

CA ARCserve® Backup

Client Agents Guide

r12



This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of the Documentation for their own internal use, and may make one copy of the related software as reasonably required for back-up and disaster recovery purposes, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the provisions of the license for the Product are permitted to have access to such copies.

The right to print copies of the Documentation and to make a copy of the related software is limited to the period during which the applicable license for the Product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

EXCEPT AS OTHERWISE STATED IN THE APPLICABLE LICENSE AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH LOSS OR DAMAGE.

The use of any product referenced in the Documentation is governed by the end user's applicable license agreement.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Copyright © 2008 CA. All rights reserved.

CA Product References

This document references the following CA products:

- Advantage™ Ingres®
- BrightStor® ARCserve® Backup for Laptops and Desktops
- BrightStor® CA-1® Tape Management
- BrightStor® CA-Dynam®/B Backup for 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 for Novell Open Enterprise Server for Linux
- CA ARCserve® Backup Agent for Open Files on NetWare
- CA ARCserve® Backup Agent for Open Files on Windows
- CA ARCserve® Backup Client Agent for FreeBSD
- CA ARCserve® Backup Client Agent for Linux
- CA ARCserve® Backup Client Agent for Mainframe Linux
- CA ARCserve® Backup Client Agent for NetWare
- CA ARCserve® Backup Client Agent for UNIX
- CA ARCserve® Backup Client Agent for Windows
- CA ARCserve® Backup Enterprise Option for AS/400
- CA ARCserve® Backup Enterprise Option for Open VMS
- CA ARCserve® Backup for Windows
- CA ARCserve® Backup for Windows Agent for IBM Informix
- CA ARCserve® Backup for Windows Agent for Lotus Domino
- CA ARCserve® Backup for Windows Agent for Microsoft Data Protection Manager
- CA ARCserve® Backup for Windows Agent for Microsoft Exchange
- CA ARCserve® Backup for Windows Agent for Microsoft SharePoint

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

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at <http://ca.com/support>.

Contents

Chapter 1: Introducing the Client Agents 9

| | |
|--|----|
| Agent Features | 9 |
| Supported Client Systems | 10 |
| How Client Agents Work | 11 |
| Agent Features | 11 |
| Push Technology | 11 |
| Windows Computer Name Resolution | 12 |
| Security Features | 12 |
| Intelligent Client-to-Server Data Encryption | 12 |
| Integrated Virus Scanning and Repair | 12 |
| Auto Discovery of Client Agents | 13 |
| Multiple Network Interface Cards | 13 |
| Enhanced Network Connectivity | 13 |
| Real-Time Remote Browsing | 13 |
| Cyclic Redundancy Check Verification | 14 |
| Backup Verification Global Options | 14 |
| Access Control Lists | 14 |
| Extended Attributes for Linux and FreeBSD Client Agents | 15 |
| File System Specific Flags for Linux and FreeBSD Client Agents | 15 |
| Data Compression | 15 |
| Multistreaming | 15 |
| Multiplexing | 16 |
| Snapshot and Direct I/O Features for Solaris and HP-UX Systems | 16 |

Chapter 2: Installing the Client Agents 17

| | |
|---|----|
| System Requirements | 17 |
| Installation Considerations | 17 |
| Client Agent for Windows | 17 |
| Client Agent for NetWare | 18 |
| Enterprise Option for OpenVMS | 19 |
| Install the Client Agents | 19 |
| Common Agent Automatic Installation | 19 |
| Common Agent Configuration File for UNIX, Linux, and Mac OS X | 20 |
| Common Agent Components | 21 |
| Common Agent Port Numbers | 21 |
| Host Equivalence User Credentials | 23 |
| Access Control List Support for UNIX and Linux | 23 |

Chapter 3: Adding and Configuring the Client Agents 25

| | |
|---|----|
| Auto Discovery and Manual Addition of Client Agents | 25 |
| Auto Discover Client Agents | 25 |
| Manually Add Client Agents | 27 |
| Windows Client Agents Configuration | 28 |
| Windows-Related Configuration Notes | 28 |
| Security Configuration Options | 29 |
| Backup Priority and Restore/Compare Priority Options | 29 |
| Multiple Concurrent Restore or Compare | 29 |
| Backup and Restore Execution Configuration Options | 30 |
| Use the Backup Agent Admin to Set Windows Parameters | 30 |
| Configure Password Security Options | 33 |
| View Configuration Selections | 33 |
| Configure Windows Network Communication | 34 |
| Set a Workstation Password | 36 |
| Create Access Control Lists | 37 |
| Enable Virus Scanning | 38 |
| Customizable Local Options | 39 |
| NetWare Client Agent Configuration | 39 |
| NetWare-related Configuration Notes | 40 |
| Configure NetWare Network Communication | 40 |
| Back Up Novell Directory Services | 41 |
| UNIX, Linux, and Mac OS X Client Agent Configuration File | 41 |
| UNIX, Linux, and Mac OS X Configuration Considerations | 42 |
| Port Address Configuration | 43 |
| UNIX, Linux, and Mac OS X Client Agent Control Files | 43 |
| Common Agent Configuration File | 44 |
| Configurable Options | 47 |
| Snapshot and Direct I/O Support for UNIX | 50 |
| UNIX, Linux, and Mac OS X Access Control Lists | 56 |
| AS/400 Enterprise Option Configuration | 57 |
| Configure Start Preferences | 57 |
| Performance Configuration | 58 |
| Configure Stop Preferences | 59 |
| OpenVMS Enterprise Option Configuration | 59 |
| Configure Port Address | 60 |
| TCP/IP Stack Optimization | 60 |
| Trace Levels for the OpenVMS Enterprise Option | 60 |

Chapter 4: Using the Client Agents 61

| | |
|--------------------------|----|
| Runtime Statistics | 61 |
|--------------------------|----|

| | |
|--|----|
| View Runtime Statistics for the Windows Client Agent | 61 |
| View Runtime Statistics for NetWare Client Agents | 62 |
| Activity Logs | 62 |
| View Activity Logs on a Windows Server | 62 |
| View Activity Log on a NetWare Client Agent Machine | 63 |
| View Activity Log on a UNIX, Linux, or Mac OS X Client Agent Machine | 63 |
| Activity Logs on Computer Running the AS/400 Enterprise Option | 64 |
| Activity Logs on Computers Running the OpenVMS Enterprise Option | 64 |
| Delete Client Agent Log Files | 64 |
| Back Up Windows Network Server Data | 65 |
| Client Agent Start and Stop Procedures | 65 |
| Start and Stop the Windows Client Agent | 65 |
| NetWare Start and Stop Requirement | 66 |
| UNIX, Linux, and Mac OS X Client Agents Start and Stop Requirement | 67 |
| AS/400 Enterprise Option Start and Stop Requirement | 68 |
| OpenVMS Enterprise Option Start and Stop Requirement | 68 |

Index

Chapter 1: Introducing the Client Agents

CA ARCserve Backup is a comprehensive storage solution for applications, databases, distributed servers, and file systems. It provides backup and restore capabilities for databases, business-critical applications, and network clients. Among the compatible agents CA ARCserve Backup offers are a specific set of operating-system-based client agents.

The client agents are separate software packages installed on network computers to supply a network interface between the computer and CA ARCserve Backup. In addition to enabling connectivity, the client agents share data storage tasks with the backup servers in your network. You may need multiple client agents, depending on the number and variety of network machines that require regular data backup and restore functionality.

This guide provides information on installing, configuring, and adding client agents for all workstations and servers in your network storage environment.

This section contains the following topics:

[Agent Features](#) (see page 9)

[Supported Client Systems](#) (see page 10)

[How Client Agents Work](#) (see page 11)

[Agent Features](#) (see page 11)

Agent Features

CA ARCserve Backup client agents are designed for organizations that need to preserve network resources by offloading tasks onto centralized backup servers and media. Among other functions, the client agents serve to:

- Minimize the load on your communications network
- Increase the efficiency of your CA ARCserve Backup servers by offloading the preprocessing of archive data to the client machine
- Supply detailed file and directory information about the remote client to the CA ARCserve Backup server
- Communicate with the server and let you browse and select backup components
- Assist with monitoring the progress of backup jobs
- Maintain backup logs of the status of backup and restore activities

Client agents can also augment data protection for all client computers from a single CA ARCserve Backup server in the network.

Supported Client Systems

CA ARCserve Backup offers the following client agents:

- CA ARCserve Backup Client Agent for Windows. This client agent supports the following:
 - Windows Server 2008 (Core operating system only)
 - Windows Vista
 - Windows 2000
 - Windows XP
 - Windows Server 2003
 - Windows Small Business Server (SBS) operating on Windows 2000 and Windows 2003 servers
- CA ARCserve Backup Client Agent for NetWare
- CA ARCserve Backup Client Agent for UNIX. This client agent supports the following:
 - AIX
 - HP-UX
 - Solaris
 - Tru64
 - FreeBSD
- CA ARCserve Backup Client Agent for Linux. This client agent supports the following:
 - Red Hat
 - SuSE
 - Turbo
 - Debian
 - RedFlag
 - Miracle Linux
- CA ARCserve Backup Client Agent for Mainframe Linux. This client agent supports the following:
 - Red Hat Enterprise Server 3, 4 (31-bit and 64-bit) operating on zSeries and S/390
 - SLES 8 and 9 (31-bit and 64-bit) operating on zSeries and S/390
- CA ARCserve Backup Enterprise Option for AS/400
- CA ARCserve Backup Client Agent for Mac OS X

- CA ARCserve Backup Enterprise Option for OpenVMS

See the readme file on the installation CD for additional hardware and software requirements for installing and running client agents. For assistance, contact Technical Support at <http://ca.com/support>.

How Client Agents Work

CA ARCserve Backup and the client agents are designed to support data storage activities for companies and organizations with networked computers. The client agents allow you to back up and restore mission-critical data on your network. They help to:

- Facilitate backup of applications or file systems
- Facilitate monitoring of the backup progress
- Facilitate monitoring for backup log activities

With client agents installed on your network computers, a single CA ARCserve Backup server can perform data backup and restore operations on multiple computers and operating systems.

Agent Features

This section discusses the features and functionality offered by the various CA ARCserve Backup client agents.

Push Technology

All client agents use push technology, which automates the backup and restore process. The client agent contains separate internal client engines that help reduce the resource-intensive backup processes for the CA ARCserve Backup server. With this feature, the client agent filters and packages its archive data for reception by the server. This data preparation and transmission method provides real-time directory browsing, offloading system resources from the backup server, improves data transfer through use of packet technology, provides network security, and monitors backup and restore jobs.

When the client agents are installed and configured, you can use CA ARCserve Backup to receive data from each workstation in your data network. The client agent browses its targeted directories, prepares the data, and transmits the data across the packet network. The backup server then prepares the data for storage on the designated backup devices. These simultaneous processes between the client workstation and the backup server create an efficient, automated backup environment.

Windows Computer Name Resolution

Computer name resolution allows the local Windows computer to automatically detect the remote Windows machine's IP address when connecting for backup and restore operations.

Both the backup server and the network clients can use this feature. A local CA ARCserve Backup server can use computer name resolution to connect to and back up data on remote machines.

Security Features

The client agents for CA ARCserve Backup offer several security features, including client agent password security, system logon security, intelligent client-to-server data encryption, and integrated virus scanning with repair of infected files. The following sections offer more information about the CA ARCserve Backup data encryption and virus scanning features.

Intelligent Client-to-Server Data Encryption

With the intelligent client-to-server data encryption feature, you can encrypt data packets transported during a backup job with a session password to enhance network security. This feature utilizes AES 256 encryption and ensures that transported or archived data is secure and password protected, and ensures both the privacy of data transmitted over the network and the security of your backup media. Tapes cannot be misused or restored by users who do not have the encryption key.

When you choose this feature, your backup data is encrypted, including data packets that are transported between the client and the server, data that resides on the local server and data that has been moved to backup media.

Integrated Virus Scanning and Repair

CA ARCserve Backup provides the scanning and curing components of eTrust Antivirus, to protect your data.

Important! *CA ARCserve Backup provides only the scanning and curing components. It does not provide a full install of eTrust Antivirus. For the Windows client agent, a full install of eTrust Antivirus is required to receive automatic virus signature updates.*

When virus scanning is enabled, CA ARCserve Backup scans data for viruses during backup and copy operations. This feature ensures that your critical data is protected against all virus threats. The curing component, when selected during configuration, repairs infected files without the need for user intervention. This feature ensures that your critical data is protected against all virus threats.

