Agent

In den folgenden Abschnitten wird die Konfiguration von CA ARCserve Backup NetWare-Client Agenten erläutert.

Hinweis: Auf dem Windows-Rechner muss der Novell-Client für Windows konfiguriert sein, damit NetWare-Server im Netzwerk installiert und ausgeführt werden können.

Konfigurationshinweise für NetWare

Beachten Sie bei der Konfiguration des Client-Agenten 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-Agenten 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-Agenten, 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-Agenten 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-Agenten 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-Agenten, 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-Agenten 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-Agenten 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-Agenten 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-Konfigurationsdatei 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 Stammverzeichnis 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-Agenten Konfigurationskonflikte bestehen, erhalten die Optionen, die über den Sicherungs-Manager festgelegt wurden, immer Vorrang gegenüber Optionen, die manuell in die Konfigurationsdatei "uag.cfg" eingetragen wurden.

Konfiguration der Port-Adresse

Die Standardadresse für TCP- und UDP-Ports 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            BABcmagt
HOME            /opt/CA/BABcmagt
TCP_PORT        7090
UDP_PORT        7085
```

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 Computer Associates Common Agent
- der Computer Associates UNIX Dateisystem-Agent (uagent)

Hinweis: Common Agent muss vor uagent installiert werden.

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

- Datei zur Verzeichnissteuerung

  In der Datei zur Verzeichnissteuerung, uag.cntl, 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, fs.cntl, werden die Dateisystemtypen auf einer bestimmten Workstation aufgeführt, die von Sicherungsvorgängen ausgeschlossen werden sollen. Tragen Sie jeden auszuschließenden Dateisystemtyp in der Datei fs.cntl 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

In der Common Agent-Konfigurationsdatei, agent.cfg, werden alle auf dem System installierten UNIX-, Linux- und Mac OS X-Agenten oder anwendungsspezifischen Backup-Agenten überwacht. Die Datei "agent.cfg" befindet sich auf jedem UNIX-, Linux- und Mac OS X-Rechner im CA Arcserve Backup-Common Agent-Installationsverzeichnis "/opt/CA/BABcmagt". In die Datei werden während des Setups die erforderlichen Informationen zum Client-Agenten eingetragen, wenn das Skript uagentsetup ausgeführt wird. Das Skript wird automatisch ausgeführt, nachdem uagent installiert wurde.

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 BABagntux	Name des Client-Agenten
VERSION nn.n	Release- und Versionsnummer des Client-Agenten
HOME /opt/CA/BABuagent	Standardmäßiges Stammverzeichnis des Client-Agenten
#ENV CA_ENV_DEBUG_LEVEL=4	Umgebungsvariable, die an den Client-Agenten übergeben wird

Dateiinhalt	Feldbeschreibung
#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-Agenten, BABuagent, 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 BABagntux. Der Name des Stammverzeichnisses des Client-Agenten wird durch die Variable HOME definiert.

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 des 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.

Option	Beschreibung
-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 1000 ms; Standardwert: 50 ms.
-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).

Option	Beschreibung
-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.

Option	Beschreibung
-I	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.
-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 *n*	Legt das Standard-Zeitlimit fest, gefolgt von einer variablen Zahl. Diese variable Zahl (*n*) 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 *Dateiname* -Postbackup *Dateiname* -Prerestore *Dateiname* -Postrestore *Dateiname*	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.
-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 *async*|*nonblocking*	Stellt die Socket-E/A auf asynchronen Nichtsperrmodus ein.
-s *bufsize*	Gibt die Größe des Socket-Puffers an. Möglich sind 4096 bis 65536. Der Standardwert ist systemabhängig.
-s *SocketMode*	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. **Hinweis:** 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 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:

Funktion	Plattform	Software-Voraussetzungen
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/BABcmagt.

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

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

2. Bereiten Sie die Konfigurationsdatei caagperf.cfg im Verzeichnis /opt/CA/BABcmagt 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.

Beispiel 1 für Konfigurationsdatei

Es folgt eine Beispieldatei für ein Betriebssystem mit 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 2 für Konfigurationsdatei

Es folgt eine Beispieldatei für ein 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
```

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.

