

Arcserve® Backup

Client Agents Guide

r17

arcserve®

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by Arcserve 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 Arcserve. This Documentation is confidential and proprietary information of Arcserve and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and Arcserve governing your use of the Arcserve software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and Arcserve.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Arcserve copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Arcserve that all copies and partial copies of the Documentation have been returned to Arcserve or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, ARCSERVE 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 ARCSERVE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF ARCSERVE IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Arcserve.

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.

© 2016 Arcserve, including its affiliates and subsidiaries. All rights reserved. Any third party trademarks or copyrights are the property of their respective owners.

Arcserve Product References

This document references the following Arcserve products:

- Arcserve® Backup
- Arcserve® Unified Data Protection
- Arcserve® Unified Data Protection Agent for Windows
- Arcserve® Unified Data Protection Agent for Linux
- Arcserve® Replication and High Availability

Contact Arcserve

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

<https://www.arcserve.com/support>

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge-base (KB) documents. From here you easily search for and find the product-related KB articles which contain field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Global User Community to ask and answer questions, share tips and tricks, discuss best practices and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.

You can access other helpful resources appropriate for your Arcserve product.

Contents

Chapter 1: Introducing the Client Agents 7

Introduction	7
Benefits of Using a Client Agent	7
Supported Client Systems	8
Access the Backup Agent Admin	10

Chapter 2: Installing the Client Agents 11

Installation Considerations	11
Client Agent for Windows	11
Communication Requirements for Client Agents Installed on UNIX, Linux, and Mainframe Linux Platforms	11
Install the Client Agents	12
Common Agent Automatic Installation	12
Installation Directories for the Common Agent and Client Agents	12

Chapter 3: Adding and Configuring the Client Agents 15

Adding Client Agents	15
How to Add, Import, and Export Agents and Nodes	15
Manually Add Client Agents	16
Windows Client Agent Configuration	19
Windows-Related Configuration Notes	19
Security Configuration Options	19
Backup Priority and Restore/Compare Priority Options	20
Multiple Concurrent Restore or Compare	20
Backup and Restore Execution Options	21
Use the Backup Agent Admin to Set Windows Parameters	21
Configure Password Security	25
View Configuration Selections	25
Enable Raw Backup and Restore	26
Configure Windows Network Communication	27
Set a Workstation Password	29
Create Windows Access Control List	30
Customizable Local Options	31
How the Client Agent for Windows Excludes Database Application Files from Backups	31
UNIX, Linux, and Mac OS X Client Agent Configuration	32
UNIX, Linux, and Mac OS X Configuration Considerations	32

UNIX, Linux, and Mac OS X Client Agent Control Files	33
Common Agent Configuration File for UNIX, Linux, and Mac OS X.....	34
Snapshot and Direct I/O Support for UNIX	42
UNIX, Linux, and Mac OS X Access Control Lists	47
Chapter 4: Using the Client Agents	51
Runtime Statistics.....	51
View Runtime Statistics for the Client Agent for Windows	51
Activity Logs	52
View Activity Logs on a Windows Server	52
View Activity Logs on a UNIX, Linux, or Mac OS X Client Agent Machine	52
Delete Client Agent Log Files.....	53
Back Up Windows Network Server Data	53
Client Agent Start and Stop Procedures	53
Windows Start and Stop Requirement	54
UNIX, Linux, and Mac OS X Client Agents Start and Stop Requirement.....	54
Glossary	57
Index	59

Chapter 1: Introducing the Client Agents

This section contains the following topics:

[Introduction](#) (see page 7)

[Benefits of Using a Client Agent](#) (see page 7)

[Supported Client Systems](#) (see page 8)

[Access the Backup Agent Admin](#) (see page 10)

Introduction

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 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 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.

Benefits of Using a Client Agent

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 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 Arcserve Backup server
- Communicate with the server and let you browse and select backup components

- Assist with monitoring the progress of backup jobs
- Maintain and monitor backup logs with the status of backup and restore activities
- Facilitate backup of applications or file systems

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

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

Supported Client Systems

Arcserve Backup offers client agents that support the following platforms:

Note: For a detailed description of supported operating systems and versions, see the *Client Agents Readme* file located on the Arcserve Backup installation media.