For more information about eTrust Antivirus integration, see the *Administrator Guide*.

Auto Discovery of Client Agents

For CA ARCserve Backup installed on a Windows server, you can enable Auto Discovery of all computers in the network that are running client agents for Windows, UNIX, Linux, and Mac OS X. With Auto Discovery, CA ARCserve Backup can detect all Windows, UNIX, Linux, and Mac OS X computers running their respective client agents and automatically create the required list of computers you designate to receive regular backups.

Multiple Network Interface Cards

The Windows client agent supports multiple network interface cards (NICs). For computers with more than one network card, the client agent checks all enabled NICs to determine which cards are activated and being used for transmission.

Enhanced Network Connectivity

Machines operating the Windows client agent can recover from temporary network failures by using reconnection algorithms (in the case of severe network malfunctions, the Windows client agent may not recover). The CA ARCserve Backup framework further provides the ability to analyze network connectivity.

Real-Time Remote Browsing

This feature enables system administrators to view real-time file and directory information about the remote target machine.

Cyclic Redundancy Check Verification

The client agents generate Cyclic Redundancy Check (CRC) codes for all the files sent to the CA ARCserve Backup server. The CRC is used to verify the integrity of the files to be backed up.

Backup Verification Global Options

Client agents support the Scan Backup Media Contents and Compare Backup Media to Disk backup verification global options, which let you, verify that your data was backed up correctly.

If you select the Scan Backup Media Contents option, CA ARCserve Backup checks the header of each file on the backup media. If the header is readable, the data is assumed to be reliable. If the header is not readable, the Activity Log is updated with this information.

Note: If you select the Scan Backup Media Contents backup verification global option and enable the Calculate and Store CRC Value on Backup Media global option, in addition to checking the header of each file on the backup media, CA ARCserve Backup will perform CRC verification by recalculating the CRC value and comparing it with the one stored on media.

If you select the Compare Backup Media to Disk option, CA ARCserve Backup reads blocks of data from the media and compares the data, byte for byte, against the source files on the source machine, ensuring that all data on the media is exactly as it is on the disk. If a mismatch is found, the Activity Log is updated with this information.

For more information on backup verification options, see the online help.

Access Control Lists

Access control lists (ACLs) for Windows, UNIX, Linux, and Mac OS X client agents let you control which CA ARCserve Backup server accesses the workstation through the client agent. The initial configuration setting for these client agents enables all backup servers to back up and restore data through a Windows, UNIX, Linux, or Mac OS X client agent. By creating an ACL, you can restrict data backup and restore operations to a specific group of servers for the particular client agent.

Note: The Agent for FreeBSD in OS version 5.3 and 5.4, will backup and restore ACLs. Both default and access ACLs will be supported. This feature is not supported in FreeBSD version 4.11.

Extended Attributes for Linux and FreeBSD Client Agents

The Client Agent for Linux and FreeBSD versions 5.3 and 5.4 will support backup and restore Extended Attributes. FreeBSD version 4.11 will not support this feature.

File System Specific Flags for Linux and FreeBSD Client Agents

The Client Agent for Linux and FreeBSD agents support backup and restore of file system specific attributes, (called Flags in FreeBSD). FreeBSD versions 4.11, 5.3 and 5.4 will support this feature.

Data Compression

The Windows, UNIX, Linux, and Mac OS X client agents support the compression of data transmitted through the Transmission Control Protocol/Internet Protocol (TCP/IP) network. Compression is the reduction in size of data designed to save space and improve transmission time. When this option is configured, the client agent compresses all data packets before it begins transmission to the backup server.

Multistreaming

If you have more than one drive and more than one volume to be backed up, you can configure that system's client agent to use multistreaming. With multistreaming, you can take advantage of all available tape devices on the system. Multistreaming works by splitting a single backup job into multiple jobs that use all tape drives. As a result, multistreaming increases the overall backup throughput compared with single-stream, sequential processing.

On a Windows server, multistreaming is performed at the volume level for regular file systems (two volumes can run simultaneously on two separate devices). For preferred shared folders, remote database servers, and Windows NT, 2000, or XP agents, multistreaming is performed at the node level. On a UNIX or Linux server, you can configure the multistreaming level.

You can have only as many jobs running simultaneously as the number of local and remote devices or groups on the system. With multistreaming, one master job is created, which triggers slave jobs for as many volumes as necessary. When a job is finished on one device, another job is executed until there are no more jobs to run. For more information on multistreaming, see the *Administration Guide*.

Multiplexing

Multiplexing is a process in which data from multiple sources is written to the same media simultaneously. When a job that has multiple sources is submitted with the multiplexing option enabled, it is broken into child jobs—one for each source. These child jobs write data to the same media simultaneously. For more information on multiplexing, see the *Administration Guide*.

Snapshot and Direct I/O Features for Solaris and HP-UX Systems

You can enhance the performance of certain UNIX file systems (UFS) and Veritas file system (VxFS) volumes by using the Snapshot and Direct I/O (Direct Input/Output) features.

Note: These features are available at the disk volume level only, and only for Solaris and HP-UX systems.

With the Snapshot feature, the client agent allows you to back up your data faster and more efficiently. The CA ARCserve Backup client agent takes a snapshot of a UNIX volume, mounts the snapshot to a temporary directory created in the root volume, and then generates the backup. After the snapshot backup has completed, the file system agent dismounts from the temporary directory and deletes the snapshot. Some network machines can create and mount a snapshot of their backup data to an alternate mount point. Backup applications can then access and back up the data using the alternate mount point.

With the Direct I/O feature, the UNIX client agent remounts the volume using the Direct I/O Mount option. This feature may improve performance during file input/output (I/O) operations and can eliminate double buffering requirements.

Chapter 2: Installing the Client Agents

To perform a backup or restore job, you must install and start the appropriate CA ARCserve Backup client agent software. The client agent provides communication between a workstation and the CA ARCserve Backup server. This chapter describes how to install client agents.

This section contains the following topics:

[System Requirements](#) (see page 17)

[Installation Considerations](#) (see page 17)

[Install the Client Agents](#) (see page 19)

[Common Agent Automatic Installation](#) (see page 19)

System Requirements

See the readme file on the installation CD for hardware and software requirements for installing and running client agents. For assistance, contact Technical Support at <http://ca.com/support>.

Installation Considerations

The following sections include information you should review before installing the client agents.

Client Agent for Windows

Before installing the client agent for Windows, review the following considerations.

- Before you can run the client agent for Windows, your computer must be configured to communicate using one or more of the following network protocols:
 - Transmission Control Protocol/Internet Protocol (TCP/IP)
 - Windows Socket (WinSock) Direct

- There are some limitations when performing a remote setup during a client agent for Windows installation. The limitations are as follows:
 - **Windows XP**—You cannot perform a remote installation on a machine running Windows XP if the computer has been configured with the feature Force Network Logons Using Local Accounts to Authenticate as Guest.
 - **Windows XP (64-bit edition)**—Remote installation is not supported.
 - **Windows 2003 (64-bit edition)**—Remote installation is not supported.

If you encounter any of these situations, you can install the client agent for Windows directly from the CA ARCserve Backup installation CD.

Client Agent for NetWare

Before installing the client agent for NetWare, review the following considerations.

- The client agent for NetWare can be installed on NetWare servers only. Also, to perform a NetWare installation, your local machine must be equipped with the Novell client for Windows.
- The NetWare server must be configured to communicate using the following network protocol:
 - TCP/IP
- You must have supervisor rights on the eDirectory tree of the NetWare computer on which you are installing this client agent. For details, see your Novell NetWare documentation.
- For optimum performance, use the latest NetWare C library (CLIB) and Systems Management Server (SMS) modules.
- The NetWare Loadable Modules (NLMs) are available from Novell.

Enterprise Option for OpenVMS

Before installing the enterprise option for OpenVMS, review the following considerations.

- A computer running the supported Alpha and VAX operating systems can use either TCP or User Data Protocol (UDP) with any of the following communications software:
 - Compaq UCX 4.2 eco 3 (on Alpha)
 - Compaq UCX 3.3 eco 13 (on VAX)
 - Compaq TCP/IP Versions 5.0 through 5.3
 - Process Software Multinet Version 4.1B (with patches) through Version 4.4
 - Process Software TCPWARE Versions 5.3 and 5.4

Important! *If necessary, you can install two or more of these communications packages on the same computer; however, you can run only one package at a time. Do not run two or more of these communications packages simultaneously on the same computer.*

Note: If you change OpenVMS TCP/IP stacks at any time, you must reinstall the OpenVMS Enterprise Option.

- You should back up your OpenVMS system disk before installing the OpenVMS Enterprise Option.
- Ensure that you have at least 10 blocks of free space for setup file.

Install the Client Agents

There are two CA ARCserve Backup installation CDs. To install a windows client agent use the CA ARCserve Backup r12 for Windows CD. To install a cross-platform agent, use the CA ARCserve Backup r12 Agent CD.

Common Agent Automatic Installation

When you install the client agent for UNIX, Linux, or Mac OS X, the CA ARCserve Backup Common Agent is automatically installed. The following sections include information on the Common Agent.

Common Agent Configuration File for UNIX, Linux, and Mac OS X

The Common Agent (caagentd binary) is a standard component for all UNIX, Linux, and Mac OS X client agents that are installed automatically during the first installation of any UNIX, Linux, or Mac OS X client agent.

The Common Agent resides in the /opt/CA/BABcmagt directory. The Common Agent keeps track of the client agents that are installed on the system in a configuration file named agent.cfg, which also resides in the /opt/CA/BABcmagt directory. During the installation of a new client agent, the agent.cfg file is updated with the new client agent's information. You will seldom need to modify this configuration file. Manual modification of this file is required only to enable some debugging messages or to change the default TCP/IP port on which the Common Agent runs.

A sample agent.cfg file with a client agent installed is shown next:

```
[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 Components

The Common Agent runs at all times as a daemon, listening for requests on behalf of all the UNIX, Linux, and Mac OS X client agents that are installed on the system. During each client agent's installation, the BROWSER, AGENT, MERGE, and VERIFY components are registered with the Common Agent in a separate section.

Not all client agents may have all of these components. For example, in the following sample configuration file, you can see the BROWSER component `cabr`, the AGENT component `uagentd`, and the MERGE and VERIFY component `umrgd` in the section for the UNIX, Linux, or Mac OS X client agent. Similarly, other client agents use other BROWSER and AGENT components.

```
[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
```

Common Agent Port Numbers

By default, the Common Agent uses port number 6051 for both TCP and user datagram protocol (UDP). To change the default port, you must modify the `BABcmagt` section of the `agent.cfg` file with the new port numbers, and then restart the Common Agent by issuing the `caagent stop` command, followed by the `caagent start` command. Do not use the `caagent update` command after modifying port numbers.

Note: Under normal conditions, this method should **not be used** to start or stop the Common Agent. Instead, you should run the Start and Stop scripts of the individual UNIX, Linux, and Mac OS X client agents installed on the system.

The following sample shows the configuration file before and after the script changes are made.

Before the change:

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

After the change:

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

The port changes take effect only after you restart the Common Agent. If you configure the Common Agent to run on a port other than the default port, you should also configure the CA ARCserve Backup server to access this Common Agent. You can do this by making an entry for the client agent in the port.cfg file. This file is in the config subdirectory under the home directory—\$BAB_HOME/config/port.cfg—on the backup server.

By default, the Common Agent uses another UDP port, 0xA234 (41524), to receive CA ARCserve Backup requests for the Auto Discovery of UNIX, Linux, and Mac OS X client agents. This port is not configurable.

Host Equivalence User Credentials

When the Common Agent checks user credentials, it gives preference to host equivalence settings of the system. A UNIX, Linux, or Mac OS X system can be set up to grant access for specific users on specific hosts without requiring the user to provide credentials. You can grant this access by adding the specific user IDs to the `/etc/hosts.equiv` or `.rhosts` file. By default, the Common Agent follows these rules, then checks the user's password for authorization. To disable host equivalence checking, define the `NO_HOSTS_EQUIV=1` environment variable in the `agent.cfg` file, as shown in the following example:

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

You can place the Common Agent in No Password mode or Single User mode with a set of access control lists if necessary. For more information about ACLs, see UNIX, Linux, and Mac OS X Access Control Lists in the chapter "Adding and Configuring the Client Agents."

Access Control List Support for UNIX and Linux

CA ARCserve Backup Client Agent for UNIX, CA ARCserve Backup Client Agent for Linux, and CA ARCserve Backup Client Agent for Mainframe Linux back up and restore the access control list (ACL) for files and directories on a Linux system that have been backed up using the Linux client agent. The extended attributes for Linux are also backed up. ACL gives administrators finer control over files and directory access. The Linux client agent can read and set the ACL for each file and directory.

Verify ACL Libraries

To enable this feature, certain ACL libraries are required. To check that you have the required ACL libraries installed, run the following command:

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

If the `libacl-devel-*` or `libacl-*` packages are not listed, install them by using the following procedure.

1. Copy the ACL library packages from the CD image, or download them from the internet to your Linux system:

```
-libacl package (such as libacl-2.2.3-1.rpm)
-libacl-devel package (such as libacl-devel-2.2.3-1.rpm)
```

2. To install the packages, run the following commands:

```
rpm -ivh <libacl-package-name>  
rpm -ivh <libacl-devel-package-name>
```

as in this example:

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

This step installs the libacl.so library into your Linux system.

If the Linux client agent is running on a 32-bit Linux system, ACL support is now enabled. If the Linux client agent is running on a 64-bit Linux system, you must ensure that the libacl.so library is a 32-bit version. You can check the version and create a link to a 32-bit library if necessary.

Verify the Linux ACL Library Version

To check the version, go to the directory where libacl.so is installed, and follow these steps:

1. Run `ls -l . /libacl.so` to display the libacl.so linking target library file.
2. Run `file libacl.so<-linking-target-library>` using the library file name.

The result will show whether libacl.so points to a 32-bit or 64-bit version.

Create Link to 32-bit Linux ACL Library

If libacl.so points to a 64-bit library, you must create a link from the 32-bit library to libacl.so. The following example shows how to create the link on a 64-bit Mainframe Linux platform:

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

Use the appropriate link command for your 64-bit Linux system.

Chapter 3: Adding and Configuring the Client Agents

After installing CA ARCserve Backup and its various client agents, you must add and configure each client agent machine in your network to the backup server. This chapter discusses the procedures for adding and configuring client agents.

This section contains the following topics:

[Auto Discovery and Manual Addition of Client Agents](#) (see page 25)

[Windows Client Agents Configuration](#) (see page 28)

[NetWare Client Agent Configuration](#) (see page 39)

[UNIX, Linux, and Mac OS X Client Agent Configuration File](#) (see page 41)

[AS/400 Enterprise Option Configuration](#) (see page 57)

[OpenVMS Enterprise Option Configuration](#) (see page 59)

Auto Discovery and Manual Addition of Client Agents

If you have CA ARCserve Backup installed on a Windows server, you can automatically discover client agents in your network using Auto Discovery or you can add client agents manually. The following sections include information on each of these methods.

Auto Discover Client Agents

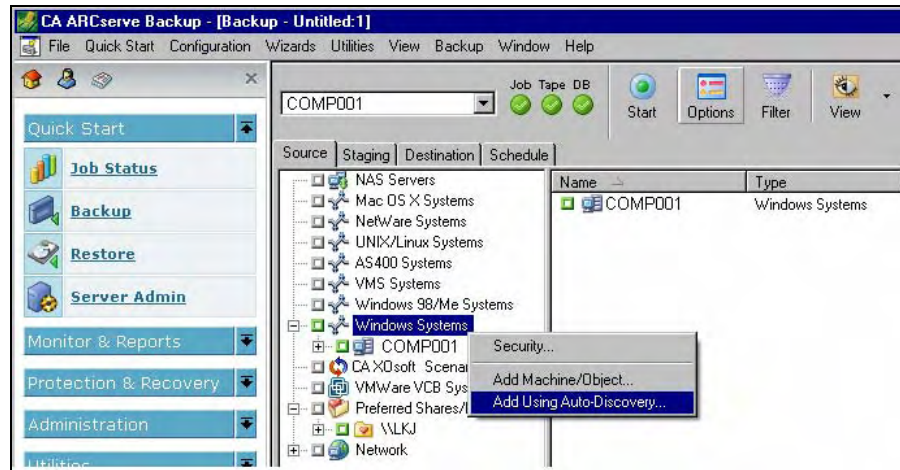
If you have CA ARCserve Backup installed on a Windows server that uses the Windows manager interface, you can use Auto Discovery to automatically detect Windows, UNIX, Linux, and Mac OS X client agents installed and running on your network. To use Auto Discovery to create your backup and restore list, ensure that the Backup Engine is running. The system default is to automatically start the Backup Engine when CA ARCserve Backup is first started; however, you may need to stop the engine during certain operations.

To auto discover client agents

1. Open the Backup Manager and click the Source tab.

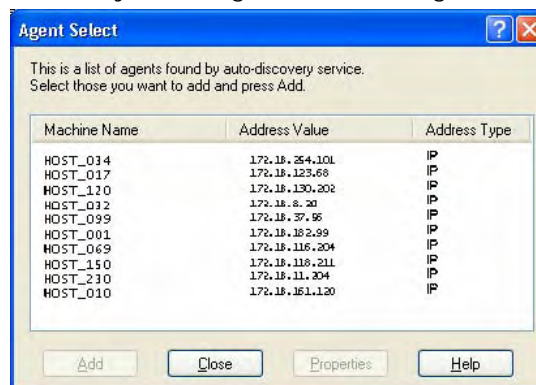
Note: If the Backup Engine is not running, you will be prompted to start it during this procedure.

2. On the Source tab, select the appropriate client agent object, such as Windows Systems.



3. Right click and choose Add Using Auto-Discovery.

CA ARCserve Backup displays a list of all the machines it finds during Auto Discovery in the Agent Select dialog.



4. From the list, select the client agents you want to add to the backup list.

Note: Hold the Ctrl key down to select multiple agents.

5. Click Add.
6. Click Close.

Each client agent you have selected now shows as a member of the corresponding operating system in the Backup Manager.

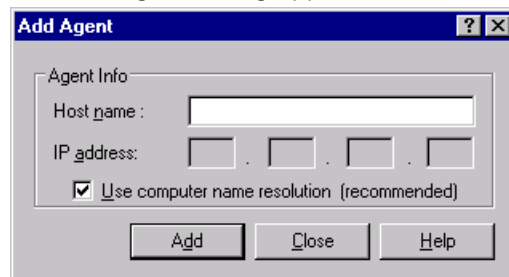
Manually Add Client Agents

If Auto Discovery does not detect all client agents in your network for some reason or if you want to add a particular client agent, you can manually add a client agent to a Windows server or NetWare server using the Windows manager interface. To manually add a client agent, you must add each client agent machine to the Backup Manager.

To manually add client agents

1. Open the Backup Manager and click the Source tab.
2. Right-click the appropriate client agent object, such as Windows Systems.
3. Select Add Machine/Object.

The Add Agent dialog appears.



4. Enter the name of the computer in the Host Name field.

Note: If you are adding a NetWare Client Agent, you MUST use the Novell server name as the host name.

5. Select the protocol you want to use to connect to the computer:
 - **TCP/IP**—Select TCP/IP and, if you are adding a Windows client agent, select Use Computer Name Resolution. Computer name resolution lets the local Windows computer automatically detect the remote Windows machine's IP address when connecting for backup and restore operations. This is the recommended method and works even if you do not know the computer's IP address.

Note: If the target Windows computer has a dynamic IP address, using computer name resolution is preferable.

If you are not adding a Windows client agent, if computer name resolution fails because of various DNS server or network configuration issues, or the target computer has multiple IP addresses and you want to be certain that a specific address is used, ensure that Use Computer Name Resolution is not selected and enter an IP address.

6. Click Add.

The client agent is added to the server.

Windows Client Agents Configuration

The following sections discuss the Windows client agent configuration options.

Windows-Related Configuration Notes

General information pertaining to the configuration of the Windows client agent includes:

- **Restoring System State**—The System State supports the Restore to Original Location option.
Note: The System State also supports restoring to an alternate location, but it will not recreate an operational system since the files are placed in default directories created by the agent at the time of restore.
- **Shares Support**—When the use agent option is selected, the client agent backs up shares selected from the Preferred Shares/Machines object in the Backup Manager by converting the share name to the real path.
Note: On Windows platforms, the client agent does not restore shares or support shares as a destination except for administrative shares.
- **Restoration of the System Hive**—The KeysNotToRestore feature is designed to protect sensitive system registry keys during a regular restore of the client agent system hive. However, this feature is unavailable when you use the Client Agent Registry session to restore individual system keys.

Security Configuration Options

The Client Agent for Windows security options are defined on the Configuration dialog. Select one of the following types of security:

System Security

Lets you use Windows security to perform backup, compare, and restore operations. The client agent impersonates the active network user; that is, the client agent uses the user name and password to log on. This ID and password should identify a valid user in the local user database or in the domain database if the workstation is a member of a domain.

Password Security

Lets you set individual passwords for security. This setting enables the client agent to run under the local system account. Password Security is disabled by default.

Note: If password security is selected, and DSA-based database agents (for example, Sybase, Informix, and so on) are installed on the machine, whole node backup is not supported. To back up databases only, you must change the security information in the Security and Agent Information dialog, to the system security before submitting the job.

Backup Priority and Restore/Compare Priority Options

The Client Agent for Windows process priority is defined on the Configuration dialog. Select one of the following settings for Backup Priority and Restore/Compare Priority:

High

Foreground processing performs client agent functions before other processes.

Normal

Standard processing performs client agent functions without special status.

Low

Standard processing performs client agent functions when other processes are idle.

Multiple Concurrent Restore or Compare

The Client Agent for Windows simultaneous restore and compare is enabled on the Configuration dialog. Enable the Allow multiple simultaneous restore or compare jobs check box on the Configuration dialog if you want the Windows client agent to accept multiple concurrent restore or compare jobs.

Backup and Restore Execution Configuration Options

The Client Agent for Windows program execution options are defined on the Configuration dialog. Select the pre-execution programs, post-execution programs, and define the execution delay.

Pre-execution

Enter or select the name of any batch programs (for example, C:\WINAGENT\PRE.COMD) that you want to automatically execute before the backup or restore operation.

Post-execution

Enter or select the name of any batch programs (for example, C:\WINAGENT\POST.COMD) that you want to automatically execute after the backup or restore operation.

Execution Delay

Select the number of seconds that you want the client agent to wait before or after executing the batch job.

Use the Backup Agent Admin to Set Windows Parameters

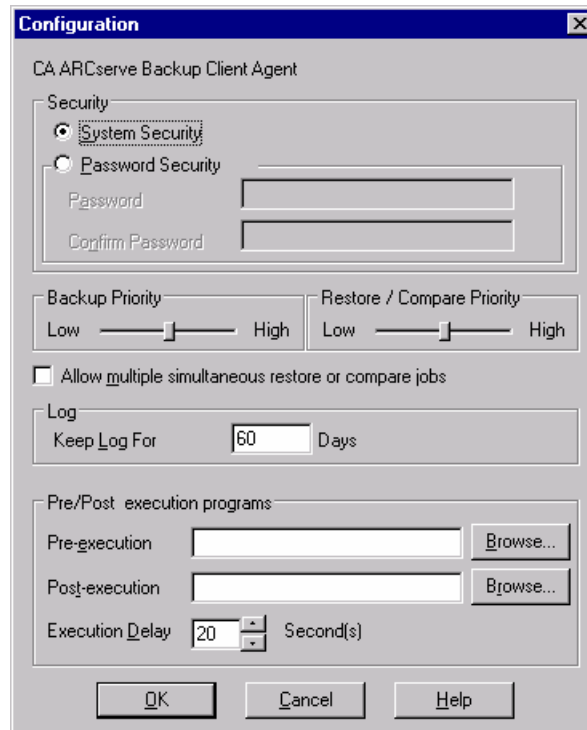
To configure the CA ARCserve Backup Client Agent

1. Access the Agent Admin. To access the Agent Admin, click Start, Programs or All Programs, CA, ARCserve Backup Agents, Backup Agent Admin.

Note: The window contents may differ slightly for each client agent, depending on the specific operating system in use.

2. From the Agent Admin, select the Options tab.

The Configuration dialog opens.



You can define the following settings using the Configuration dialog:

- **Security Type Specification**--Select one of the following types of security:
 - System Security**--Select this Security option to use Windows security to perform backup, compare, and restore operations. The client agent impersonates the active network user; that is, the client agent uses the user name and password to log on. This ID and password should identify a valid user in the local user database or in the domain database if the workstation is a member of a domain.
 - Password Security**--Select this Security option to set an individual password for security. This setting enables the client agent to run under the local system account. Password Security is disabled by default.

- **Setting Process Priority**--These settings determine the priority given to the processes needed for the backup, restore, or compare operations. Select one of the following settings for Backup Priority and Restore/Compare Priority:

High--Foreground processing performs client agent functions before other processes.

Normal--Standard processing performs client agent functions without special status.

Low--Standard processing performs client agent functions when other processes are idle.

- **Allow multiple simultaneous restore or compare jobs**--Enable this if you want the Windows client agent to accept multiple concurrent restore or compare jobs.

Note: By default, this option is disabled to ensure that new backup or restore jobs of the same data set are not accidentally launched during a running restore job. If this does occur, the agent denies the new job's request and reports that the client agent is busy to the CA ARCserve Backup server.

- **Log**--The Log folder is stored in the following directory: c:\Program Files\CA\ARCserve Backup Client Agent for Windows. The log files and index files for every job that runs are stored in this folder.

Keep Log For--Specifies the number of days (the default is 60 days) to keep the agent log. After the specified number of days has elapsed the log will be deleted when the next agent backup, restore, or compare job runs.

- **Pre-Execution and Post-Execution Programs**--Select the following execution options:

Pre-execution--Enter or select the name of any batch programs (for example, C:\WINAGENT\PRE.CMD) that you want to automatically execute before the backup operation.

Post-execution--Enter or select the name of any batch programs (for example, C:\WINAGENT\PRE.CMD) that you want to automatically execute after the backup operation.

Execution Delay--Select the amount of seconds that you want the client agent to wait before or after the execution of the batch job.

3. Click OK to save your changes and exit the dialog.

Note: To change your configuration later, you must return to the Configuration dialog.

Configure Password Security Options

The client agent service uses the node (machine) user name and assigned password to log on to the CA ARCserve Backup Backup network.

To set password security for the client agent

1. Start the Backup Manager, and then right-click the machine name. A pop-up menu appears.
2. Choose Security from the pop-up menu to open the Security dialog. The User Name field should already contain the client agent's assigned user name.
3. Enter the password for the client agent.

Note: The user name and password should identify a valid user in the local machine's database or in the domain database, if the workstation is a member of a domain.

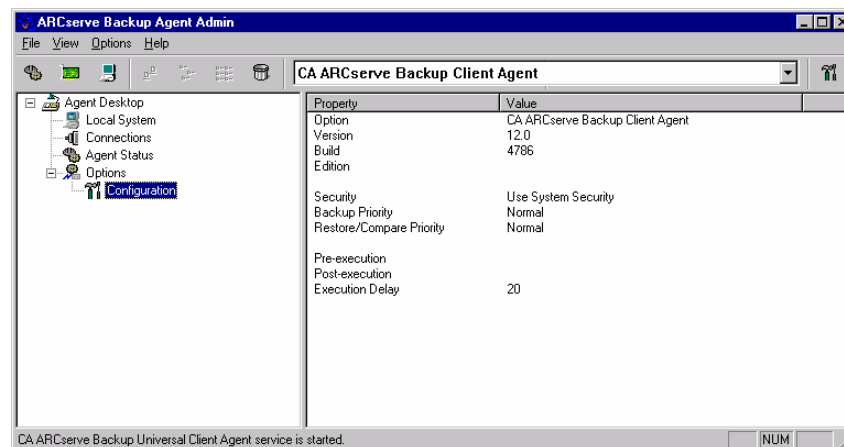
Also, when you specify the account to use, it may be necessary to distinguish between two accounts that use the same name (such as Administrator) by indicating where Windows can find each account. You can identify the client object's location by using tree name formats when identifying the user name. For example, for a domain named NTDEV containing a workstation named ENGINEER, the respective administrators are:

NTDEV\Administrator

ENGINEER\Administrator

View Configuration Selections

To view your configuration selections, open the Backup Agent Admin, expand Options, and then select Configuration, as shown in the following example:



Configure Windows Network Communication

CA ARCserve Backup client agent services are shared across all configured client agents. By default, Windows client agents use TCP/UDP port 6050. You can change this behavior by using the Network Configuration menu in the Backup Agent Admin.

To configure network communication

1. Open the Backup Agent Admin.
2. From the Options menu, select Network Configuration:

The screenshot shows the 'Backup Agent Admin' dialog box with the 'Network Configuration' menu item selected. The dialog is titled 'Backup Agent Admin' and contains the following sections:

- Specify Port Number:** A section with the text 'The Backup Agent will listen using these port values.' It contains two rows: 'TCP/IP' with a text box containing '6050' and a 'Reset' button; and 'UDP' with a text box containing '6050' and a 'Reset' button.
- VI protocol:** A section with a checkbox labeled 'Enable VI support' and the text 'Attempt to use Virtual Interface Protocol.' The checkbox is currently unchecked.
- Select IP Address:** A section with a checkbox labeled 'Select IP Address' and a dropdown menu showing '155.35.76.239'. The text next to it says 'Allows you to select a specific IP Address to be used by Backup Agent.' The checkbox is currently unchecked.
- Footer:** A text box containing the message: 'The Backup Agent service must be restarted for the new configuration to take effect. Upon restart, please verify the new configuration in the Agent Status view.' Below this are three buttons: 'OK', 'Cancel', and 'Help'.

- Using this dialog, set the following network parameters for the client agent:

Specify Port Number

Accept the defaults or enter the port values you want CA ARCserve Backup to use. If you want to use the original default port, click the Reset button. The updated port information will be saved in the local PortsConfig.cfg file located in \Program Files\CA\SharedComponents\ARCserve Backup.

Note: Updated port information must be registered with the CA ARCserve Backup server component. To do this, you must modify the remote server PortsConfig.cfg file. For more information on port configuration, see the *Administration Guide*.

Select IP Address

The Windows client agent supports the use of multiple network interface cards (NICs). For computers with more than one network card, the agent checks all enabled NICs in the machine. You can manually override this selection by choosing the IP address of the NIC that you want to dedicate for backup purposes. When you define this configuration, the client agent will listen using only this interface card. All other NICs are ignored and you will not be able to use their IP addresses to connect to the client agent.

Any updated information also needs to be modified in the Windows CAPortConfig.cfg file and copied to the CA ARCserve Backup home directory. The following example shows a CAPortConfig.cfg file:

```
#Hostname IP address (optional) TCP port UDP port
#myhost nnn.nnn.nnn.nnn 6050 6050
mymachine nnn.nnn.nnn.nnn 7090 7085
```

Set a Workstation Password

If you selected password security when configuring the Windows client agent from the Backup Agent Admin, you must specify the same password in CA ARCserve Backup.

To specify the client agent password in CA ARCserve Backup

1. From the Backup Manager, right-click the name of the client agent.
2. Choose Security from the pop-up menu.



3. Enter the local Windows user account name or enter the Windows domain account using the tree format.
4. Enter the password and click OK.

Note: If you use a client agent to perform remote client backups and restores, the password you set for the client agent overrides any shared password set for the workstation. If you do not use client agent software for your backup jobs, you must specify share-level passwords on the Backup Manager window. Make sure that the password on the Backup Manager and the share-level password are the same.

Create Access Control Lists

You can limit the servers authorized to perform backups on a Windows client agent object by generating an access control list (ACL). This feature is defined through the Backup Manager and the Backup Agent Admin. By creating an access control list and defining its type, you can restrict data backup and restore to a specific group of CA ARCserve Backup servers for the particular client agent. The ACL type can be:

No ACL used

No list is specified; this is the default.

Include list

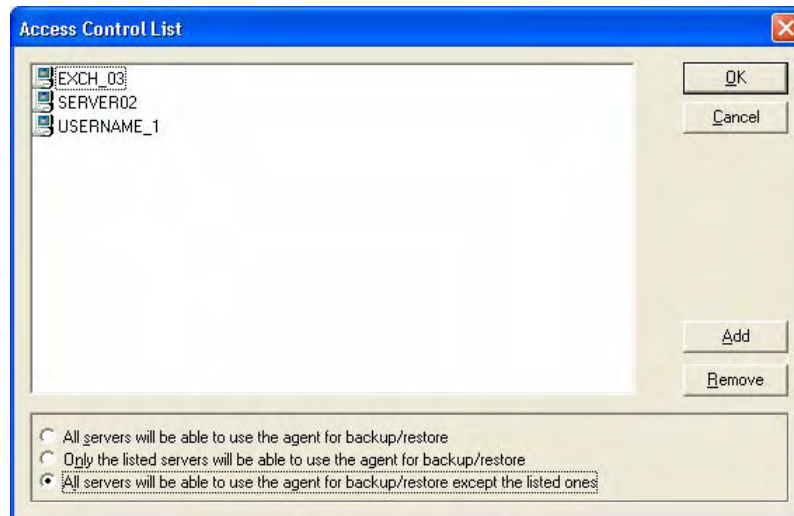
A list of servers allowed to access the client agent machine for backup and restore options.

Exclude list

A list of servers that are not allowed to access the client agent machine for backup and restore options. All other servers in the network can access the client object.

To create an ACL and define types

1. Open the Backup Agent Admin.
2. From the Options menu, select Access Control List.



3. When the Access Control List dialog appears, the default is to **not** use ACL and the setting **All servers will be able to use the agent for backup/restore** is selected. To create an ACL, select **one** of the following choices:
 - Only the listed servers will be able to use the agent for backup/restore
 - All servers will be able to use the agent for backup/restore except the listed ones
4. Click Add to add client agent names to the access control list, including as many names as you need for the ACL. If you want to remove client agents from the list, click Remove for each client agent being removed.
5. Click OK when you are finished adding or removing client agent names.

Enable Virus Scanning

eTrust Antivirus software offers extra protection for your critical data, securing it from virus threats even during backup and restore activities.

Using this option, you can configure the Windows client agent to automatically detect and repair viruses during a backup, copy, count, or restore operation.

To enable virus scanning for Windows client agents

1. Open the Backup Manager or the Restore Manager.
2. From the toolbar, click the Options button to display the Global Options dialog.
3. Click the Virus tab.
4. Select Enable Virus Scanning.

5. Click the virus scanning options that you want to apply to the client agent. Available options include:

Skip

Do not back up or restore an infected file.

Rename

Rename the infected files with the extension x.AVB (for example, 0.AVB, 1.AVB, 2.AVB). If a file with the same name and the extension AVB exists, the system will name the file with a numeric version of that extension, for example, AV0, AV1, AV2.

Delete

Delete the infected file.

Cure

eTrust Antivirus cures the files that have been found to be infected. With the Cure option, infected files are automatically repaired during a backup without user intervention.

6. If you want each archive's component files individually verified, enable Scan Compressed Files.

Note: This option may reduce backup or restore performance.

Customizable Local Options

When you explicitly select a parent object (in a parent-child database configuration), you can right-click a client agent object to customize local backup options. For more information on explicit job packaging see the *Implementation Guide*, and for more information on how to select sources when customizing local options see the *Administration Guide*.

NetWare Client Agent Configuration

The following sections discuss the configuration of CA ARCserve Backup NetWare client agents.

Note: Your Windows machine must be configured with the Novell client for Windows to install and run NetWare servers in your network.

NetWare-related Configuration Notes

Be aware of the following issues when configuring the NetWare client agent:

- Multiple jobs are not supported. The NetWare client agent can service only one job at a time. Trying to submit jobs to the client agent from multiple CA ARCserve Backup servers at the same time may cause the current job to fail.
- CA ARCserve Backup skips open NetWare files during a backup. When backing up NetWare files using the NetWare client agent, in some cases multiple files are detected as open and are skipped during the backup. Should this happen, select the Retry tab in the Backup Options dialog, and then select the Use Lock Mode if Deny Write Fails option in the File Sharing section, and resubmit the job.
- NetWare has a 255 character path name limit; for example, DIR1\DIR2\...DIRx. This restriction applies only to NetWare and not to other client agents, such as those for Windows, UNIX or Linux systems.

Note: If a NetWare path name exceeds 255 characters, backup and restore operations work properly but path entries are truncated when they are displayed during browsing. Also, the Restore to Original or Alternate Location options still work for restores to the same client agent types.

Configure NetWare Network Communication

To configure the NetWare client agent for communication, edit the ASCONFIG.INI file to specify the IP address assigned to the client agent by the system administrator. Specifying an IP address is useful in a server with multiple IP addresses. Instead of using only the first bound address, the client agent uses the ASCONFIG.INI file to find the IP address to use.

To edit the ASCONFIG.INI file

1. From a text editor, open the ASCONFIG.INI file located in the client agent home directory.
2. Add the following line to the NetWare Agent section of the file, specifying the IP address that you want the client agent to use:

```
IPAddress = nnn.nnn.nnn.nnn
```

If a NetWare Agent section does not exist, create one by adding the following line to the end of the ASCONFIG.INI file:

```
[NetWare Agent]
```


3. Save the file and exit from the editor.
4. Unload and restart the client agent. Unloading is required for changes to the ASCONFIG.INI file to take effect. To unload the client agent, use the NetWare client agent's Unload & Exit menu option. Alternatively, you can enter the following command at the server console:

```
unload nwagent
```

5. When the client agent has been unloaded, restart the client agent (that is, reload the agent) at the server prompt by issuing the following command:

```
nwagent
```

A message appears at the server prompt, confirming the use of the IP address specified in the ASCONFIG.INI file:

```
IP Address nnn.nnn.nnn.nnn from ASCONFIG.INI file will be used.
```

A similar message is displayed on the client agent runtime message screen:

```
IP Address nnn.nnn.nnn.nnn is bound for use by NetWare Push Agent.
```

The client agent is now ready to service backup and restore jobs using the IP address specified in the ASCONFIG.INI file.

Back Up Novell Directory Services

To properly back up Novell Directory Services (NDS), you must enter the full NDS name in the NDS Login name field. For example:

```
.cn=admin.o=organization_name
```

When restoring any NetWare sessions, you must supply the full NDS name when prompted for security information.

UNIX, Linux, and Mac OS X Client Agent Configuration File

The UNIX, Linux, and Mac OS X client agent configuration file, `uag.cfg`, is located on the remote client workstation in the client agent home directory. This file, which is scanned for entries whenever a job is submitted to the workstation, can be used to set multiple options associated with the client agent.

Important! *Do not change any of the variables in the agent configuration unless instructed to do so by a representative of CA Technical Support.*

UNIX, Linux, and Mac OS X Configuration Considerations

The following list describes issues that you should be aware of when configuring the client agent on the UNIX, Linux, and Mac OS X platforms.

- **Session passwords**—Session passwords cannot be longer than 22 bytes for UNIX, Linux, and Mac OS X sessions.
- **Single character directory names**—You may experience display issues in restore views when restoring single character directory names. The data appears correctly in the database view.
- **Traverse Symbolic Links and Traverse NFS**—The options Traverse Symbolic Links and Traverse Network File System (NFS) are not supported for restore operations.

Note: If a configuration discrepancy exists in the CA ARCserve Backup option definitions for these client agents, the options that were set through the Backup Manager always take precedence over the options manually entered in the uag.cfg configuration file.

Port Address Configuration

The default TCP and UDP ports are 6051. The TCP port is used for communication and data transfer between the backup server (cprocess) and the client agent. The Backup Manager user interface uses the UDP port to browse hosts.

If you want to configure either the TCP port or the UDP port, or both, you must modify the configuration files on both the CA ARCserve Backup server and the client agent so that their values match.

The names of the configuration files are as follows:

- **CAPortConfig.cfg**—for CA ARCserve Backup Windows servers
- **agent.cfg**—for client agents

Note: See UNIX, Linux, and Mac OS X Client Agent Control Files for important information about the UNIX, Linux, and Mac OS X configuration files.

The following example shows the Windows server configuration file (CAPortConfig.cfg):

```
#Hostname IP address (optional) TCP port UDP port
#myhost xxx.xxx.xxx.xxx 6051 6051
```

The following example shows the syntax for the client agent configuration file (agent.cfg):

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

UNIX, Linux, and Mac OS X Client Agent Control Files

The UNIX, Linux, and Mac OS X client agent control files specify which directories, file systems, or file system types are to be excluded from backup operations on a specific workstation. In particular, the following packages must be installed with the UNIX, Linux, and Mac OS X client agents:

- The Computer Associates Common Agent
- The Computer Associates UNIX File System Agent (uagent)

Note: You must install the Common Agent before you install the uagent.

The control files installed for both packages include:

- Directory Control file

Use the Directory Control file, `uag.cntl`, to list all directories or file systems (or both) that you want to exclude from backup operations on a workstation. To specify directories and file systems in this file, enter a slash (/) followed by a one line, complete path name. For example:

```
/opt/account1
```

Note: The Directory Control file is stored on the client agent workstation in the `uagent` home directory.

- File System Control file

The File System Control file, `fs.cntl` lists the file system types on a particular workstation that are to be excluded from backup operations. To exclude a particular file system type, enter the type on a separate line in the `fs.cntl` file.

Note: The File System file is stored on the client agent workstation in the `uagent` home directory.

- Browser Configuration File

The Browser Configuration file, `cabr.cfg`, enables raw devices to be viewed with the browser. You must ensure that you have entered the absolute name of the raw device on a separate line in the `cabr.cfg` file.

- Common Agent Configuration File

The Common Agent configuration file, `agent.cfg`, keeps track of each UNIX, Linux, or Mac OS X client agent installed on your system. This script is run automatically after the `uagent` is installed.

Note: Only a system administrator can edit the Directory and File System control files. However, other users may be able to append the files, depending on the file access rights the system administrator has assigned to the file.

Common Agent Configuration File

The Common Agent configuration file, called `agent.cfg`, tracks each UNIX, Linux, or Mac OS X client agent or application-specific backup agent installed on your system. The `agent.cfg` file is located under the CA ARCserve Backup Common Agent installation directory, `/opt/CA/BABcmagt`, of each UNIX, Linux, and Mac OS X machine. The file is populated with the required client agent information during the setup process, when the `uagentsetup` script is run. This script runs automatically after the `uagent` is installed.

Common Agent Configuration File Structure

Each section of the agent.cfg file contains groups of fields that directly correspond to an installed client agent on a UNIX, Linux, or Mac OS X device in the backup network. Except for the agent home directory location, all fields in the file are predetermined.

The environment variable field (ENV) contents are also determined during client agent installation and configuration. However, if required, you can enter values for this variable into the file manually. You should modify the agent.cfg only in certain circumstances; for example, if you wanted to associate an additional environment field with a particular database.

Note: Modifications to the agent.cfg file take effect only after the client agent machine is started (or stopped and restarted).

An example of the agent.cfg file is shown in the following table, with a description of each agent field.

| File Contents | Field Description |
|---------------------------|---|
| [0] | Object type, a predefined number of a specific client agent in the network for UNIX and Linux |
| [4] | Object type, a predefined number of a specific client agent in the network for Mac OS X |
| NAME BABagtux | Name of the client agent |
| VERSION nn.n | Release and version number of the client agent |
| HOME /opt/CA/BABuagent | Default home directory for the client agent |
| #ENV CA_ENV_DEBUG_LEVEL=4 | Environment variable passed to the client agent |
| #ENV CAAGPERF_ENABLE=1 | Enables the features Snapshot and Direct I/O on Solaris and HP. For more information, see the section Configure Snapshot and Direct I/O |
| ENV LD_LIBRARY_PATH | Shared library search path for Sun, Linux, Tru64, and Mac OS X |
| ENV SHLIB_PATH | Shared library search path for HP |
| ENV LIBPATH | Shared library search path for AIX |
| BROWSER cabr | Browser module for the client agent |

| File Contents | Field Description |
|----------------------|---|
| AGENT uagentd | Backup module for the client agent daemon |
| MERGE umrgd | Merge daemon |
| VERIFY umrgd | Scan daemon |

Client Agent Home Directory

The default client agent home directory, BABuagent, is automatically defined during installation and setup. If required, however, you can specify a different home directory.

To locate the name of the home directory, look in the agent.cfg file under the BABagntux section of the file. The name of the client agent home directory is defined by the HOME variable.

How Common Agent Connection Requests Work

To initiate a client agent session, the CA ARCserve Backup server requests a connection for a UNIX, Linux, or Mac OS X client agent to use a specific backup component (such as BROWSER, BACKUP, or RESTORE). When it receives the request, the Common Agent accepts the connection and verifies the user's credentials for the system.

Upon user validation, the Common Agent checks the agent.cfg file for an entry corresponding to that particular client agent and the specified component. Only after it has validated both the client agent and the requested component does the Common Agent activate the client agent and the component. The Common Agent then returns to a state of waiting for additional requests.

Configurable Options

Options are used to optimize and customize the operation of the client agent. However, none of these options are required for the client agent to run. A complete list of options available for use when starting the UNIX, Linux, or Mac OS X client agent is shown in the following table.

Note: These options should be carefully set by administrators having UNIX, Linux, or Mac OS X knowledge. If you do not understand what an option or parameter means, do not set the feature unless instructed to do so by a CA Technical Support representative.

| Option | Description |
|--|---|
| -ALLOW < <i>network address</i> > < <i>host address</i> > | Use this option with Single User mode, with the -S or -NOPASSWORD option, to define the IP addresses of computers that are authorized to access the client agents without requiring validation. |

-ALLOW N:172.16.0.0(255.255.255.0) H:172.31.255.255

In this example, N denotes a network address and H denotes a host IP address. You can set an optional subnet mask.

| Option | Description |
|---------------------|--|
| -b <i>bufsize</i> | Defines the disk I/O buffer size in bytes. Options are 16384 to 65536 bytes; the default is 65536 bytes. |
| -c <i>n</i> | Specifies the sleep time while waiting, in milliseconds (ms). Options are zero (0) to 1000 ms; the default is 50 ms. |
| -CAUSER <i>USER</i> | Defines Single User mode. Used with the -S or NOPASSWORD option to set the Allow or Deny list on a per-user basis. |

For example:

-CAUSER A: USER1 N: USER2

In this example, A means –ALLOW and N corresponds to -DENY.

| Option | Description |
|---|---|
| -DENY < <i>network address</i> > < <i>host address</i> > | Use this option with Single User mode, with the -S or NOPASSWORD option, to define the IP addresses that are not allowed access to the client agents. |

For example:

-DENY N:172.16.0.0(255.255.255.0) H:172.31.255.255

In this example, N denotes a network address and H denotes a host's IP address. You can set an optional subnet mask.

| Option | Description |
|------------------|--|
| -l | Causes the client agent to check for advisory locks. The default is mandatory locks only. |
| -m <i>maxbuf</i> | Sets the number of buffers allocated for I/O. Options are 2 to 1024 buffers; the default is 128. |
| -NOPASSWORD | Specify this option if you need to use either the -ALLOW, -DENY, or -CAUSER options. This option is the same as the -S option in Single User mode with no password required. |
| -P <i>n</i> | Specifies the default time out, followed by a variable number (<i>n</i>), which is user-defined and measured in minutes (0 to 10). The default is 5 minutes. |

For example, the option `-P 10` assigns a wait time period for the backup or restore pre-script of 10 minutes.

Note: An error occurs if you use the `-P` option without defining a number *n*.

| Option | Description |
|---|---|
| <code>-Prebackup filename</code> | Executes the default pre-scripts and post-scripts associated with the type of backup or restore job being run. The filename is optional and if is not specified, <code>uag_pre_backup</code> will be treated as the filename. |
| <code>-Postbackup filename</code> | |
| <code>-Prerestore filename</code> | |
| <code>-Postrestore filename</code> | |
| <code>-S</code> | Enables the Single User mode option. In Single User mode, user credentials are not checked against valid user IDs and passwords. Instead, access is granted based on the <code>-ALLOW</code> , <code>-DENY</code> , or <code>-CAUSER</code> options. For more information see the specific option. |
| <code>-s <i>async</i> <i>nonblocking</i></code> | Sets socket I/O to asynchronous, nonblocking mode. |
| <code>-s <i>bufsize</i></code> | Specifies the size of the socket buffer. Options are 4096 to 65536. The default is system dependent. |
| <code>-s <i>SocketMode</i></code> | Specifies to use socket mode for backup operations. |
| <code>-sparse</code> | Differentiates between sparse file and regular file operations. This option increases the efficiency of sparse file backups and restores. Note: Quota files are always treated as sparse files in backup and restore operations, regardless of whether you specify <code>-sparse</code> . |
| <code>-verbose</code> or <code>-v</code> | Places the system in verbose mode to enable the entry of detailed debugging messages at the console. |

Snapshot and Direct I/O Support for UNIX

UNIX client agents support the Snapshot and Direct I/O features. To take advantage of these features, one of the following environments must exist on the machine running the UNIX client agent:

| Feature | Platform | Software Requirements |
|------------|------------|--|
| Snapshot | Solaris | UFS file system with the fssnap package installed (Solaris 8 and 9) or the advanced version of VxFS file system. |
| Snapshot | HP-UX 11.0 | Advanced version of VxFS file system or Online Journaling File System (JFS). |
| Direct I/O | Solaris | UFS file system or VxFS file system. |
| Direct I/O | HP-UX 11.0 | Advanced version of VxFS file system or Online JFS. |

Snapshot and Direct I/O Descriptions

With Direct I/O, the client agent takes a snapshot on advanced versions of VxFS, Online JFS (HP-UX), and UFS with fssnap installed on Solaris. The client agent mounts the snapshot to a temporary directory created in the root volume, and then generates the snapshot backup. After the snapshot backup is complete, the client agent dismounts from the temporary directory and deletes the snapshot.

To perform a snapshot backup, you must specify a snapshot buffer. A snapshot buffer is the disk space used to store the original data before it is overwritten in the snapped volume. Remember these considerations when using the snapshot buffer:

- The snapshot buffer needs to be large enough to store all the data that changes in the snapped volume for the duration of the backup. If the snapshot buffer runs out of space, the snapshot becomes invalid and the backup fails.
- The snapped volume and the snapshot buffer should not be on the same file system.
- For better performance, the snapped volume and the snapshot buffer should be on separate physical disks.
- For UFS on the Solaris platform (using fssnap), the snapshot buffer can be a file name, a directory name, or a raw partition.

For a Direct I/O backup or restore, you need to check the client environment and edit the `caagperf.cfg` configuration file. You can view Snapshot and Direct I/O on the file systems in the `caagperf.cfg` file by executing the `mount` command at the command line after submitting the backup or restore job.

For Snapshot, the output that appears after executing the `mount` command is a new, read-only file system with the mount point starting with the prefix `SNAP_HOME_`. A Direct I/O user can observe the changes in the mount options on that particular file system. You can also see the detailed messages in the `caagperf.log` file if you enabled the logging flag in the `caagperf.cfg` file.

The following sections describe how to configure a UNIX client agent to use these features.

Configure Snapshot and Direct I/O

To configure the Snapshot and Direct I/O features, follow these steps:

1. Enable the environment variable `CAAGPERF_ENABLE` by adding the following line in the `agent.cfg` file:

```
ENV CAAGPERF_ENABLE=1
```

Note: The `agent.cfg` file is in the `/opt/CA/BABcmagt` directory.

After you enable this environment variable, the client agent section of the `agent.cfg` file looks like this:

```
[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. Prepare the configuration file named `caagperf.cfg` in the `/opt/CA/BABcmagt` directory. You need to specify the types of operations to be completed on the specified file systems in the `caagperf.cfg` file. See the next section for detailed descriptions.

Configuration Table Parameters and Values

The format of the configuration file is similar to a Windows .inf file. It has sections and key value pairs. The section names are the names inside the square brackets, and key value pairs are in KEY=VALUE format with one pair on each line. All the entries in the configuration file are case-sensitive.

The key value pairs are under the volumes to which they belong, and the section names are the names of those volumes. Two examples of the syntax of the section name in the caagperf.cfg file are [/] or [/export/home]. If a volume has multiple entries, the behavior of the client agent is undefined.

The key value pairs are used to set parameters for the volume under which they belong. By default, all options are disabled. If no special processing is needed for a volume, that volume should not be in the caagperf.cfg file.

The keys and their values are described in the following table:

| Key | Value |
|----------------|---|
| DOSNAP | Enables the Snapshot feature on a volume. The value should be BACKUP, meaning that a snapshot should be taken during the backup operation. |
| SNAPSHOTBUFFER | Specifies the buffer used for storing original data before it is overwritten in the snapped volume. The value should be a file name or partition. The file can be a file or a directory from a different volume. The value of this field depends on the file system type. For the advanced version of VxFS or Online JFS, the value is the name of an empty partition. For UFS, the value is a file name, a directory name, or a partition name. |
| DOUBIO | Enables the Direct I/O feature on a volume. Values are BACKUP, RESTORE, and BACKUP_RESTORE. The value of this field depends on your backup or restore requirements. |

You may find the following configuration file samples useful.

Configuration File Example 1

This is a sample configuration file for a Solaris 8 or Solaris 9 operating system with a UFS file system with fssnap installed. The first line of the file is a debugging flag. The three sections that follow the debug entry correspond to the /opt, /export/home, and / volumes on the disk.

The sections for /opt and /export/home have Snapshot enabled during backup, and the / section has Direct I/O enabled for backup and restore.

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

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

[/]
DOUBIO=BACKUP_RESTORE
```

Configuration File Example 2

This is a sample configuration file for a Solaris 8 operating system with the advanced version of the VxFS file system installed.

The file contains three sections. The first line of the file is a debugging flag. The three sections in the file are /opt, /export/home, and / volume. Sections for /opt and /export/home have Snapshot enabled during backup, and the / volume has Direct I/O enabled for backup and restore.

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

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

[/]
DOUBIO=BACKUP_RESTORE
```

Trace Levels for the AS/400 Enterprise Option

Occasionally, based on instructions from CA Technical Support, you may need to change the level of activity that is logged for the AS/400 Enterprise Option. Because tracing levels can affect backup performance, do not change the values unless you receive specific instructions from CA Technical Support.

The following table shows all of the AS/400 Enterprise Option trace levels:

| Level | Description |
|------------------|--|
| ASO\$TRACE | This controls the trace depth of the client agent. Valid values are -1 and 0 to 0xFFFFFFFF. Setting the ASO\$TRACE value to -1 logs the most detail. |
| ASO\$TRACE_AST | This is a toggle. If defined, Asynchronous System Traps (ASTs) are traced. |
| ASO\$TRACE_IDENT | This is a formatting parameter. The recommended value is between 0 and 5. The default is 3. |
| ASO\$TRACE_DATA | This controls the number of bytes in each packet that is logged. The range is unlimited and starts at 0. The default is 300. |

Configuration File Example 3

This is a sample configuration file for the HP-UX operating system that can have either an advanced version of the VxFS file system or the online JFS file system installed.

The file contains four sections. The first line of the file is a debugging flag. The sections in the file are the /, /var, /usr, and /export volumes. In this file the / volume is enabled for Direct I/O during backup and restore and the other volumes are enabled for Snapshot during backup.

```
##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
```

UNIX, Linux, and Mac OS X Access Control Lists

For UNIX, Linux, and Mac OS X client agents, ACLs are supported in Single User mode only. This is also known as No Password mode. A UNIX, Linux, and Mac OS X client agent—or database backup agent—can be put into Single User mode by specifying a NOPASSWORD entry in its corresponding section in the Common Agent configuration file, `agent.cfg`, located in `/opt/CA/BABcmagt`. A UNIX, Linux, and Mac OS X client agent can also be put into Single User mode by specifying the `-S` or `-NOPASSWORD` option in the `uag.cfg`. You can use two types of ACLs with the UNIX, Linux, or Mac OS X client agent:

- An access control list that denies or allows specific users to perform backups or restores. For example, a part of the `agent.cfg` file is shown in the following sample. You need to make similar changes for other client agent sections if you want to apply ACLs to those client agents too.

```
[0]
NAMEBABagentux
VERSIONnn.n.n
HOME/opt/uagent
NOPASSWORD
CAUSER A:CAUSER1 N:CAUSER2
```

NOPASSWORD enables Single User mode, and CAUSER specifies the users for whom permission is being granted or denied. (A stands for ALLOW and N stands for DENY.) A:CAUSER1 enables CAUSER1 to perform jobs, and N:CAUSER2 denies access to CAUSER2.

Note: For UNIX and Linux client agents, the object type is [0]. For the Mac OS X client agent, the object type is [4].

- An access control list that determines whether specific IP addresses can access the system. For example, a part of the `agent.cfg` file is shown in the following sample. You must make similar changes for other client agent sections of the file if you want to apply ACLs to those client agents too.

```
[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
```

NOPASSWORD enables the Single User mode, and ALLOW and DENY specify whether a particular network or IP address is allowed to access the system. N denotes a network address and H denotes a host's IP address.

Note: An optional subnet mask can follow a network address; subnet masks are shown in parentheses.

For UNIX, Linux, and Mac OS X client agents, the specific type of ACL can be specified in `uag.cfg`, or you can specify them using the `-S`, `-NOPASSWORD`, `-CAUSER`, `-ALLOW`, and `-DENY` options. For more information about these options, see the section Configurable Options.

You can apply both types of ACLs concurrently. In each case, DENY takes precedence over ALLOW. In the Single User mode, all operations on the client agent are performed with superuser privileges. The `caagentd.log` contains information about the users, IP addresses, and network addresses denied during Single User mode.

AS/400 Enterprise Option Configuration

The AS/400 Enterprise Option start and stop preferences are configured using STRASO and ENDASO.

Configure Start Preferences

To configure start preferences for the AS/400 Enterprise Option, follow these steps:

1. From the command line, issue:

```
straso
```

2. Press F4.

The available options display.

- Type your preferences and press Enter.

Note: You can configure the preferences for Library Level Backup and Use QaneSava. These preferences enhance performance. For more information, see the section Performance Configuration.

```

File Edit View Communication Actions Window Help
Start Client Agent for AS400 (STRASD)

Type choices, press Enter.

Job description . . . . . ASQJOB      Name
Job description library . . . *LIBL      Name, *LIBL
Job queue . . . . . *JOB       Name, *JOB
Job queue library . . . . .          Name, *LIBL
Start subsystem . . . . . *YES       *YES, *NO
Subsystem to start . . . . . ASQSBS     Name
Subsystem library . . . . . *LIBL      Name, *LIBL
Trace level . . . . . *OFF       Character value, *OFF...
I/O buffer size . . . . . 32K        16K, 24K, 32K, 40K, 48K...
Socket buffer size . . . . . 64K        64K, 64K
Initial Receive Timeout(30Sec) 000015 - 999999
Library Level backup . . . . . *ON        *OFF, *ON
Use QaneSava . . . . . *ON        *ON, *OFF

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys

```

Performance Configuration

By default both Use QaneSava and Library Level Backup are set to *ON. These settings increase the performance of the agent for library level back ups.

Use the Use QaneSava flag to toggle between *ON and *OFF. With the Use QaneSava flag set to *ON back ups are executed without creating a temporary SAVF file. By setting the flag to *OFF, back ups are executed and will create a temporary SAVF file.

Use the Library level backup flag to control the back up of libraries. When the Library level backup flag is set to *ON, the SAVLIB command is applied to library objects. The SAVLIB command improves performance because it saves both library information and all files inside a library in one backup. The Library Level Backup feature is especially useful when performing multiple library backups.

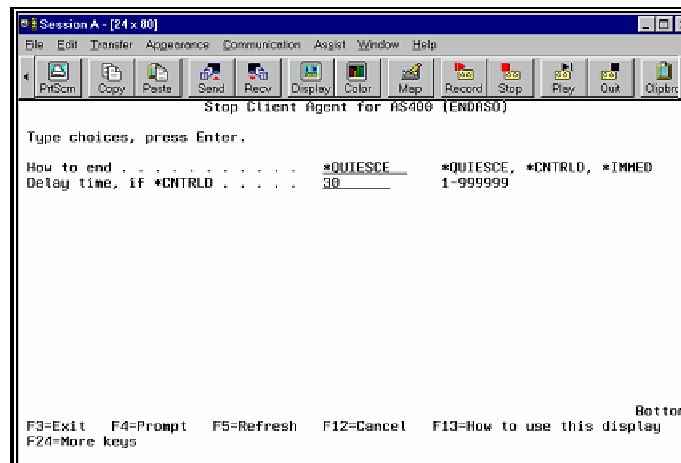
By setting the flag to *OFF, the SAVOBJ command is used to back up each file inside a library separately. Use this approach if you are not intending to do Library Level Backups.

Note: The Library Level Backup feature does not support incremental and differential backups.

Configure Stop Preferences

To configure stop preferences for the AS/400 Enterprise Option, follow these steps:

1. From the command line, issue:
endaso
2. Press F4. The options display on the configuration screen.
3. Type your preferences and press Enter.



OpenVMS Enterprise Option Configuration

Other than the port address, the OpenVMS Enterprise Option does not require additional configuration after installation.