Beispiel 3 für Konfigurationsdatei

Es folgt ein Beispiel für eine Konfigurationsdatei unter dem 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
```

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/BABcmagt 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:

- Eine Zugriffssteuerungsliste, die es bestimmten Benutzern ermöglicht oder verbietet, 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]
  NAMEBABagentux
  VERSIONnn.n.n
  HOME/opt/uagent
  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 dabei für ALLOW (Zulassen) und N für DENY (Verweigern).) Mit A:CAUSER1 wird 11 die Durchführung von Jobs ermöglicht, mit N:CAUSER2 wird 12 der Zugriff verweigert.

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

- Eine Zugriffssteuerungsliste, die festlegt, 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]
  NAMEBABagentux
  VERSIONnn.n.n
  HOME/opt/uagent
  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.

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

Gehen Sie folgendermaßen vor, um Voreinstellungen zum Starten für die AS/400 Enterprise Option zu konfigurieren:

1. Geben Sie in der Befehlszeile Folgendes ein:

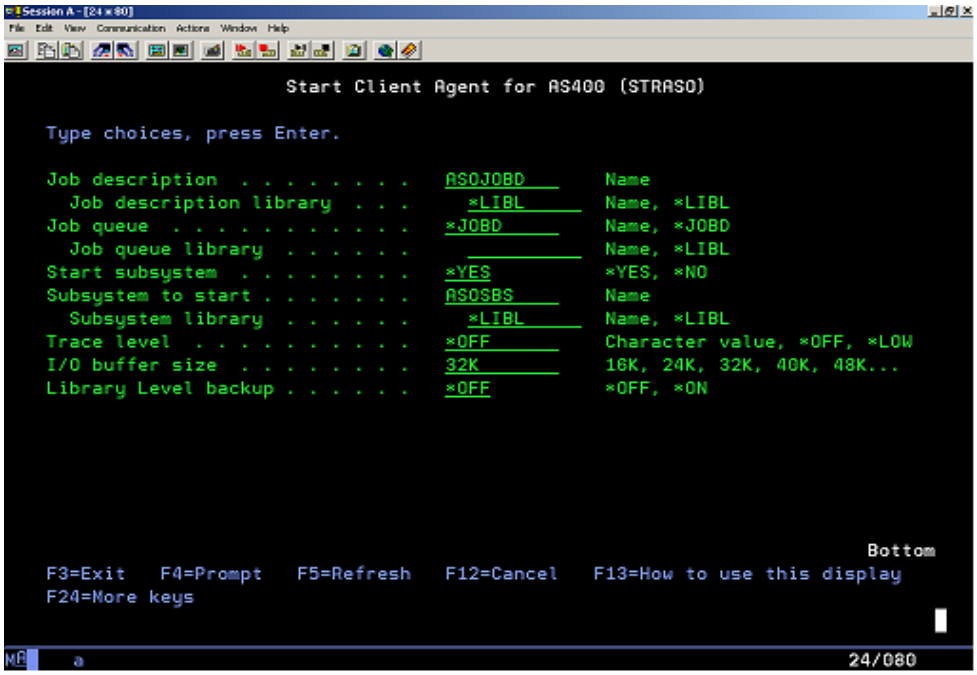
   ```
   straso
   ```

2. Drücken Sie F4.

   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".



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 SAVLIB-Befehl auf die Bibliotheksobjekte angewendet. Der SAVLIB-Befehl 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 SAVOBJ-Befehl 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

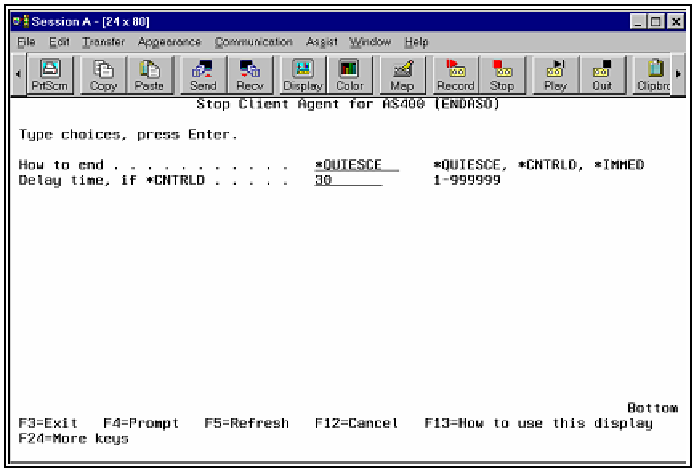
Gehen Sie folgendermaßen vor, um Voreinstellungen zum Stoppen für die AS/400 Enterprise Option zu konfigurieren:

1. Geben Sie in der Befehlszeile Folgendes ein:

   endaso

2. Drücken Sie F4. 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-Agenten 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 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.

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

In diesem Kapitel wird die Verwendung der Client-Agenten in einer standardmäßigen Sicherungsumgebung beschrieben. Folgende Themen werden behandelt:

- Beschreibung der Sicherungs- und Wiederherstellungsstatistik, welche die Client-Agenten abrufen und in Online-Protokolle schreiben können, sowie der Vorgehensweise für den Zugriff auf diese protokollierten Daten
- Einzelheiten zum Starten und Beenden der Client-Agenten
- Anweisungen für das Planen und Initiieren von Sicherungs- und Wiederherstellungsjobs sowie für die Statusüberprüfung von Online-Client-Agenten

Dieses Kapitel enthält folgende Themen:

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 Windows Client Agent

So zeigen Sie die Laufzeitstatistik für Windows Client Agent an:

1. Klicken Sie im Startmenü von Windows auf "Programme" (bzw. unter Windows XP auf "Alle Programme"), und wählen Sie "CA", "ARCserve Backup", "Backup Agent - Verwaltung".
2. Wählen Sie "Verbindungen". Das System zeigt die letzten zehn verarbeiteten 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 Verbindungsstatistik wird im Arbeitsspeicher gespeichert und geht folglich verloren, wenn Sie das Dialogfeld "Backup Agent - Verwaltung" und den Universal Agent-Dienst schließen. 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.

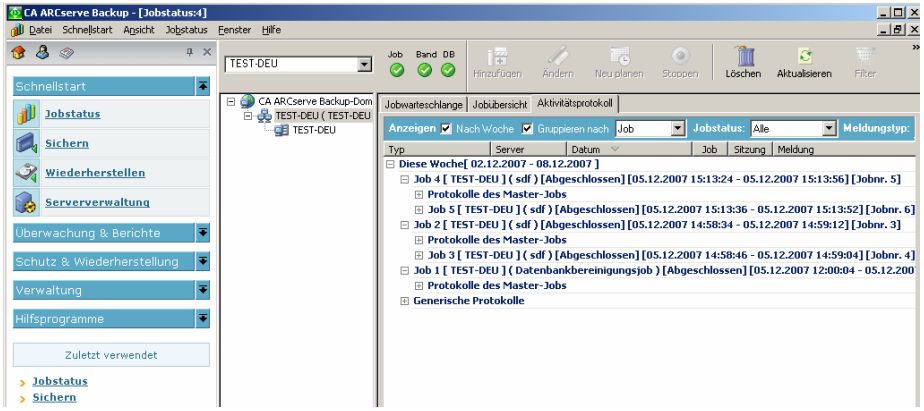
Aktivitätsprotokolle

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 aus anzeigen können.

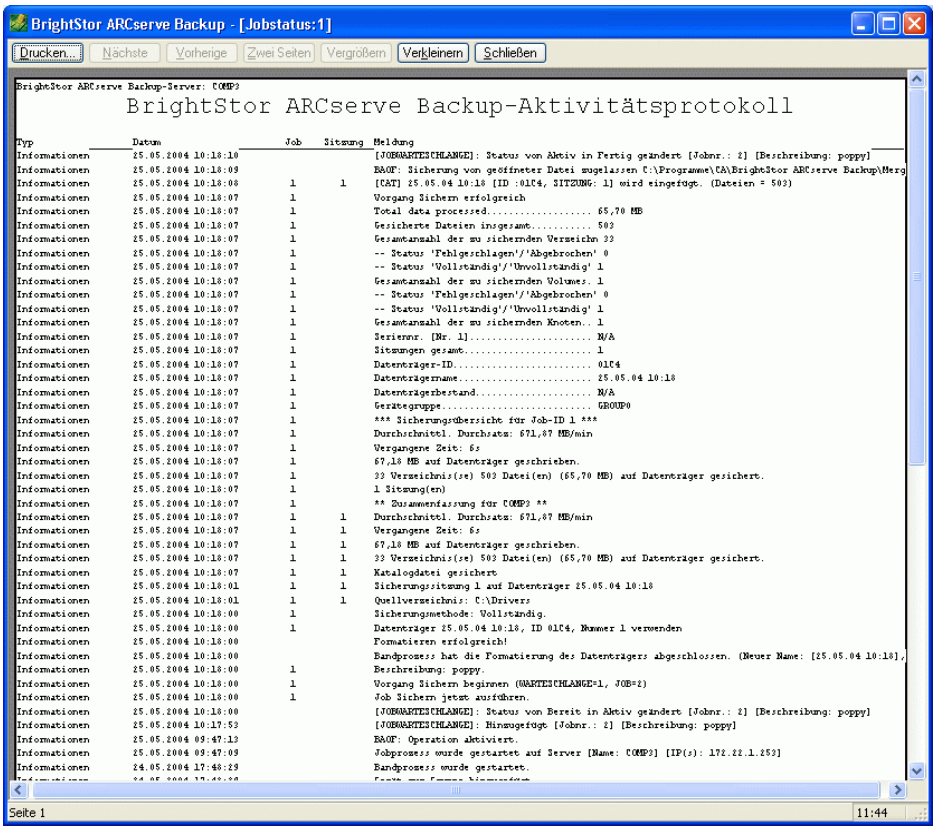
Anzeigen der Aktivitätsprotokolle auf einem Windows-Server

Gehen Sie folgendermaßen vor, um das Aktivitätsprotokoll auf einem CA ARCserve Backup-Windows-Server anzuzeigen:

1. Wählen Sie auf der Startseite von CA ARCserve Backup das Menü "Jobstatus" aus, um den Jobstatus-Manager zu öffnen.
2. Klicken Sie auf die Registerkarte "Aktivitätsprotokoll", um eine Liste mit Protokollen anzuzeigen (siehe folgendes Beispiel):



Die Ausgabe eines Client Agent-Aktivitätsprotokolls in einem Ausdruck oder einer Datei sieht folgendermaßen aus:



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/BABcmagt/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

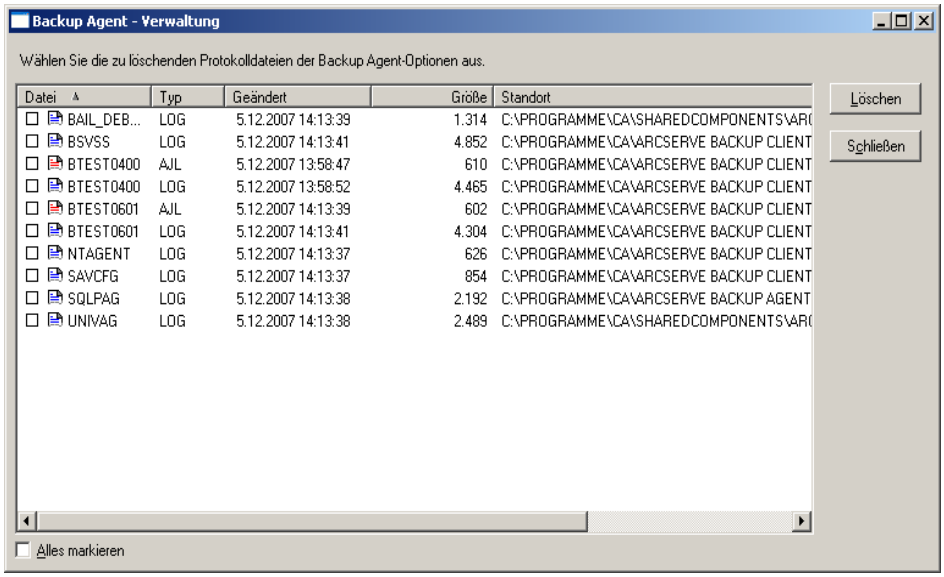
Sobald der Agent auf dem Server ausgeführt wird, erzeugt CA ARCserve Backup eine Aktivitätsprotokolldatei mit den Namen "aso$agent_<Knotenname>.log" und speichert diese im Protokollverzeichnis. Für jeden Job und jeden folgenden Start des Agenten wird eine neue Protokolldatei angelegt (zu erkennen an 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 Windows-Client-Agenten müssen Sie zum Löschen von Protokolldateien die Backup Agent-Verwaltung verwenden:



Sichern von Daten auf einem Windows-Netzwerkserver

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

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.

Starten und Stoppen von Windows Client Agent

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.

Gehen Sie folgendermaßen vor, um den Client Agent für Windows zu starten oder stoppen:

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 beim Systemstart automatisch 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 erzeugt. 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 Konsolenaufforderung 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:

```
#babuagent/uagentsetup
```

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

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

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

```
# uagent stop
```

Statuskommunikation 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 aktivierten Einträge in der Konfigurationsdatei, ob er weiter ausgeführt werden soll.

Beispielsweise wird mit dem Befehl "uagent stop" für einen UNIX-Client der Abschnitt für [BABagntux] als deaktiviert markiert. Ist "BABagntux" 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 [BABagntux] 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 aktivierten 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:

```
#babuagent/uagentsetup
```

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

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-Agenten für die AS/400 Enterprise Option

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

```
straso
```

Stoppen des Client-Agenten für die AS/400 Enterprise Option

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-Agenten für die OpenVMS Enterprise Option

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-Agenten für die OpenVMS Enterprise Option

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 Client Agent-Status

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

E

F

H

I

J

K

L

M

N

O