- Arcserve Backup Client Agent for Windows. This client agent supports the following:
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows 8
 - Windows Server 2008
 - Windows Server 2008 R2
 - Windows 7
 - <vista>
 - Windows XP
 - Windows Server 2003
 - Windows Small Business Server (Windows 2003)
 - Windows 10
- Arcserve Backup Client Agent for UNIX. This client agent supports the following:
 - AIX
 - HP-UX
 - Solaris
 - Tru64
 - FreeBSD

- Arcserve Backup Client Agent for Linux. This client agent supports the following:
 - Red Hat
 - SuSE
 - Turbo
 - Debian
 - RedFlag
 - Miracle Linux
 - Asianux
- Arcserve Backup Client Agent for Mainframe Linux. This client agent supports the following:
 - Red Hat Enterprise Server
 - SLES
- Arcserve Backup Client Agent for Mac OS X

Access the Backup Agent Admin

The Backup Agent Admin allows you to configure various agents and set multiple options. You can view data about the agent desktop regarding the local system, connections, agent status, and configuration options. The following options are available using the Backup Agent Admin:

- [Services](#) (see page 54)
- [Network Configuration](#) (see page 27)
- Access Control List
- [Delete Client Agent Log Files](#) (see page 53)
- AD Object Level Restore Utility

To access the Backup Agent Admin:

1. From the Windows Start menu, select All Programs, Arcserve, Arcserve Backup, Backup Agent Admin.

The Arcserve Backup Agent Admin dialog opens.

2. Select one of the following agents to configure from the drop-down list:

- Agent for Microsoft Exchange
- Agent for Microsoft SharePoint
- Agent for Microsoft SQL Server
- Agent for Virtual Machines
- Client Agent

3. Click the Configuration icon.

The appropriate configuration dialog opens.

4. Complete the fields and click OK.

The selected agent is configured.

Chapter 2: Installing the Client Agents

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

This section contains the following topics:

[Installation Considerations](#) (see page 11)

[Install the Client Agents](#) (see page 12)

[Common Agent Automatic Installation](#) (see page 12)

[Installation Directories for the Common Agent and Client Agents](#) (see page 12)

Installation Considerations

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

Client Agent for Windows

Before you install or 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

Communication Requirements for Client Agents Installed on UNIX, Linux, and Mainframe Linux Platforms

To help ensure that Arcserve Backup primary servers and member servers can communicate with the Arcserve Backup agents that are installed on UNIX, Linux, and Mainframe Linux computers, you must allow Arcserve Backup to communicate with the agent through the firewall, if any, that is configured on the agent computers. You can allow Arcserve Backup to communicate with the agent computers by adding Arcserve Backup to the firewall exceptions list on the agent computers.

As a best practice, you should add Arcserve Backup to the firewall exceptions list on the agent computers before you install the agents.

This requirement affects the following Arcserve Backup components:

- Client Agent for UNIX
- Client Agent for Linux
- Client Agent for Mainframe Linux
- Oracle Agent on UNIX platforms
- Oracle Agent on Linux platforms
- UNIX and Linux Data Mover

For information about how to configure the firewall on the agent computers, see the platform-specific documentation.

Note: By default, Arcserve Backup communicates using port 6051.

Install the Client Agents

To install a windows client agent or a cross-platform agent, use the Arcserve Backup for Windows DVD.

For more information about installing Arcserve Backup client agents, click the following links on the Arcserve Backup installation browser:

- [Installation Instructions for Arcserve Backup Client Agents for non-Windows platforms.](#)
- [Installation Instructions for Arcserve Backup UNIX and Linux Data Mover.](#)

Common Agent Automatic Installation

When you install the client agent for UNIX, Linux, or Mac OS X, the Arcserve Backup Common Agent is automatically installed.

Installation Directories for the Common Agent and Client Agents

The following table describes the default installation paths for the Arcserve Backup Common Agent and the Arcserve Backup Client Agents for UNIX and Linux platforms.

Platform	Version	Common Agent / Agent Configuration File	Client Agent (File System Agent)
AIX		/opt/CA/ABcmagt	/opt/CA/ABuagent

Platform	Version	Common Agent / Agent Configuration File	Client Agent (File System Agent)
HP		/opt/CA/ABcmagt	/opt/CA/ABuagent
Solaris	SPARC 8, 10 x86	/opt/CA/BABcmagt	/opt/CA/BABuagent
Solaris	SPARC 9, 10	/opt/CA/ABcmagt	/opt/CA/ABuagent
Linux	SUSE Redhat Linux-OES Asianux Miracle Red Flag Turbo Linux	/opt/Arcserve/ABcmagt	/opt/Arcserve/ABuagent
FreeBSD		/opt/CA/BABcmagt	/opt/CA/BABuagent
Debian		/opt/Arcserve/ABcmagt	/opt/Arcserve/ABuagent
ESX		/opt/CA/ABcmagt	/opt/CA/ABuagent
Tru64		/opt/CA/BABcmagt	/opt/CA/BABuagent

Note: The above directories also appear in the Common Agent configuration file (agent.cfg) along with other related configuration files for the file system agents and the Agent for Oracle.

For a complete list of supported versions of operating systems, see the Client Agents Readme file located on the Arcserve Backup installation media.

Chapter 3: Adding and Configuring the Client Agents

After installing 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:

[Adding Client Agents](#) (see page 15)

[Windows Client Agent Configuration](#) (see page 19)

[UNIX, Linux, and Mac OS X Client Agent Configuration](#) (see page 32)

Adding Client Agents

If you have Arcserve Backup installed on a Windows server, you can add client agents from your network using the Add, Import, Export Node feature or you can add client agents manually. The following sections include information on each of these methods.