Configure Port Address

The default TCP and UDP port addresses are both 6050. The TCP port is used for communication and data transfer between the cprocess and the client agent. CA ARCserve Backup uses the UDP port to browse the hosts.

If you want to configure the TCP port or the UDP port, include the following command in the bab\$startup.com file:

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

In this example, nnnn is the port number of the Backup Manager.

Important! *OpenVMS requires that both the UDP and TCP ports be assigned the same port number.*

TCP/IP Stack Optimization

The configuration of the TCP/IP stack can affect client agent performance. Typically, the TCP Send and Receive quotas are set to 4096. Set these values to the largest value allowed by the specific stack installed on the OpenVMS system.

Trace Levels for the OpenVMS Enterprise Option

Occasionally, based on instructions from Computer Associates Technical Support, you may need to change the level of activity that is logged for the OpenVMS Enterprise Option. Because tracing levels can affect backup performance, do not change the values unless you receive specific instructions from CA Technical Support.

| Level | Description |
|------------------|--|
| ASO\$TRACE | This controls the trace depth of the client agent. Valid values are -1 and 0 to 0xFFFFFFFF. Setting the ASO\$TRACE value to -1 logs the most detail. |
| ASO\$TRACE_AST | This is a toggle. If defined, Asynchronous System Traps (ASTs) are traced. |
| ASO\$TRACE_IDENT | This is a formatting parameter. The recommended value is between 0 and 5. The default is 3. |
| ASO\$TRACE_DATA | This controls the number of bytes of each packet that is logged. The range is unlimited and starts at 0. The default is 300. |

Chapter 4: Using the Client Agents

This chapter describes how to use the client agents in a standard backup environment. It includes:

- Descriptions of the backup and restore statistics that the client agents can obtain and write to online logs, as well as the procedures for accessing this logged data
- Details on how to start and stop the client agents
- Instructions for scheduling and initiating backup and restore jobs and for checking the status of online client agents

This section contains the following topics:

[Runtime Statistics](#) (see page 61)

[Activity Logs](#) (see page 62)

[Back Up Windows Network Server Data](#) (see page 65)

[Client Agent Start and Stop Procedures](#) (see page 65)

Runtime Statistics

The client agent runtime components for both Windows and NetWare provide real-time statistics and display the progress of backup and restore jobs as they are being processed.

Note: Runtime statistics apply only to Windows and NetWare.

View Runtime Statistics for the Windows Client Agent

To obtain runtime statistics for Windows client agents, follow these steps:

1. From the Windows Programs (or All Programs, on XP machines) menu, select CA, ARCserve Backup, Backup Agent Admin.
2. Select Connections. The system displays the last ten jobs processed. If the job is still active, you can click the job to display its current runtime statistics. If the job has completed, completed statistics for that job are displayed.

Note: The statistics are kept in memory; therefore, if you close the Backup Agent Admin dialog and the Universal Agent service, the connection statistics will be lost. You will, however, still be able to view the results of the job in the activity log.

View Runtime Statistics for NetWare Client Agents

With the NetWare client agent, if the Runtime window is not available, you must switch windows to display it. If you are running Remote Console (RCONSOLE.EXE) to view the server console, press the ALT and F3 keys simultaneously and continue pressing the keys until the Runtime window opens. If you are at the server console, press the ALT and ESC keys simultaneously to switch windows.

Note: You can press the Ctrl and ESC keys simultaneously to display a list of current windows, and then you can choose the Runtime window.

Activity Logs

The server-based CA ARCserve Backup system generates an activity log, which displays information about all the jobs that the client agent processes. The following sections explain how to display the activity log for each client agent from the server side and from the client agent side.

View Activity Logs on a Windows Server

To view the activity log on a Windows CA ARCserve Backup server, follow these steps:

1. From the CA ARCserve Backup Home Page, select the Job Status menu to open the Job Status Manager.
2. Click the Activity Log tab to view a list of logs, as shown in the following example:

| Type | Server | Date | Job | Session | Message |
|----------------------------------|-----------------|--|------------|---|---------|
| Job11 | | [Merge on 2007-04-23] | [Failed] | [04/23/2007 11:34:52 AM - 04/23/2007 11:34:54 AM] | |
| Job9 | Phil_001-042307 | [Finished] | | [04/23/2007 11:29:22 AM - 04/23/2007 11:29:22 AM] | |
| Logs of the Master Job | | | | | |
| Job10 | | [STAGING [JOB 3] SUBJOB 1, Source [\\LUFDA028], Phil_001-042307] | [Finished] | | |
| Job8 | | [Database pruning job] | [Finished] | [04/22/2007 12:00:30 PM - 04/22/2007 12:00:30 PM] | |
| Generic Logs | | | | | |
| Week [04/15/2007 - 04/21/2007] | | | | | |
| Job7 | | [Database pruning job] | [Finished] | [04/21/2007 12:00:46 PM - 04/21/2007 12:00:46 PM] | |
| Job6 | | [Database pruning job] | [Finished] | [04/17/2007 12:00:48 PM - 04/17/2007 12:00:48 PM] | |
| Job5 | | [Database pruning job] | [Finished] | [04/15/2007 12:00:26 PM - 04/15/2007 12:00:26 PM] | |
| Generic Logs | | | | | |
| Week [04/08/2007 - 04/14/2007] | | | | | |
| Job4 | | [Database pruning job] | [Finished] | [04/14/2007 12:00:32 PM - 04/14/2007 12:00:32 PM] | |
| Job3 | | [Database pruning job] | [Finished] | [04/13/2007 12:00:32 PM - 04/13/2007 12:00:32 PM] | |
| Job2 | | [Database pruning job] | [Finished] | [04/12/2007 12:00:34 PM - 04/12/2007 12:00:34 PM] | |
| Job1 | | [Database pruning job] | [Finished] | [04/11/2007 12:00:28 PM - 04/11/2007 12:00:28 PM] | |
| Generic Logs | | | | | |
| Week [04/01/2007 - 04/07/2007] | | | | | |
| Generic Logs | | | | | |
| Week [03/25/2007 - 03/31/2007] | | | | | |
| Generic Logs | | | | | |

The printer or print-to-file output of a client agent activity log file looks like the one shown in the following sample:

```

CA ARCserve Backup Server: COMPO01
CA ARCserve Backup Activity Log

Type      Server      Date              Job      Session  Message
-----
This Week [ 06/10/2007 - 06/16/2007 ]
Week [ 06/03/2007 - 06/09/2007 ]
Week [ 05/27/2007 - 06/02/2007 ]
Job43 ( Database pruning job ) [Finished] [05/23/2007 12:00:06 PM - 05/23/2007 12:00:26 PM] [Job No. 1]
Logs of the Master Job
Information  COMPO01      05/23/2007 12:00:27 PM      49      End pruning logs
Information  COMPO01      05/23/2007 12:00:27 PM      49      Begin pruning logs.
Information  COMPO01      05/23/2007 12:00:06 PM      49      Prune Database Operation Successful.
Information  COMPO01      05/23/2007 12:00:06 PM      49      ** Summary for Job **
Information  COMPO01      05/23/2007 12:00:06 PM      49      End pruning database. (PRUNED=0)
Information  COMPO01      05/23/2007 12:00:06 PM      49      Pruning sessions older than 20 days.
Information  COMPO01      05/23/2007 12:00:06 PM      49      Begin pruning database.
Information  COMPO01      05/23/2007 12:00:06 PM      49      Run Prune Database Job Scheduled for 5/23/07 at 12:00 PM.
Job46 ( Database pruning job ) [Finished] [05/26/2007 12:00:00 PM - 05/28/2007 12:00:30 PM] [Job No. 1]
Job47 ( Database pruning job ) [Finished] [05/27/2007 12:00:12 PM - 05/27/2007 12:00:32 PM] [Job No. 1]
Generic Logs:
Week [ 05/20/2007 - 05/26/2007 ]
Week [ 05/13/2007 - 05/19/2007 ]
Week [ 05/06/2007 - 05/12/2007 ]
Week [ 04/29/2007 - 05/05/2007 ]
Week [ 04/22/2007 - 04/28/2007 ]
Job17 ( Database pruning job ) [Finished] [04/26/2007 12:00:22 PM - 04/28/2007 12:00:22 PM] [Job No. 1]
Job16 ( Database pruning job ) [Finished] [04/27/2007 12:00:30 PM - 04/27/2007 12:00:30 PM] [Job No. 1]
Job15 ( Backup[Custom] ) [Failed] [04/27/2007 08:38:58 AM - 04/27/2007 08:38:58 AM] [Job No. 2]
Job14 ( Database pruning job ) [Finished] [04/26/2007 12:00:18 PM - 04/26/2007 12:00:18 PM] [Job No. 1]
Job13 ( Database pruning job ) [Finished] [04/25/2007 12:00:36 PM - 04/25/2007 12:00:36 PM] [Job No. 1]
Job12 ( Database pruning job ) [Finished] [04/24/2007 12:00:36 PM - 04/24/2007 12:00:36 PM] [Job No. 1]
Job11 ( Merge on 2007-04-23 ) [Failed] [04/23/2007 11:34:52 AM - 04/23/2007 11:34:54 AM] [Job No. 5]
Job9 ( USER_001-042307 ) [Finished] [04/23/2007 11:29:22 AM - 04/23/2007 11:29:22 AM] [Job No. 2]

```

View Activity Log on a NetWare Client Agent Machine

The NetWare client agent writes to the `nwagent.log`, which is created in the client agent home directory. You can view this log using Windows Explorer by opening the file in the client agent home directory. Alternatively, you can view log file contents by selecting `View nwagent.log` at the console.

View Activity Log on a UNIX, Linux, or Mac OS X Client Agent Machine

As soon as the UNIX, Linux, or Mac OS X client agent begins running, an activity log file called `uag.log` is created and stored in the logs directory. The logs directory resides under the client agent home directory.

The `uag.log` file records all activities and errors that occur during machine backup and restore jobs. Each job is identified numerically in sequence, as well as by date and time, in the log display.

On the client agent machine, you can view the contents of these logs using the print `filename` command.

Note: All log messages relating to the Common Agent are located in the `/opt/CA/BABcmagt/logs/caagentd.log` file.

Activity Logs on Computer Running the AS/400 Enterprise Option

The Enterprise Option for AS/400 creates a log file in the CA ARCserve Backup library. The two file members are:

- AGENT.MBR, which records the activities and errors relating to agent operations
- ASBR.MBR, which records information on CA ARCserve Backup browsing activities

Activity Logs on Computers Running the OpenVMS Enterprise Option

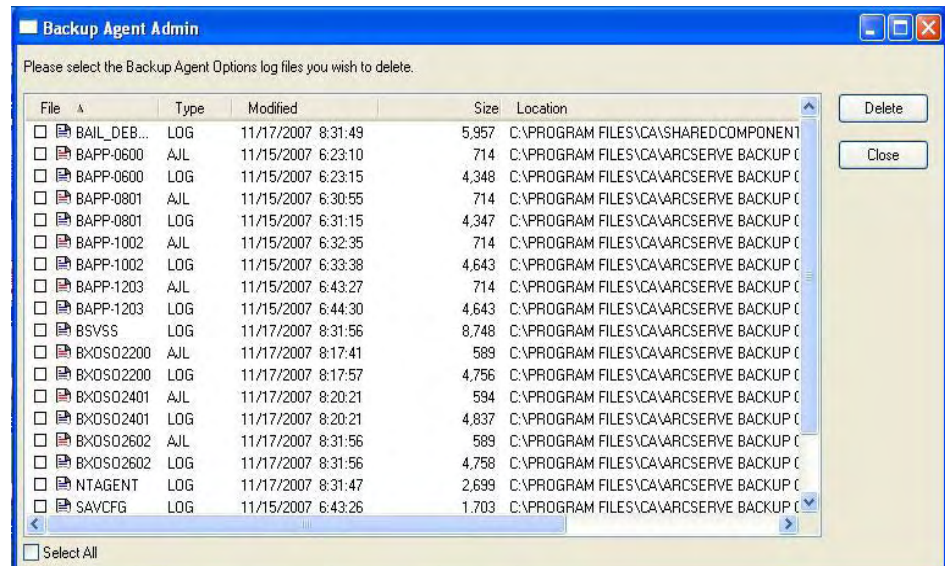
As soon as the agent begins running on the server, CA ARCserve Backup generates an activity log file named `aso$agent_<nodename>.log`, and stores it in the logs directory. A new log file—identified by sequential job number, date, and time—is created for each job and every subsequent startup of the agent. The content of each log file is determined by the level of tracing enabled on the agent.

Delete Client Agent Log Files

For UNIX, Linux, and Mac OS X client agents, delete log files from the client machine the same way you would delete any file on that machine. For example, run:

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

For Windows client agents, use the Backup Agent Admin to delete log files:



Back Up Windows Network Server Data

If you installed a client agent on a Windows server, you can back up the server data through the client agent by following these steps:

1. Open the Backup Manager.
2. Click the Source tab.
3. Expand the Network object, and then expand the Windows Systems network object until you locate the client machine.
4. Right-click the client machine. Choose Use Agent from the pop-up menu.
5. Check the Use Agent check box.
6. Select a protocol. Either select TCP/IP and enter the address for the client computer or select Use Computer Name Resolution, to specify that the client agent should determine an IP network address using the Dynamic Host Configuration Protocol.
7. Click OK.
The client agent is now selected.
8. If you are prompted for security, enter the appropriate security for your environment.

Client Agent Start and Stop Procedures

The following sections describe the procedures for starting and stopping the various client agents.

Note: If the client agent is stopped at any time during a backup or restore job, the job will fail and must be restarted.

Start and Stop the Windows Client Agent

The Windows client agent uses a common component called the Universal Agent. This component is installed or updated during installation. The Universal Agent is registered as a service that starts automatically and runs under the local system account by default. When the service starts, the Windows client agent is loaded. The Windows client agent is available even when no users are logged into the system.

Use the Backup Agent Admin to start or stop the Windows client agent. The Backup Agent Admin monitors the client agent activity and protects against accidental job failures if the Universal Agent service stops.

To start or stop a Windows client agent, follow these steps:

1. Open the Backup Agent Admin.
2. From the Options menu, select Services.
3. (Optional) If you do not want the client agent to start automatically each time you start the computer, clear the **Autostart Backup Agent when System starts** check box.
4. Click the arrow to start the service or the red dot to stop the service.

Note: Stopping the service affects other components that use the Universal Agent.

5. Close the Backup Agent Service Manager.

NetWare Start and Stop Requirement

The installation process for the NetWare client agent creates a Network Client Facility file called NWAGENT.NCF. Before starting the client agent, ensure that this file was created and stored properly in the SYSTEM directory on the NetWare server's SYS volume.

Start the NetWare Client Agent

To start the Netware client agent, issue the following command at the remote server console prompt:

```
nwagent
```

The NetWare client agent includes a module called CSLOADER.NLM, which performs monitoring functions. When you start the NetWare client agent, CSLOADER.NLM also starts. CSLOADER.NLM displays, and records in log files, the results of this process as a series of informational messages. These messages can be helpful in tracking the source of a problem.

CSLOADER.NLM also works with the Pre-Flight Check (PFC.NLM), which evaluates the environment in which the client agent will be running. If the environment fails to meet its requirements, this checking mechanism signals CSLOADER.NLM to stop the loading sequence.

Stop the NetWare Client Agent

To stop the NetWare client agent, issue the following command at the NetWare server console prompt:

```
unload nwagent
```

UNIX, Linux, and Mac OS X Client Agents Start and Stop Requirement

Before starting the client agent, ensure that it has been configured. If the client agent has not been configured, run the following script:

```
#babuagent/uagentsetup
```

In this example, *babuagent* represents the full path name of the agent home directory. The default path is `/opt/CA/BABuagent`.

Start the UNIX, Linux, or Mac OS X Client Agent

After installing a UNIX, Linux, or Mac OS X client agent, the agent is started automatically.

To check the status of the agent, issue the following command at the command line:

```
# uagent status
```

To start the agent, issue the following command at the command line:

```
# uagent start
```

If the agent is not enabled, run the configuration script, `uagentsetup`.

Stop the UNIX, Linux, or Mac OS X Client Agent

To stop the UNIX, Linux, or Mac OS X client agent, log in as root and issue the following command at the command line:

```
# uagent stop
```

Common Agent Start and Stop Status Communication

Whenever a client agent is started or stopped, the UNIX, Linux, or Mac OS X system scripts modify the `agent.cfg` file by marking the client agent entry in the file as enabled or disabled. The scripts also notify the Common Agent of the change. The Common Agent then determines whether to continue running, depending on the number of entries in the configuration file that are still enabled.

For example, issuing `uagent stop` for a UNIX client marks the `BABagntux` section disabled. If `BABagntux` is the only section of the file (that is, there is only one CA ARCserve Backup client agent installed), the Common Agent stops. You would then need to issue `uagent start` to enable the `BABagntux` section of the `agent.cfg` file.

When you enter the `uagent` start command, the Common Agent status changes from disabled to enabled. In summary, when a particular client agent is started or stopped, the scripts modify the `agent.cfg` file accordingly, and notify the Common Agent. At that point, the Common Agent decides whether to continue running, depending on the number of sections in the configuration file that are still enabled.

Check the Status of the UNIX, Linux, and Mac OS X Client Agents

To check the status of a UNIX, Linux, or Mac OS X client agent, log in as root and issue the following command at the command line:

```
# uagent status
```

If this command fails, the client agent may need to be configured. To configure the client agent, run the following script:

```
#babuagent/uagentsetup
```

In this example, *babuagent* represents the full path name of the agent home directory. The default path is `/opt/CA/BABuagent`.

AS/400 Enterprise Option Start and Stop Requirement

You must have *JOBCTL (job control) authority to start or stop the client agent.

Start the Client Agent for the AS/400 Enterprise Option

To start the agent, log on to AS/400 and issue the following command at the command line:

```
straso
```

Stop the Client Agent for the AS/400 Enterprise Option

To stop the agent, log on to AS/400 and issue the following command at the command line:

```
endaso
```

OpenVMS Enterprise Option Start and Stop Requirement

Ensure that you have the appropriate network credentials to operate the OpenVMS machine on which the client agent resides.

Start the Client Agent for the OpenVMS Enterprise Option

To start the agent, log in as system and issue the following command at the command line:

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

Stop the Client Agent for the OpenVMS Enterprise Option

To stop the agent, log in as system and issue the following command at the command line:

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

Check the Client Agent Status

To check the status of the client agent, log in and issue the following command at the command line:

```
show sys /proc=aso$*
```


Index

A

- access control lists (ACL)
 - about • 14
 - for UNIX, Linux, Mac OS X • 56
- ACL library
 - 32-bit Linux • 23
 - Linux libacl.so • 23
 - packages • 23
 - requirements • 23
- activity log
 - about • 62
 - AS/400 trace levels • 54
 - sample • 62
 - viewing • 62
- add a client agent
 - manually to a Windows or NetWare server • 27
- add or auto discover Client Agents • 25
- agent.cfg
 - client agent configuration file • 43
 - Common Agent configuration file • 44
- AS/400
 - configuration • 57
 - endaso command • 59
 - job control authority • 68
 - Library Level Backup feature • 58
 - straso command • 68
- ASCONFIG.INI • 40
- Auto Discovery
 - of client agents for Windows or NetWare servers • 25
 - of client agents for Windows, UNIX, Linux, Mac • 13

B

- bab\$shutdown.com OpenVMS command • 69
- bab\$startup.com OpenVMS command • 69
- BABuagent/uagentsetup command • 67
- Backup Agent Admin • 30
- backup verification global options • 14
- Browser Configuration file • 43

C

caagent

- start command • 21
- stop command • 21
- update command • 21
- caagentd
 - binary for Common Agent • 20
 - log file for Common Agent • 63
- caagperf.cfg configuration file • 50, 51
- caagperf.log file • 50
- cabr.cfg Browser Configuration file • 43
- CAPortConfig.cfg
 - configuration file • 43
 - example • 34
- check agent status
 - OpenVMS • 69
 - UNIX, Linux, Mac OS X • 67
- commands
 - \$>rm uag.log • 64
 - bab\$shutdown.com OpenVMS • 69
 - bab\$startup.com OpenVMS • 69
 - BABuagent/uagentsetup • 67
 - caagent • 21
 - endaso AS/400 • 68
 - mount • 50
 - nwagent • 66
 - print filename to view logs • 63
 - straso AS/400 • 68
 - uagent status • 67
- Common Agent
 - agent.cfg • 20
 - automatic installation • 19
 - caagentd binary • 20
 - configuration file • 20
 - connecting • 46
 - directory • 20
 - host equivalence user access • 23
 - port numbers • 21
 - use start and stop scripts • 21
- computer name resolution
 - about • 12
 - select protocol • 65
- configuration files
 - agent.cfg • 43
 - caagperf.cfg • 50, 52
 - CAPortConfig.cfg • 34, 43
 - port.cfg • 43
 - PortsConfig.cfg • 34

- Solaris sample • 53
- configuring
 - AS/400 • 57
 - NetWare client agent • 39
 - OpenVMS • 59
 - Snapshot and Direct I/O • 51
 - UNIX, Linux, and Mac OS X client agent • 41
 - Windows client agent • 28
 - Windows network communication • 34
 - Windows security options • 33
- control files • 43
- cprocess • 43
- create link from 32-bit library to libacl.so • 24
- cyclic redundancy check • 14

D

- data compression • 15
- Direct I/O
 - about • 50
 - Solaris and HP-UX features • 16
 - UNIX support • 50
- Directory Control file • 43

E

- endaso AS/400 command • 68
- environment variable (ENV) • 45

F

- File System Control file • 43
- fs.cntl File System Control file • 43
- fssnap • 50

H

- home directory • 46
- host equivalence user access • 23

I

- install
 - ACL libraries • 23
 - client agent for Windows • 19
- installation considerations
 - NetWare • 18
 - OpenVMS • 19
 - Windows • 17
- IP address
 - on remote Windows machine • 12
 - UNIX, Linux, and Mac OS X ACLs • 56

J

- job control authority for AS/400 • 68
- job packaging • 39

L

- libacl.so ACL library • 23
- Library Level Backup feature • 58
- Linux
 - 32-bit ACL library • 23
 - Auto Discovery of client agents • 13
 - link to 32-bit ACL Library • 24
 - verify ACL library version • 24
- log files
 - activity • 62
 - caagperf.log • 50
 - deleting • 64
 - nwagent.log • 63

M

- manager interface for Windows • 27
- multiplexing • 16
- multistreaming • 15

N

- NetWare
 - ASCONFIG.INI • 40
 - configuring client agent • 39
 - CSLOADER.NLM • 66
 - NDS • 41
 - network client facility • 66
 - nwagent command • 66
 - open files • 40
 - path name • 40
 - unload nwagent command • 66
- network interface cards (NIC)
 - IP address • 34
 - multiple on Windows • 13
- Novell directory services (NDS) • 41
- nwagent command • 66
- nwagent.log NetWare log file • 63

O

- OpenVMS
 - bab\$shutdown.com command • 69
 - bab\$startup.com command • 69
 - configuration • 59
 - show sys /proc=aso\$* command • 69
 - TCP/IP stack optimization • 60

P

- password, Windows • 36
- port address configuration • 43
- port numbers, Common Agent • 21
- port.cfg
 - about UNIX and Linux configuration file • 43
 - for Common Agent • 21
- PortsConfig.cfg configuration file • 34
- print filename command • 63
- protocol • 27
- push technology • 11

R

- runtime statistics • 61

S

- scripts
 - uagentsetup • 67
 - use to modify agent.cfg file • 67
- security features • 12
- show sys /proc=aso\$* OpenVMS command • 69
- single user mode • 56
- Snapshot
 - about • 50
 - buffer • 50
 - feature overview • 16
 - features • 50
 - output • 50
 - UNIX support • 50
- starting client agents • 65
- stopping client agents • 65
- straso AS/400 command • 68
- system requirements • 17

T

- trace levels
 - AS/400 • 54
 - OpenVMS • 60

U

- uag.cfg • 41
- uag.cntl Directory Control file • 43
- uag.log activity log file • 63
- uagent command • 67
- uagentsetup script • 67
- UDP port, Common Agent • 21
- unload nwagent command • 66

- user access, Common Agent • 23

V

- virus scanning • 38
- virus scanning (Windows and NetWare) • 12

W

Windows

- Auto Discovery of client agents • 13
- Backup Agent Admin • 30
- enable virus scanning • 38
- IP address • 34
- password security • 30
- port number • 34
- process priority • 30
- shares support • 28
- system hive restore • 28
- system state restore • 28