How to Add, Import, and Export Agents and Nodes

Setting up a job in an environment with many agents and nodes can be a time-consuming and tedious task. If you have multiple agents and nodes to back up, it may take time to add the agents and nodes to the Backup Manager one at a time. The Add, Import, and Export Agents and Add, Import, and Export Nodes features let you add multiple nodes and agents using the Arcserve Backup user interface, whether the nodes and agents will be backed up.

Note: The Central Agent Admin also lets you add, import, or export agents and nodes.

You can use the Add, Import, and Export Nodes feature to add multiple nodes and agents into the system in either of the following ways:

Add multiple agents and nodes using the user interface

1. From the Backup Manager Source Tab or the Restore Manager Destination Tab, select a node.
2. Use the Add/Import/Export Nodes dialog to manually enter the names of all the nodes and agents or select the nodes from the left-pane list of nodes and agents detected by auto-discovery.
3. Specify a user name and password for the nodes.

4. Save the information in the Arcserve Backup database.
5. View the nodes and agents in the Backup Manager Source tree or the Central Agent Admin.

Add multiple nodes and agents using a .csv and .txt file

1. From the Backup Manager Source Tab or the Restore Manager Destination Tab, select a node.
2. Use the Import function on the Add/Import/Export Nodes dialog and specify the name of the .csv or .txt file from the user interface.

The node and agent names are imported from the .csv or .txt file and are added into the system.

3. Specify a user name and password for the nodes and agents.
4. View the nodes and agents in the Backup Manager Source tree.

Manually Add Client Agents

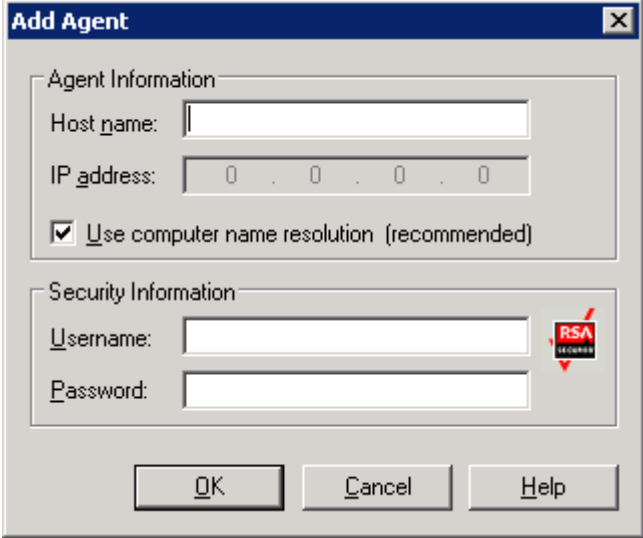
If Auto Discovery does not detect all client agents in your network for some reason or if you want to add a particular client agent, you can manually add a client agent to a Windows server using the Windows manager interface. To manually add a client agent, whether it's through Group View or Classic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

To manually add client agents in a Group View

1. Open the Backup Manager and click the Source tab.
The Source directory tree appears.
2. Select Group View from the drop-down list.
3. Right-click the appropriate client agent object, such as Client Agent.

4. Select Add Machine/Object.

The Add Agent dialog appears.



5. Enter the name of the computer in the Host Name field.
6. Select the protocol you want to use to connect to the computer. 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.

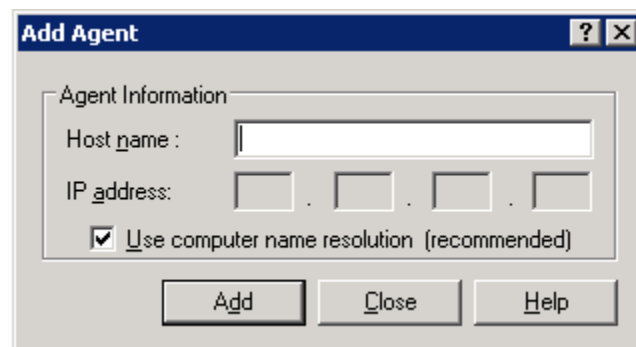
7. Enter the Username and Password for the computer in the Security Information section.
8. Click OK.

The client agent is added to the server.

To manually add client agents in a Classic View

1. Open the Backup Manager and click the Source tab.
The Source directory tree appears.
2. Select Classic View from the drop-down list.
3. Right-click the appropriate client agent object, such as Windows Systems.
4. Select Add Machine/Object.

The Add Agent dialog appears.



5. Enter the name of the computer in the Host Name field.
6. Select the protocol you want to use to connect to the computer. 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.

7. Click Add.

The client agent is added to the server.

Windows Client Agent 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 (such as 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 Options

The Client Agent for Windows 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.CMD) 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.CMD) 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

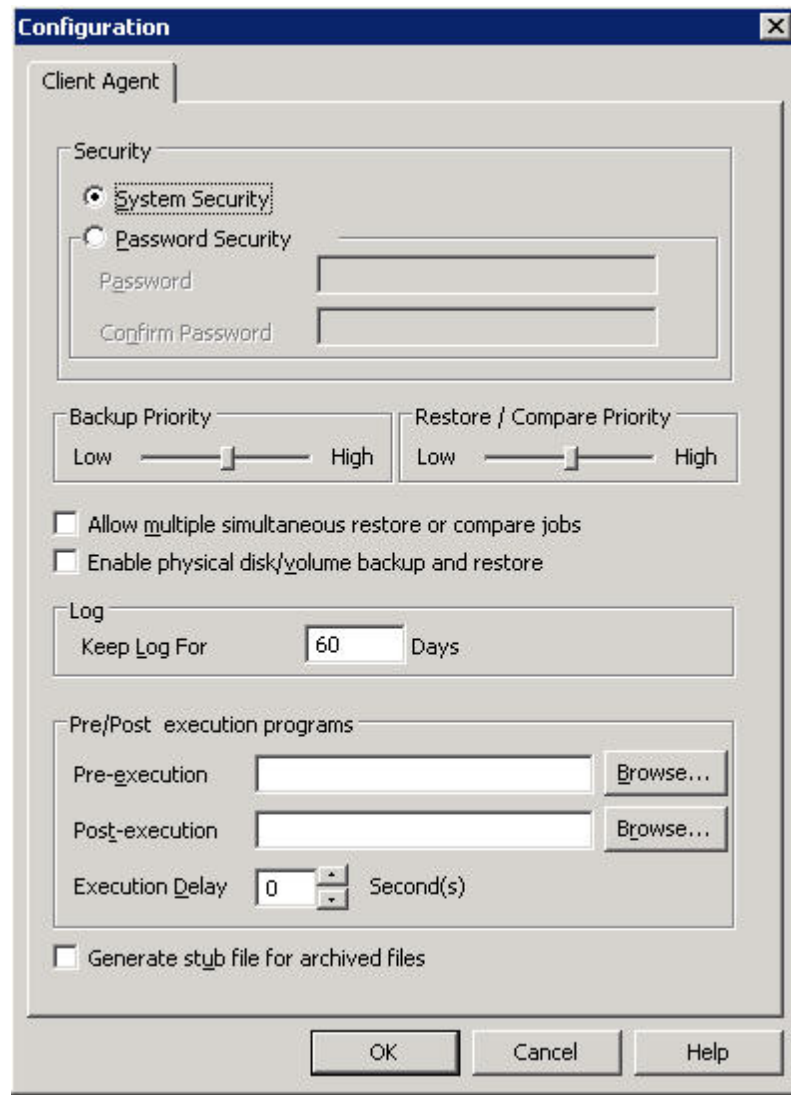
To use the Backup Agent Admin to set Windows parameters

1. Access the Agent Admin by clicking Start, Programs or All Programs, Arcserve, 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.

- 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.

Note: If you select System Security, Exchange Server 2010 database files are not backed up (that is, they are skipped) when you use the client agent to select partitions, folders or files for backup when the client agent backup account is a domain account with View Only Organization Management role or higher privileges. Exchange Server 2010 database files are not skipped if you select Password Security, or if you use some other account role, such as local administrator or domain account without View-only Organization Management privileges. The system displays a warning when these database files are in use.

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 Arcserve Backup server.

- **Enable physical disk/volume backup and restore**--Lets you perform raw backups and restores on physical disks and volumes.

Note: For more information, see the Administration Guide.

- **Log**--The Log file is stored in the following path: <ARCserve_HOME>\ARCserve Backup Client Agent for Windows\ntagent.log. The log for every job that runs is stored in this log file.

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\POST.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.

- **Generate stub file for archived files**--Select this option to generate files that contain information about the data included in an archive 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

The client agent service uses the node (machine) user name and assigned password to log on to the Arcserve 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

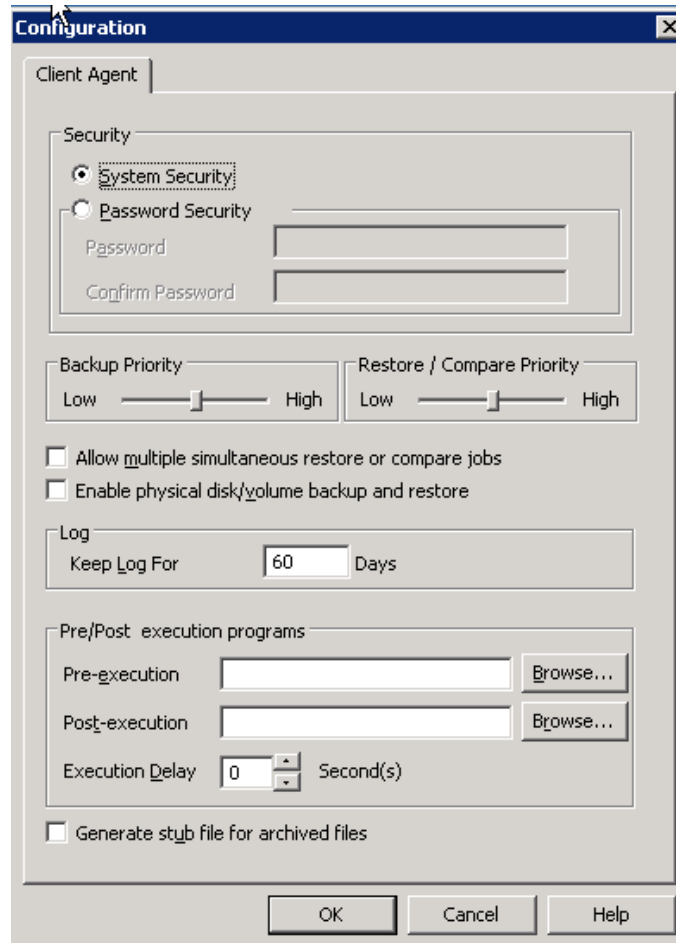
Before making changes to your configuration settings, you should verify your current configuration.

To view your configuration selections

1. Open the Backup Agent Admin.

- Expand Options and then select Configuration.

The current settings are displayed.



Enable Raw Backup and Restore

You can use Arcserve Backup to perform raw backup and restore of physical disks and volumes.

The capability to perform raw backup and restore of physical disks and volumes is disabled by default. You must enable the option for each agent.

To enable raw backup and restore of a physical disk or volume

- From the Windows Start menu, click Start, Programs, Arcserve, Arcserve Backup, and Backup Agent Admin.

The Arcserve Backup Agent Admin window appears.

2. Click Options, Configuration.

The Configuration window appears.

3. Click Enable physical disk/volume backup and restore.
4. Click OK.

The raw backup and restore feature is enabled for the agent.

For more information on how you can perform raw backup and restore, see the *Administration Guide*.

Configure Windows Network Communication

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 Windows network communication

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

Network Configuration

Specify Port Number

The Backup Agent will listen using these port values.

TCP/IP

UDP

VI protocol

Enable VI support Lets the agent attempt to communicate using Virtual Interface Protocol.

Select IP Address

Lets you specify an IP address that the agent will use to communicate.

You must restart the Client Agent for Windows service to apply the new configurations. After the service restart, you can verify the configuration in the Agent Status view.

3. 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 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 Arcserve Backup server component. To do this, you must modify the remote server PortsConfig.cfg file. For more information on port configuration, see the *Implementation 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 Arcserve Backup home directory.

Example:

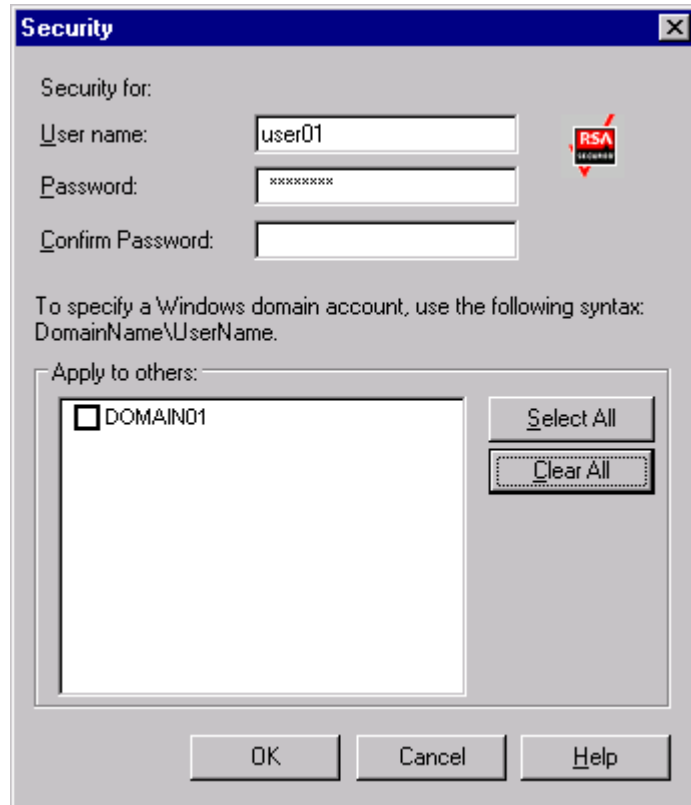
```
#Hostname IP address (optional) TCP port UDP port
#myhost nnn.nnn.nnn.nnn 6050 6050
mymachine nnn.nnn.nnn.nnn 7090 7085
```

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 Arcserve Backup.

To set a workstation password

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 Windows Access Control List

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 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

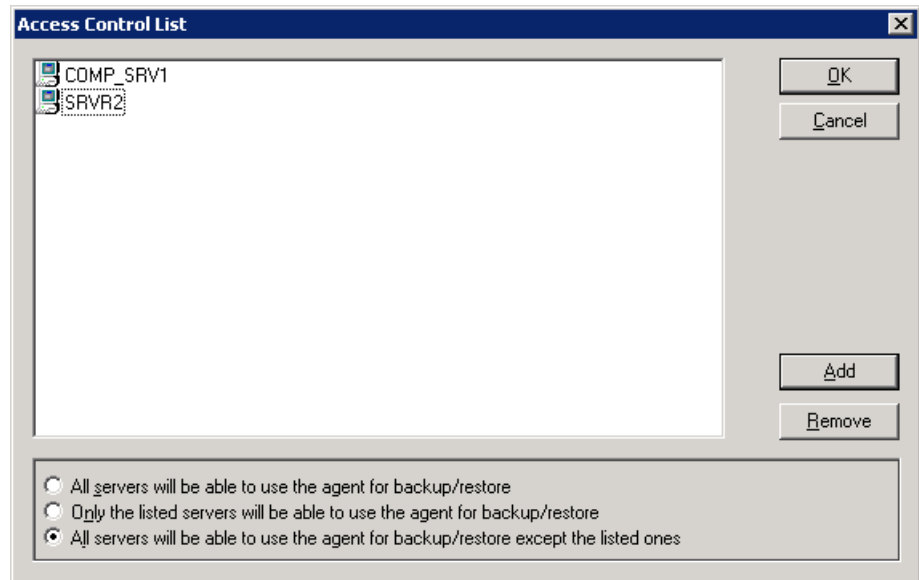
A list of servers allowed to access the client agent machine for backup and restore options.

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 a Windows access control list

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. Do not provide IP address as a name to add client agents.
5. Click Remove for each client node, if you want to remove the client agent from the list.
6. Click OK when you finish adding or removing client agent names.

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*.

How the Client Agent for Windows Excludes Database Application Files from Backups

The Client Agent for Windows can exclude database and log files from backups of database applications, such as Microsoft Exchange and Microsoft SQL Server, when performing backups.

During the backup job, the Client Agent for Windows communicates with the database agent to obtain a list of files that the backup job should exclude from the file system backup. The Client Agent for Windows then excludes files from the file system backup based on the response received from the database agent. If the database agent is offline, the Client Agent assumes all files should be backed up and the file system backup job proceeds accordingly.

Example:

When you select a Microsoft Exchange server directory as the backup source and perform file system backup using the Client Agent for Windows, the following exclusion behavior occurs:

- If the Exchange Information Store is online, the Agent for Microsoft Exchange Server provides a list of the Exchange databases and log files that should be excluded from the backup job.

As a result, Arcserve Backup skips the excluded files and completes the file system backup.

- If the Exchange Information Store is offline, the Agent for Microsoft Exchange Server provides an empty list of Exchange databases and log files that should be excluded from the backup job.

As a result, Arcserve Backup does not skip the Exchange server files and includes all files during the file system backup.

UNIX, Linux, and Mac OS X Client Agent Configuration

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 Arcserve 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 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.

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 Common Agent
- The Universal 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 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. It is installed automatically during the first installation of UNIX, Linux, or Mac OS X client agent.

The Common Agent resides in the /opt/Arcserve/BABcmagt directory. It 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/Arcserve/BABcmagt directory.

Note: Arcserve Backup installs related configuration files for the Common Agent, the file system agents, and the Agent for Oracle in different directories on the various UNIX and Linux platforms. For more information, see Installation Directories for the Common Agent and Client Agent For UNIX and Linux.

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 as follows:

```
[0]
#[ABagtux]
NAME    ABagtux
VERSION nn.nn.nn
HOME    /opt/Arcserve/ABuagent
#ENV    CA_ENV_DEBUG_LEVEL=4
ENV     UAGENT_HOME=/opt/Arcserve/ABuagent

ENV
        LD_LIBRARY_PATH=/opt/Arcserve/ABcmagt:$LD_LIBRARY_PATH:/SharedComponents/lib:/opt/Arcserve/ABuagent/lib
ENV
        SHLIB_PATH=/opt/Arcserve/ABcmagt:$SHLIB_PATH:/SharedComponents/lib:/opt/Arcserve/ABuagent/lib
ENV
        LIBPATH=/opt/Arcserve/ABcmagt:$LIBPATH:/SharedComponents/lib:/opt/Arcserve/ABuagent/lib
BROWSER    cabr
AGENT      uagentd
MERGE      umrgd
VERIFY     umrgd

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

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 ABagtux	Name of the client agent
VERSION nn.n	Release and version number of the client agent
HOME /opt/Arcserve/ABuagent	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
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, ABuagent, 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 ABagntux section of the file. The name of the client agent home directory is defined by the HOME variable.

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 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]
#[ABagntux]
NAME          ABagntux
VERSION       nn.nn.nn
HOME          /opt/Arcserve/ABuagent
#ENV          CA_ENV_DEBUG_LEVEL=4
ENV           UAGENT_HOME=/opt/Arcserve/ABuagent

ENV
LD_LIBRARY_PATH=/opt/Arcserve/ABcmagt:$LD_LIBRARY_PATH:/SharedComponents/lib:/opt/Arcserve/ABuagent/lib
ENV
SHLIB_PATH=/opt/Arcserve/ABcmagt:$SHLIB_PATH:/SharedComponents/lib:/opt/Arcserve/ABuagent/lib
ENV
LIBPATH=/opt/Arcserve/ABcmagt:$LIBPATH:/SharedComponents/lib:/opt/Arcserve/ABuagent/lib
BROWSER       cabr
AGENT         uagentd
MERGE         umrgd
VERIFY        umrgd
```

Port Address Configuration

The default port for TCP and UDP is 6051. The TCP port is used for communication and data transfer between the backup server 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 Arcserve Backup server and the client agent so that their values match.

The names of the configuration files are as follows:

- **CAPortConfig.cfg**—for 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.

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

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

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

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

Common Agent Port Numbers

By default, the Common Agent uses port number 6051 for both TCP and UDP. To change the default port, you must modify the ABcmagt 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, **do not use** this method 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]
#[ABcmagt]
#NAME          ABcmagt
#HOME          /opt/Arcserve/ABcmagt
#TCP_PORT      6051
#UDP_PORT      6051
```

After the change:

```
[36]
#[ABcmagt]
NAME          ABcmagt
HOME          /opt/Arcserve/ABcmagt
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 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— \$AB_HOME/config/port.cfg—on the backup server.

By default, the Common Agent uses another UDP port, 0xA234 (41524), to receive 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]
#[ABcmagt]
NAME    ABcmagt
HOME    /opt/Arcserve/ABcmagt
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.

How Common Agent Connection Requests Work

To initiate a client agent session, the 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 are available for use when starting the UNIX, Linux, or Mac OS X client agents as 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 Arcserve Technical Support representative.

Option	Description
-ALLOW <network address> <host address>	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.

Option	Description
-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
-Prebackup <i>filename</i>	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, uag_pre_backup will be treated as the filename.
-Postbackup <i>filename</i>	
-Prerestore <i>filename</i>	
-Postrestore <i>filename</i>	
-S	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 -ALLOW, -DENY, or -CAUSER options. For more information see the specific option.
-s <i>async / nonblocking</i>	Sets socket I/O to asynchronous, nonblocking mode.
-s <i>bufsize</i>	Specifies the size of the socket buffer. Options are 4096 to 65536. The default is system dependent.
-s <i>SocketMode</i>	Specifies to use socket mode for backup operations.
-sparse	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 -sparse.
-verbose or -v	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/Arcserve/ABcmagt directory.

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

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

2. Prepare the configuration file named caagperf.cfg in the /opt/Arcserve/ABcmagt directory. You need to specify the types of operations to be completed on the specified file systems in the caagperf.cfg file.

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 the 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.

Configuration Files for UNIX Systems

The following are examples of different variations of UNIX systems configuration files.

Example: 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
```

Example: 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
```

Example: HP-UX operating system having 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
```

Trace Levels for the AS/400 Enterprise Option

Occasionally, based on instructions from Arcserve 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 Arcserve 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.

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/ABcmagt`. 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:

Example: Allow or Deny Users

An access control list can deny or allow 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]
NAME ABagentux
VERSION nn.n.n
HOME /opt/Arcserve/ABuagent
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].

Example: Access the System with IP Addresses

An access control list can determine 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]
NAME ABagentux
VERSION nn.n.n
HOME /opt/Arcserve/ABuagent
NOPASSWORD
ALLOW N:172.16.0.0(255.255.255.0) H:172.31.255.255
DENY N:192.168.0.0(255.255.255.0) H:192.168.255.255
```

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.

Backup and Restore Access Control List Support for UNIX and Linux

Arcserve Backup Client Agent for UNIX, Arcserve Backup Client Agent for Linux, and 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 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, you must install them.

Install ACL Library Packages

To install ACL library packages

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-2.3.3-1.rpm)
```

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

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

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.

Verify the Linux ACL library version

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 4: Using the Client Agents

This chapter includes details such as how you can start and stop client agents, and how you can schedule or initiate backup and restore jobs of client agents in a standard backup environment.

This section contains the following topics:

[Runtime Statistics](#) (see page 51)

[Activity Logs](#) (see page 52)

[Back Up Windows Network Server Data](#) (see page 53)

[Client Agent Start and Stop Procedures](#) (see page 53)

Runtime Statistics

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

Note: Runtime statistics apply only to Windows.

View Runtime Statistics for the Client Agent for Windows

Arcserve Backup lets you view runtime statistics for computers running the Client Agent for Windows.

To view runtime statistics for the Client Agent for Windows

1. From the Windows Start Menu, select Programs, Arcserve, Arcserve Backup, and click Backup Agent Admin.

The Backup Agent Admin opens.

2. Select Connections.

Arcserve Backup displays the last 32 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 stored in memory. Therefore, if you close the Backup Agent Admin and the Universal Agent service, the connection statistics will be lost. However, you will still be able to view the results of the job in the Activity Log.

Activity Logs

The server-based 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 Arcserve Backup server

1. From the Quick Start menu on the Arcserve Backup Manager Console, select Job Status.
The Job Status Manager opens.
2. Click the Activity Log tab to view a list of logs.
3. From the Job Status menu, select Activity Log and click Print Preview.
The print preview output of a client agent activity log file appears.

View Activity Logs 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/Arcserve/ABcmagt/logs/caagentd.log` file.

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 agent, use the Backup Agent Admin to delete log files. In the Options menu, select Delete Client Agent Log Files. Select the log files you want to delete and click Delete.

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.

To back up Windows network server data

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.

Windows Start and Stop Requirement

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.

Start or Stop the Windows Client Agent

To start or stop a Windows client agent

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 option, Start the backup agent service as the system starts.
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.

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:

```
#abuagent/uagentsetup
```

In this example, *abuagent* represents the full path name of the agent home directory. The default path is `/opt/Arcserve/ABuagent`.

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, type the following command at the command line:

```
# uagent status
```

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

```
# uagent stop
```

Common Agent Start and Stop Status

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 `ABagntux` section disabled. If `ABagntux` is the only section of the file (that is, there is only one Arcserve Backup client agent installed), the Common Agent stops. You would then need to issue `uagent start` to enable the `ABagntux` 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:

```
#abuagent/uagentsetup
```

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

Glossary

access control list

An *access control list* (ACL) is a list of access control entries (ACE). Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied, or audited for that trustee.

activity log

An *activity log* is a log file that displays information about all the jobs that the client agent processes.

client agents

The *client agents* are separate software packages installed on network computers to supply a network interface between the computer and Arcserve Backup. In addition to enabling connectivity, the client agents share data storage tasks with the backup servers in your network.

Index

A

- ABuagent/uagentsetup command • 55
- ACL library
 - 32-bit Linux • 48
 - Linux libacl.so • 48
 - packages • 48
 - requirements • 48
- activity log
 - about • 52
 - sample • 52
 - viewing • 52
- add a client agent
 - manually to a Windows server • 16
- add or auto discover Client Agents • 15

B

- Browser Configuration file • 33

C

- caagperf.cfg configuration file • 42
- caagperf.log file • 42
- cabr.cfg Browser Configuration file • 33
- CAPortConfig.cfg
 - example • 27
- check agent status
 - UNIX, Linux, Mac OS X • 55
- commands
 - \$>rm uag.log • 53
 - ABuagent/uagentsetup • 55
 - mount • 42
 - uagent status • 55
- Common Agent
 - automatic installation • 12
 - connecting • 39
- computer name resolution
 - select protocol • 53
- configuration files
 - caagperf.cfg • 42, 44
 - CAPortConfig.cfg • 27
 - PortsConfig.cfg • 27
 - Solaris sample • 45
- configuring
 - UNIX, Linux, and Mac OS X client agent • 32
 - Windows client agent • 19

- Windows network communication • 27
- Windows security options • 25
- control files • 33
- create link from 32-bit library to libacl.so • 49

D

- Direct I/O
 - about • 42
 - UNIX support • 42
- Directory Control file • 33

F

- File System Control file • 33
- fs.cntl File System Control file • 33
- fssnap • 42

H

- home directory • 36

I

- install
 - ACL libraries • 48
 - client agent for Windows • 12
- installation considerations
 - Windows • 11

J

- job packaging • 31

L

- libacl.so ACL library • 48
- Linux
 - 32-bit ACL library • 48
 - link to 32-bit ACL Library • 49
 - verify ACL library version • 49
- log files
 - activity • 52
 - caagperf.log • 42
 - deleting • 53

M

- manager interface for Windows • 16

N

network interface cards (NIC)
IP address • 27

P

password, Windows • 29
PortsConfig.cfg configuration file • 27
protocol • 16

R

runtime statistics • 51

S

scripts
uagentsetup • 55
use to modify agent.cfg file • 55
Snapshot
about • 42
buffer • 42
features • 42
output • 42
UNIX support • 42
starting client agents • 53
stopping client agents • 53

U

uag.cfg • 32
uag.cntl Directory Control file • 33
uagent command • 55

W

Windows
IP address • 27
port number • 27
shares support • 19
system hive restore • 19
system state restore • 19